Riverbed® Command-Line Interface Reference Manual

Steelhead® CX (Series *xx*55) - RiOS Version 8.5.1
Steelhead® EX (Series *xx*60) - EX Version 3.0
Steelhead® (Series *xx*50) - RiOS Version 8.5.1
Granite™ Core Appliance - Version 2.5
Riverbed® Central Management Console - Version 8.5
Interceptor® Appliance - Version 4.0
Steelhead® Mobile Controller- Version 4.0
Cloud Steelhead® - Version 2.0
Steelhead® Cloud Accelerator - Version 1.0

November 2013

This documentation is furnished “AS IS” and is subject to change without notice and should not be construed as a commitment by Riverbed Technology. This documentation may not be copied, modified or distributed without the express authorization of Riverbed Technology and may be used only in connection with Riverbed products and services. Use, duplication, reproduction, release, modification, disclosure or transfer of this documentation is restricted in accordance with the Federal Acquisition Regulations as applied to civilian agencies and the Defense Federal Acquisition Regulation Supplement as applied to military agencies. This documentation qualifies as “commercial computer software documentation” and any use by the government shall be governed solely by these terms. All other use is prohibited. Riverbed Technology assumes no responsibility or liability for any errors or inaccuracies that may appear in this documentation.

riverbed

Riverbed Technology
199 Fremont Street
San Francisco, CA 94105

Phone: 415.247.8800
Fax: 415.247.8801
Web: http://www.riverbed.com

Part Number
712-00002-19

Contents

Preface

Welcome to the *Riverbed Command-Line Interface Reference Manual.* Read this preface for an overview of the information provided in this guide and the documentation conventions used throughout, hardware and software dependencies, additional reading, and contact information. This preface includes the following sections:

About This Guide

The *Riverbed Command-Line Interface Reference Manual* is a reference manual for the command-line interface. The following products are discussed in this guide:

- Riverbed Optimization System (RiOS system)
- Riverbed Steelhead appliance (Steelhead appliance)
- Riverbed Steelhead CX appliance (Steelhead CX)
- Riverbed Steelhead EX appliance (Steelhead EX)
- Riverbed Granite Core appliance (Granite Core)
- Riverbed Cloud Steelhead appliance (CSH)
- Riverbed Steelhead Cloud Accelerator software (SCA)
- Riverbed Interceptor appliance (Interceptor appliance)
- Riverbed Central Management Console (CMC)
- Riverbed Steelhead Mobile Controller (Mobile Controller)

This manual documents command descriptions, syntax, parameters, usage guidelines, examples, and related topics for each command.

Audience

This guide is written for storage and network administrators familiar with administering and managing WANs using common network protocols such as TCP, CIFS, HTTP, FTP, and NFS.

Document Conventions

This manual uses the following standard set of typographical conventions.

Convention	Meaning
italics	Within text, new terms and emphasized words appear in italic typeface.
boldface	Within text, CLI commands and GUI controls appear in bold typeface.

Courier	Code examples appears in Courier font:
	`amnesiac > enable`
	`amnesiac # configure terminal`

< >	Values that you specify appear in angle brackets: **interface <ipaddress>**
[ ]	Optional keywords or variables appear in brackets: **ntp peer <addr> [version <number>]**
{ }	Required keywords or variables appear in braces: **{delete <filename>}**
|	The pipe symbol represents a choice to select one keyword or variable to the left or right of the symbol. (The keyword or variable can be either optional or required): **{delete <filename> | upload <filename>}**

Product Dependencies and Compatibility

This section provides information about product dependencies and compatibility. It includes the following information:

- "Hardware and Software Dependencies" on page 2

Hardware and Software Dependencies

The following table summarizes the hardware and software requirements for the Steelhead appliance.

Riverbed CLI Hardware Requirements	Software/Operating System Requirements
One of the following: • An ASCII terminal or emulator that can connect to the serial console (9600 baud, 8 bits, no parity, 1 stop bit, and no flow control). • A computer with a Secure Shell (ssh) client that is connected by an IP network to the appliance primary interface.	• Secure Shell (ssh). Free ssh clients include PuTTY for Windows computers, OpenSSH for many Unix and Unix-like operating systems, and Cygwin.

Additional Resources

This section describes resources that supplement the information in this guide. It includes the following information:

- "Release Notes" on page 3
- "Riverbed Documentation and Support Knowledge Base" on page 3

Release Notes

The following online file supplements the information in this guide. It is available on the Riverbed Support site at https://support.riverbed.com.

Online File	Purpose
<product>_<version_number> <build_number>.pdf	Describes the product release and identifies fixed problems, known problems, and work-arounds. This file also provides documentation information not covered in the guides or that has been modified since publication.

Examine this file before you begin installation and configuration. It contains important information about this release of the Steelhead appliance.

Riverbed Documentation and Support Knowledge Base

For a complete list and the most current version of Riverbed documentation, visit the Riverbed Support Web site located at https://support.riverbed.com.

The Riverbed Knowledge Base is a database of known issues, how-to documents, system requirements, and common error messages. You can browse titles or search for keywords and strings.

To access the Riverbed Knowledge Base, log in to the Riverbed Support site located at https://support.riverbed.com.

Contacting Riverbed

This section describes how to contact departments within Riverbed.

Internet

You can learn about Riverbed products at http://www.riverbed.com.

Technical Support

If you have problems installing, using, or replacing Riverbed products, contact Riverbed Support or your channel partner who provides support. To contact Riverbed Support, open a trouble ticket by calling 1-888-RVBD-TAC (1-888-782-3822) in the United States and Canada or +1 415 247 7381 outside the United States. You can also go to https://support.riverbed.com.

Professional Services

Riverbed has a staff of professionals who can help you with installation, provisioning, network redesign, project management, custom designs, consolidation project design, and custom coded solutions. To contact Riverbed Professional Services, email proserve@riverbed.com or go to http://www.riverbed.com/us/products/professional_services/.

Documentation

The Riverbed Technical Publications team continually strives to improve the quality and usability of Riverbed documentation. Riverbed appreciates any suggestions you might have about its online documentation or printed materials. Send documentation comments to techpubs@riverbed.com.

CHAPTER 1 Using the Command-Line Interface

This chapter describes how to access and use the CLI. This chapter includes the following sections:

Connecting to the CLI

This section assumes you have already performed the initial setup of the appliance using the configuration wizard. For detailed information, see the installation guide for the system.

To connect the CLI

1. You can connect to the CLI using one of the following options:

   - An ASCII terminal or emulator that can connect to the serial console. It must have the following settings: 9600 baud, 8 bits, no parity, 1 stop bit, and no flow control.

   - A computer with an SSH client that is connected to the appliance Primary port (in rare cases, you might connect through the Auxiliary port).

2. At the system prompt enter the following command if the appliance resolves to your local DNS:

   ```
   ssh admin@host.domain
   ```

   otherwise at the system prompt enter the following command:

   ```
   ssh admin@ipaddress
   ```

3. When prompted, enter the administrator password. This is the password you set during the initial configuration process. The default password is **password**. For example:

```
login as: admin
Riverbed Steelhead
Last login: Wed Jan 20 13:02:09 2010 from 10.0.1.1
amnesiac >
```

You can also log in as a monitor user (**monitor**). Monitor users cannot make configuration changes to the system. Monitor users can view statistics and system logs.

Overview of the CLI

The CLI has the following modes:

- User - When you start a CLI session, you begin in the default, user-mode. From user-mode you can run common network tests such as ping and view network configuration settings and statistics. You do not enter a command to enter user-mode. To exit this mode, enter exit at the command line.
- Enable - To access system monitoring commands, you must enter enable-mode. From enable-mode, you can enter any enable-mode command or enter configuration-mode. You must be an administrator user to enter enable-mode. In enable-mode you can perform basic system administration tasks, such as restarting and rebooting the system. To exit this mode, enter disable at the command line.

  You cannot enter enable-mode if you are a monitor user.
- Configuration - To make changes to the running configuration, you must enter configuration-mode. To save configuration changes to memory, you must enter the write memory command. To enter configuration-mode, you must first be in enable-mode. To exit this mode, enter exit at the command line.

The commands available to you depend on which mode you are in. Entering a question mark (?) at the system prompt provides a list of commands for each command mode.

Mode	Access Method	System Prompt	Exit Method	Description
user	Each CLI session begins in user-mode.	host >	**exit**	• Perform common network tests, such as ping. • Display system settings and statistics.
enable	Enter the **enable** command at the system prompt while in user-mode.	host #	**disable**	• Perform basic system administration tasks, such as restarting and rebooting the system. • Display system data and statistics. • Perform all user-mode commands.
configuration	Enter the **configure terminal** command at the system prompt while in enable-mode.	host (config) #	**exit**	• Configure system parameters. • Perform all user and enable-mode commands.

CLI Cross-Product Support

Many of the CLI commands are applicable to multiple Riverbed products. For example the following Riverbed products use the **enable** command: Steelhead appliance, CMC Appliance, Interceptor appliance, and Steelhead Mobile.

Each CLI command includes the list of products that support it in the Product row.

Note: Many CLI commands that are common across product lines might contain information that is applicable only to the Steelhead appliance.

If you have questions about the usage of a command, contact Riverbed Support.

Entering Commands

The CLI accepts abbreviations for commands. The following example is the abbreviation for the configure terminal command:

```
amnesiac # configure t
```

You can press the tab key to complete a CLI command automatically.

Accessing Online Help

At the system prompt, type the full or partial command string followed by a question mark (**?**). The CLI displays the command keywords or parameters for the command and a short description. You can display help information for each parameter by typing the command, followed by the parameter, followed by a question mark.

To access online help

- At the system prompt enter the following command:

```
amnesiac (config) # show ?
```

- To display help for additional parameters, enter the command and parameter:

```
amnesiac (config) # access ?
enable           Enable secure network access
inbound          Secure access inbound configuration
amnesiac (config) # access inbound ?
rule             Secure access inbound rule configuration
amnesiac (config) # access inbound rule ?
add              Add a secure network access rule
edit             Edit a secure network access rule
move             Move a secure network access rule
```

Error Messages

If at any time the system does not recognize the command or parameter, it displays the following message:

```
amnesiac (config) # logging files enable
% Unrecognized command "enable".
Type "logging files?" for help.
```

If a command is incomplete, the following message is displayed:

```
amnesiac (config) # logging
% Incomplete command.
Type "logging ?" for help.
```

Command Negation

You can type **no** before many of the commands to negate the syntax. Depending on the command or the parameters, command negation disables the feature or returns the parameter to the default value.

Running the Configuration Wizard

You can restart the configuration wizard so that you can change your initial configuration parameters.

To restart the configuration wizard

- Enter the following set of commands at the system prompt:

```
enable
configure terminal
configuration jump-start
```

Saving Configuration Changes

The **show configuration running** command displays the current configuration of the system. When you make a configuration change to the system, the change becomes part of the running configuration.

The change does not automatically become part of the configuration file in memory until you write the file to memory. If you do not save your changes to memory, they are lost when the system restarts.

To save all configuration changes to memory, you must enter the **write memory** command while in configuration-mode.

CHAPTER 2 User-Mode Commands

This chapter is a reference for user-mode commands. It includes the following sections:

- "System Administration Commands" on page 10
- "Displaying System Data" on page 16

User-mode commands allow you to enter enable-mode, display system data, and perform standard networking tasks. Monitor users can perform user-mode commands. All commands available in user-mode are also available to administrator users. For detailed information about monitor and administrator users, see the *Steelhead Appliance Management Console User's Guide*.

To enter user-mode

- Connect to the CLI and enter the following command:

```
login as: admin
Riverbed Steelhead
Last login: Wed Jan 20 13:02:09 2010 from 10.0.1.1
amnesiac >
```

System Administration Commands

This section describes the system administration commands that are available in user-mode.

enable

Description

Enters enable mode.

Syntax

enable

Parameters

None

Usage

You must enter enable mode before you can perform standard network monitoring tasks.

Example

```
amnesiac > enable
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

exit

Description

Exits the CLI when in user mode; exits configuration mode when in configuration mode.

Syntax

exit

Parameters

None

Example

```
amnesiac > exit
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

ping

Description

Executes the ping utility to send ICMP ECHO_REQUEST packets to network hosts using IPv4 addresses, for troubleshooting.

Syntax

ping [<options>]

Parameters

<options>	The **ping** command takes the standard Linux options. For detailed information, see the Linux manual (man) page.

Usage

The **ping** command without any options pings from the primary or the auxiliary (aux) interface and not the in-path interfaces.

If the primary and auxiliary interfaces are not on the same network as the in-path interfaces, you will not be able to ping an IP address on the in-path interface network unless you have a gateway between the two networks.

To ping from an in-path interface, use the following syntax:

```
ping -I <in-path interface IP address> <destination IP address>
```

Example

```
amnesiac > ping -I 10.1.1.1 10.11.22.15
PING 10.11.22.15 (10.11.22.15) from 10.1.1.1: 56(84) bytes of data.
64 bytes from 10.11.22.15: icmp_seq=0 ttl=64 time=0.044 ms
64 bytes from 10.11.22.15: icmp_seq=1 ttl=64 time=0.038 ms
64 bytes from 10.11.22.15: icmp_seq=2 ttl=64 time=0.040 ms
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

ping6

Description

Sends ICMP6_ECHO_REQUEST packets to a network host or gateway using IPv6 addresses, for troubleshooting.

Syntax

ping6 [<options>]

Parameters

<options>	The **ping6** command takes the standard Linux options. For detailed information, see the Linux manual (man) page.

Usage

The **ping6** command without any options pings from the primary or the auxiliary (aux) interface.

Example

```
amnesiac > ping6 fe80::20e:b6ff:fe04:2788 fe80::20e:b6ff:fe02:b5b0

PING fe80::20e:b6ff:fe04:2788(fe80::20e:b6ff:fe04:2788) from fe80::20e:b6ff:fe02:b5b0 primary: 56
data bytes
64 bytes from fe80::20e:b6ff:fe04:2788: icmp_seq=0 ttl=64 time=1.14 ms
64 bytes from fe80::20e:b6ff:fe04:2788: icmp_seq=1 ttl=64 time=0.186 ms
--- fe80::20e:b6ff:fe04:2788 ping statistics ---
2 packets transmitted, 2 received, 0% packet loss, time 1001ms
rtt min/avg/max/mdev = 0.186/0.667/1.148/0.481 ms, pipe 2::0101:B3FF:FE1E:8937
2001:38dc:52::e9a4:c5:1001
```

Product

Steelhead appliance, CSH, CMC

Related Topics

"ipv6 in-path-gateway"

slogin

Description

Enables log in to another system securely using SSH.

Syntax

slogin [<options>]

Parameters

<options>	Specify slogin options. To view options, enter slogin at the system prompt

Example

```
amnesiac > slogin -l usertest
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"show ssh client," "show ssh server"

ssh slogin

Description

Enables log in to another system using ssh.

Syntax

ssh slogin [<slogin options>]

Parameters

<slogin options>	Specify slogin options. To view options, enter slogin at the system prompt.

Example

```
amnesiac > ssh slogin
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"show ssh client," "show ssh server"

stats export

Description

Enables the export of statistics.

Syntax

stats export <csv> <report name> after <yyyy>/<mm>/<dd> before <yyyy>/<mm>/<dd> email <email-addr> filename <filename>

Parameters

<csv>	Specify the file format for export: **csv**
<report name>	Specify one of the following reports: • **cpu_util** - CPU utilization • **memory** - Memory utilization • **paging** - Paging I/O • **appvis-summary** - Application visibility summary report • **appvis-history** - Application visibility history report • **bw** - Aggregate bandwidth • **th_peak** - Peak throughput • **th_p95** - P95 throughput • **pass** - Aggregate pass-through traffic • **cpool** - Aggregate connection pooling • **nfs** - Aggregate NFS report • **pfs** - Aggregate PFS report • **conn_history** - Connection history • **dstore** - Data store hit • **ssl** - SSL statistics • **ssl_peak** - SSL peak statistics • **http** - HTTP statistics • **qos** - QoS statistics • **qos_inbound** - Inbound QoS statistics • **snapmirror** - Snapmirror statistics • **snapmirror_peak** - Snapmirror peak statistics • **top-conversations** - Top conversations report • **top-senders** - Top senders report • **top-receivers** - Top receivers report • **top-applications** - Top applications report
after <yyyy>/<mm>/<dd>	Includes statistics collected after a specific time.
before <yyyy>/<mm>/<dd>	Includes statistics collected before a specific time.
email <email-addr>	Specify the address where the report is to be emailed.
filename <filename>	Specify a filename for the new report.

Example

```
amnesiac > stats export csv ssl after 2008/09/01 filename ssltest
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"show stats bandwidth"

telnet

Description

Enables log in to another system using telnet.

Syntax

telnet [<telnet options>]

Parameters

<telnet options>	Specify telnet command options: • **close** - Close current connection. • **logout** - Forcibly logout remote user and close the connection. • **display** - Display operating parameters. • **mode** - Try to enter line or character mode ('mode ?' for more). • **open** - Connect to a site. • **quit** - Exit telnet. • **send** - Transmit special characters ('send ?' for more). • **set** - Set operating parameters ('set ?' for more). • **unset** - Unset operating parameters ('unset ?' for more). • **status** - Print status information. • **toggle** - Toggle operating parameters ('toggle ?' for more). • **slc** - Change state of special characters ('slc ?' for more). • **z** - Suspend telnet. • **!** - Invoke a subshell. • **environ** - Change environment variables ('environ ?' for more). • **?** - Print help information.

Example

```
amnesiac > telnet
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"show terminal"

terminal

Description

Sets terminal settings.

Syntax

terminal {length <lines> | type <terminal_type> | terminal width <number of characters>}

Parameters

terminal length <lines>	Sets the number of lines 0-1024; 0 to disable paging. The **no** command option disables the terminal length.
[no] terminal type <terminal_type>	Sets the terminal type. The **no** command option disables the terminal type.
terminal width <number of characters>	Sets the width number of characters. The **no** command option disables the terminal width.

Usage

The **no** command option disables terminal settings.

Example

```
amnesiac > terminal width 1024
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"show cli," "show clock," "show terminal"

traceroute

Description

Executes the traceroute utility for IPv4 addresses. The **traceroute** command takes the standard Linux options.

Syntax

traceroute [<options>]

Parameters

<options>	The **traceroute** command takes the standard Linux options. For detailed information, see the Linux manual (man) page.

Example

```
amnesiac > traceroute amnesiac
traceroute to amnesiac.domain.com (10.0.0.3), 30 hops max, 38 byte packets
1 amnesiac (10.0.0.3) 0.035 ms 0.021 ms 0.013 ms
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

traceroute6

Description

Executes the traceroute utility for IPv6 addresses. The **traceroute6** command takes the standard Linux options.

Syntax

traceroute6 [<options>]

Parameters

<options>	The **traceroute6** command takes the standard Linux options. For detailed information, see the Linux manual (man) page.

Example

```
amnesiac > traceroute6 amnesiac
traceroute6 to amnesiac.domain.com (2001:38dc:52::e9a4:c5:6282/64), 30 hops max, 38 byte packets
1 amnesiac (2001:38dc:52::e9a4:c5:6282/64) 0.035 ms 0.021 ms 0.013 ms
```

Product

CMC, Steelhead appliance

Related Topics

"ipv6 in-path-gateway"

Displaying System Data

This section describes the commands to display system data. Monitor users can display non-sensitive system data (for example, data that does not include passwords or user information).

show access inbound rules

Description

Displays secure network access inbound configuration.

Syntax

show access inbound rules

Parameters

None

Example

```
amnesiac > show access inbound rules
Secure network access enabled: no

Rule  A Prot Service/ports Src network        iface     Description
----- - ---- ------------- ------------------ --------- -----------------------
      A tcp  7800          0.0.0.0/0
      A tcp  7801          0.0.0.0/0
      A tcp  7810          0.0.0.0/0
      A tcp  7820          0.0.0.0/0
      A tcp  7850          0.0.0.0/0
      A tcp  ssh           10.0.24.7/32
1     A udp  all           0.0.0.0/0                    Allow DNS lookups
2     A udp  53            0.0.0.0/0                    DNS Caching
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"ACL Management Commands"

show access status

Description

Displays secure network access status.

Syntax

show access status

Parameters

None

Example

```
amnesiac > show access status
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"ACL Management Commands"

show admission

Description

Displays admission control settings, including actual values of current connections and memory usage are displayed.

Syntax

show admission {control | cbad}

Parameters

control	Displays admission control settings.
cbad	Displays the client-based auto-discovery (CBAD) table.

Usage

After performing a model upgrade (for example, upgrading from a 1020 to a 1520), you must reapply admission control overrides relative to the default admission control values of the new model. For assistance with setting admission control overrides, please contact Riverbed Support.

Example

```
amnesiac > show admission control
Enable Admission Control Override Settings: no

  Override Settings:
    Connection Enable:    6000
    Connection Cutoff:    6100
    Memory Enable:        5100 MB
    Memory Cutoff:        5200 MB
    Low Memory Ratio:     96%

  Current Settings:
    Connection Enable:    6000
    Connection Cutoff:    6100
    Memory Enable:        5100 MB
    Memory Cutoff:        5200 MB
    Low Memory Ratio:     96%

  Current State:
    Connections:          0
    Memory:               4042 MB
```

Product

Steelhead appliance

Related Topics

"Configuration File Commands"

show alarm

Description

Displays the status of the specified alarm.

Syntax

show alarm <type>

Parameters

<type>	See the "alarm enable"command for a complete listing and description of alarm types.

Example

```
amnesiac # show alarm warning_temp
Alarm Id: Warning Temperature
Alarm Description: The temperature of the appliance is above normal
Enabled: yes
Alarm State: ok
Error threshold: 70
Clear threshold: 67
Last error at: None
Last clear at: None
```

Product

CMC, Steelhead appliance

Related Topics

"alarm clear," "alarm enable," "show alarms"

show alarms

Description

Displays the status of all alarms. For detailed information about alarms, see the *Steelhead Appliance Management Console User's Guide*.

Syntax

show alarms [triggered]

Parameters

triggered	Displays status and configuration of triggered alarms.

Example

```
amnesiac > show alarms
Alarm Id:          admission_conn
Alarm Description: Steelhead Connection Limit Pressure
Status:            ok
-----------------------------------------
Alarm Id:          admission_control
Alarm Description: Steelhead Admission Control Pressures
Status:            ok
----------------------------------------
Alarm Id:          admission_cpu
Alarm Description: Steelhead CPU Pressure
Status:            ok
----------------------------------------
Alarm Id:          admission_mapi
Alarm Description: Steelhead MAPI Pressure
Status:            ok
----------------------------------------
Alarm Id:          admission_mem
Alarm Description: Steelhead Memory Pressure
Status:            ok
----------------------------------------
Alarm Id:          admission_tcp
Alarm Description: Steelhead TCP Pressure
Status:            ok
----------------------------------------
Alarm Id:          arcount
Alarm Description: Asymmetric Routing
Status:            ok
----------------------------------------
Alarm Id:          block_store
Alarm Description: Blockstore
Status:            ok
----------------------------------------
<<this is a partial listing>>
```

Product

CMC, Steelhead appliance

Related Topics

"alarm clear," "alarm enable," "show alarm"

show authentication policy

Description

Displays the status of the authentication policy.

Syntax

show authentication policy

Parameters

None

Example

```
amnesiac > show authentication policy
Authentication policy enabled:                        yes
Maximum unsuccessful logins before account lockout:   none
      Wait before account unlock:                     300 Seconds
Minimum password length:                              6
Minimum upper case characters in password:            1
Minimum lower case characters in password:            1
Minimum numerical characters in password:             1
Minimum special characters in password:               1
Minimum interval for password reuse:                  5
Minimum characters diff for password change:          4
Prevent dictionary words in password:                 yes
User passwords expire:                                60 days
Warn user of an expiring password:                    7 days before
```

```
User accounts with expired passwords lock:                305 days
```

Product

Steelhead appliance, CMC

Related Topics

"Account Control Management Commands"

show bootvar

Description

Displays the software image that is booted upon the next reboot.

Syntax

show bootvar

Parameters

None

Example

```
amnesiac > show bootvar
Installed images:
Partition 1:
rbtsh/linux columbia #1 2004-02-07 19:24:24 root@test:repository
Partition 2:
rbtsh/linux Columbia #2 2004-02-13 17:30:17 root@test:repository
Last boot partition: 1
Next boot partition: 1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"hardware watchdog enable," "image boot"

show cascade shark

Description

Displays the Cascade Shark status.

Syntax

show cascade shark

Parameters

None

Example

```
amnesiac > show cascade shark
Shark function status: Shark user does not have a password
```

Product

Steelhead appliance

Related Topics

"cascade shark enable," "user shark"

show cli

Description

Displays current CLI settings.

Syntax

show cli

Parameters

None

Example

```
amnesiac > show cli
CLI current session settings
Maximum line size:  8192
Terminal width:     157 columns
Terminal length:    15 rows
Terminal type:      xterm
Auto-logout:        30 minutes
Paging:             enabled
CLI defaults for future sessions
Auto-logout:     30 minutes
Paging:          enabled
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"CLI Terminal Configuration Commands"

show clock

Description

Displays current date and time.

Syntax

show clock [all]

Parameters

all	Displays the system time, date, and ntp peers.

Example

```
amnesiac > show clock
Time: 15:11:13
Date: 2008/10/18
Zone: America North United_States Pacific
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Host Setup Commands"

show cmc

Description

Displays CMC related settings.

Syntax

show cmc

Parameters

None

Example

```
amnesiac > show cmc
CMC auto-registration enabled:       yes
CMC auto-registration hostname:      riverbedcmc.nbttech.com
Managed by CMC:                      yes
CMC hostname:                        tsfe7 (10.02.20.7)
Auto configuration status:           Inactive
Last message sent to cmc:            Auto-registration
Time that message was sent:          Fri Oct 17 09:37:57 2008
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

"Central Management Console Feature Commands"

show connection

Description

Displays information about a single connection.

Syntax

show connection srcip <source ip-addr> srcport <source port> dstip <destination ip-addr> dstport <destination port>

Parameters

srcip <source ip-addr>	Specify the source IP address.
srcport <source port>	Specify the source port.
dstip <destination ip-addr>	Specify the destination IP address.
dstport <destination port>	Specify the destination port.

Example

```
amnesiac > show connection srcip 10.11.62.56 srcport 36433 dstip 10.11.60.9 dstport 7810
Type:                 Passthrough
Source:               10.11.62.56:36433
Destination:          10.11.60.9:7810
Application:
Reduction:            0%
Client Side:          no
Since:                2006/02/21 17:24:00
Peer Appliance:       0.0.0.0:0
Inner Local Port:     0
Outer Local:          0.0.0.0:0
Outer Remote:          0.0.0.0:0
LAN Side Statistics:
Bytes:               0
Packets:             0
Retransmitted:       0
Fast Retransmitted:  0
Timeouts:            0
Congestion Window:   0
WAN Side Statistics:
Bytes:               0
Packets:             0
Retransmitted:       0
Fast Retransmitted:  0
Timeouts:            0
Congestion Window:     0
```

Product

Steelhead appliance

Related Topics

"System Administration and Service Commands"

show connections

Description

Displays the connections running through the appliance.

Syntax

show connections [<type> brief | full | filter <filter-string> | sort-by <state> | path-selection [path-name <path-name>] [full]

Parameters

<type>	**all**	Displays all connection types.
	optimized	Displays the total active connections optimized. A **U** appears next to the appliance name if the connection is in an unknown state.
	passthrough	Displays the total connections passed through, unoptimized. A **U** appears next to the appliance name if the connection is in an unknown state.
	opening	Displays the total half-opened active connections. A half-opened connection is a TCP connection in which the connection has not been fully established. Half-opened connections count toward the connection count-limit on the appliance because at any time they might become fully opened connections. If you are experiencing a large number of half-opened connections, consider deploying an appropriately sized appliance. A **U** appears next to the appliance name if the connection is in an unknown state.
	closing	Displays the total half-closed active connections. A half-closed connection is a TCP connection that closed on one side. The other side of the connection can still send data. These connections count toward the appliance connection count-limit. If you experience a large number of half-closed connections, consider deploying an appropriately sized appliance. A **U** appears next to the appliance name if the connection is in an unknown state.
	discarded	Displays discarded connections only.
	denied	Displays denied connections only.
brief | full	Specify a brief or full report.	
filter <string>	Filters the list according to string. For example, to filter by IP address (such as **srcip** or **destip**); the filter string is the IP address.	
sort-by <state>	Sort results by the following states: • **state -** Sort connections by state. • **srcip** - Sort connections by source IP address. • **srcport** - Sort connections by source port. • **destip** - Sort connections by destination IP address. • **destport** - Sort connections by destination port. • **peerip** - Sort connections by peer IP address. • **peerport** - Sort connections by peer port. • **app** - Sort connections by application, such as HTTP. • **reduction** - Sort connections by percent of reduction in bandwidth. • **bytes_in** - Sort connections by total number of bytes in. • **bytes_out** - Sort connections by total number of bytes out. • **starttime** - Sort connections by start time. • **interface** - Sort connections by interface.	
path-selection [full]	Displays a list of connections using path selection. Specify the **full** option to show a detailed list. Path selection statistics are only reported if path selection is enabled.	
path-selection path-name <path-name> [full]	Displays a list of connections about a specific path name. Specify the **full** option to show a detailed list about the specified path. Path selection statistics are only reported if path selection is enabled.	

Example

```
amnesiac > show connections

T Source                Destination           App  Rdxn Since
```

```
--------------------------------------------------------------------------------
O 10.11.141.1      2842 10.11.141.2       135 EPM  45% 2007/05/02 14:21:59
O 10.11.141.1      2843 10.11.141.2      1025 TCP  16% 2007/05/02 14:22:00
O 10.11.141.3      4765 10.11.141.4      445 CIFS  23% 2007/05/02 14:21:14
O 10.11.141.4      4667 10.11.141.2      445 CIFS   1% 2007/05/02 14:04:40
--------------------------------------------------------------------------------
Established Optimized (O):     4
Half-Opened Optimized (H):     0
Half-Closed Optimized (C):     0
Pass Through (P):              0
Discarded (not shown):         0
Denied    (not shown):         0
--------------------------------
Total:                         4
```

Product

Steelhead appliance

Related Topics

"System Administration and Service Commands," "Path Selection Commands"

show datastore

Description

Displays the current data store settings.

Syntax

show datastore

Parameters

None

Example

```
amnesiac > show datastore
Datastore Wrap-Around Notification:                    no
  Expected Period (days) Before Datastore Wrap-Around: 1

Priority for Deferred Writes:                          yes
Anchor Selection:                                      1
Encryption Type:                                       NONE

Automated Online Datastore Synchronization:            no
  Master:                                              no
  Peer IP Address:                                     0.0.0.0
  Port:                                                7744
  Reconnect Seconds:                                   30
  Connection Status:
  Catch-Up Synchronization Status:
    Catch-Up Percent Completed:
  Keep-Up Synchronization Status:
  Disk Load:
  SDR_A Traffic:
  Hit Rate:
  In-memory-only Hit Rate:
  Hit Count:
  Miss Count:
```

Product

Steelhead appliance

Related Topics

"Data Store Replication and Protection Commands"

show datastore branchwarming

Description

Displays current branch warming settings.

Syntax

show datastore branchwarming

Parameters

None

Example

```
amnesiac > show datastore branchwarming
Branchwarming enabled: yes
```

Product

Steelhead appliance

Related Topics

"Data Store Replication and Protection Commands"

show datastore disk

Description

Displays current data store disk configuration.

Syntax

show datastore disk

Parameters

None

Example

```
amnesiac > show datastore disk
Read Pressure Check Interval: 90
```

Product

Steelhead appliance

Related Topics

"Data Store Replication and Protection Commands"

show datastore disklayout

Description

Displays current data store disk layout status.

Syntax

show datastore disklayout

Parameters

None

Example

```
amnesiac > show datastore disklayout
Datastore disk layout: fifo
```

Product

Steelhead appliance

Related Topics

"Data Store Replication and Protection Commands"

show datastore sdr-policy

Description

Displays data store SDR policy.

Syntax

show datastore sdr-policy

Parameters

None

Example

```
amnesiac > show datastore sdr-policy
datastore sdr policy: default
```

Product

Steelhead appliance

Related Topics

"Data Store Replication and Protection Commands"

show datastore sync

Description

Displays data store disk synchronization status.

Syntax

show datastore sync

Parameters

None

Example

```
amnesiac > show datastore sync
Keepup enabled:   yes
Keepup max pages: 1024
Catchup enabled:  yes
```

Product

Steelhead appliance

Related Topics

"Data Store Replication and Protection Commands"

show datastore write-q-prior

Description

Displays the data store disk write priority setting.

Syntax

show datastore write-q-prior

Parameters

None

Example

```
amnesiac > show datastore write-q-prior
Priority for deferred writes: yes
```

Product

Steelhead appliance

Related Topics

"Data Store Replication and Protection Commands"

show disk state

Description

Displays the disk status.

Syntax

show disk state

Parameters

None

Usage

Use this command to display disk status reports on Steelhead appliance models enabled with Fault Tolerant Storage (FTS).

Example

```
amnesiac > show disk state
CLI> show disk state Disk Status Task
--------------------------------
1 Online Management
2 Online Management
3 Online Data Store
4 Online Data Store
```

Product

Steelhead appliance

Related Topics

"show datastore disk"

show dns cache

Description

Displays the DNS cache settings.

Syntax

show dns cache

Parameters

None

Example

```
amnesiac > show dns cache
Cache size:                1048576 bytes
Minimum cache TTL:         0 seconds
Maximum cache TTL:         604800 seconds
Minimum ncache TTL:        0 seconds
Maximum ncache TTL:        10800 seconds
Cache frozen:              no
```

Product

Steelhead appliance

Related Topics

"DNS Cache Commands"

show dns forwarders

Description

Displays a list of all the forwarders.

Syntax

show dns forwarders

Parameters

None

Example

```
amnesiac > show dns forwarders
```

Product

Steelhead appliance

Related Topics

"DNS Cache Commands"

show dns interfaces

Description

Displays a list of all the interfaces.

Syntax

show dns interfaces

Parameters

None

Example

```
amnesiac > show dns interfaces
```

Product

Steelhead appliance

Related Topics

"DNS Cache Commands"

show dns settings

Description

Displays the DNS settings.

Syntax

show dns settings

Parameters

None

Example

```
amnesiac > show dns settings
DNS:                                 running
Fallback to root nameservers:        yes
Detect down forwarders:              no
Time till forwarder is down:          120 seconds
Lost requests till forwarder is down: 30
Time for forwarder to stay down:     300 seconds
```

Product

Steelhead appliance

Related Topics

"DNS Cache Commands"

show domain

Description

Displays the domain settings.

Syntax

show domain {configuration | settings | status}

Parameters

configuration	Displays domain configuration.
settings	Displays domain settings.
status	Displays domain status.

Example

```
amnesiac > show domain configuration
Domain Name                  : GEN-VCS276.DOMAIN.TEST
Short Domain Name            : GEN-VCS2760
Login                        : Administrator
Domain Controller List       : gen-vcs276
Domain Required              : yes
Domain Check Required        : no
Domain Join Type             : win2k8-mode
```

Product

Steelhead appliance

Related Topics

"DNS Cache Commands"

show email

Description

Displays the current email settings.

Syntax

show email

Parameters

None

Example

```
amnesiac > show email
Mail hub:       exchange
Mail hub port:  30
Domain:         example.com
Event emails
  Enabled: yes
  Recipients:
    example@riverbed.com
Failure emails
  Enabled: yes
  Recipients:
    example@riverbed.com
Autosupport emails
  Enabled: no
  Recipient:
    autosupport@eng.riverbed.com
  Mail hub:
    eng.riverbed.com
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Notification Commands"

show failover

Description

Displays the current failover device settings.

Syntax

show failover

Parameters

None

Example

```
amnesiac > show failover
Enabled:          no
```

```
Master:            yes
Local Port:        7220
Buddy IP Address: 0.0.0.0
Buddy Port:        7220
```

Product

Interceptor appliance, Steelhead appliance

Related Topics

"Data Store Replication and Protection Commands"

show flash images

Description

Displays the RiOS images stored in flash memory.

Syntax

show flash images

Parameters

None

Example

```
amnesiac > show flash images
Flash Image 1: rbt_sh 6.5.0-prealpha #46 2010-10-04 15:19:58 x86_64 root@bratisl
ava:svn://svn/mgmt/trunk
      Flash support: yes
```

Product

Interceptor appliance, Steelhead appliance containing flash memory.

Related Topics

"write flash"

show flow

Description

Displays detailed information for a single flow.

Syntax

show flow srcip <source ip-addr> srcport <source port> dstip <destination ip-addr> dstport <destination port> [protocol <protocol-name>]

Parameters

srcip <source ip-addr>	Specify the source IP address.
srcport <source port>	Specify the source port.
dstip <destination ip-addr>	Specify the destination IP address.
dstport <destination port>	Specify the destination port.
protocol <protocol-name>	Specify the protocol to display information about within the flow.

Example

```
amnesiac > show flow srcip 10.12.1.37 srcport 52092 dstip 10.12.9.164 dstport 7680 protocol TCPv4
```

```
Type:                           Dedicated
Optimization Policy:            SDR, LZ
Source:                         10.12.1.37:52092
Destination:                    10.12.9.164:7680

Protocol:                       TCPv4
Reduction:                      98%
Since:                          2013/01/14 17:39:14

Peer Appliance:                 10.12.3.84:7810
Inner:                          10.12.0.201:40269

Statistics:
  Bytes received:               3629131688
  Bytes sent:                   48531166
  Packets sent:                 193545
  Retransmitted:                0
  Fast Retransmitted:           0
  Timeouts:                     0
  Congestion Window:            8
```

Product

Steelhead appliance

Related Topics

"show flows"

show flows

Description

Displays a list of flows.

Syntax

show flows [all [<sub-type>]| packet-mode <sub-type> | tcp-term <sub-type>] [filter <filter-string>] [sort-by <state>] [brief | debug| full]

Parameters

all	Displays information about all flow types.	
<sub-type>	**destip <ip-addr>**	Optionally, displays a list of flows filtered by destination IP address.
	destport <port>	Optionally, displays a list of flows filtered by destination port.
	path-selection [path-name <path-name>] [full]	Optionally, displays the list of all flows or the flows filtered by path name using path selection. The **full** option displays detailed information about the flows using path selection. Path selection statistics are only reported if path selection is enabled.
	srcip <ip-addr>	Optionally, displays a list of flows filtered by source IP address.
	srcport <port?	Optionally, displays a list of flows filtered by source port.
packet-mode	Displays information about packet-mode optimized flows.	
<sub-type>	**optimized**	Displays the total active optimized flows.
	passthrough	Displays the total flows passed through unoptimized.
	srcip <ip-addr>	Displays a list of flows filtered by source IP address.
tcp-term	Displays a list of terminated TCP optimized flows.	
<sub-type>	**optimized**	Displays the total active optimized flows.
	passthrough	Displays the total flows passed through unoptimized.
	opening	Displays the total half-opened active connections. A half-opened connection is a TCP connection in which the connection has not been fully established. Half-opened connections count toward the connection count limit on the appliance because at any time they might become fully opened connections. If you are experiencing a large number of half-opened connections, consider deploying an appropriately sized appliance.
	closing	Displays the total half-closed active connections. A half-closed connection is a TCP connection that closed on one side. The other side of the connection can still send data. These connections count toward the appliance connection count limit. If you experience a large number of half-closed connections, consider deploying an appropriately sized appliance.
	srcip <ip-addr>	Displays a list of flows filtered by source IP address.
	path-selection [path-name <path-name>] [full]	Optionally, displays the list of all flows or the flows filtered by path name using path selection. The **full** option displays detailed information about the flows using path selection. Path selection statistics are only reported if path selection is enabled.
filter <string>	Filters the list according to the string. For example, to filter by IP address (such as **srcip** or **destip**), the filter string is the IP address.	

sort-by <state>	Sort results by the following states: • **state -** Sort connections by state. • **srcip** - Sort connections by source IP address. • **srcport** - Sort connections by source port. • **destip** - Sort connections by destination IP address. • **destport** - Sort connections by destination port. • **peerip** - Sort connections by peer IP address. • **peerport** - Sort connections by peer port. • **protocol -** Sort connections by protocol. • **reduction** - Sort connections by percent of reduction in bandwidth. • **bytes_in** - Sort connections by total number of bytes in. • **bytes_out** - Sort connections by total number of bytes out. • **starttime** - Sort connections by start time.
brief | debug | full	Specify a brief flow list, debug information with each flow, or full details on each flow.

Usage

When packet-mode optimization is enabled, use the **show flows** command to view packet-mode optimization flow information. Path selection statistics are only reported if path selection is enabled.

Example

```
amnesiac > show flows

T  Source                Destination           App     Rdn Since
--------------------------------------------------------------------------------
N  10.190.0.1:406        10.190.5.2:1003       UDPv4   99% 2011/04/30 23:58:01
O  192.168.0.1:80        192.168.5.79:52912    NAGLE   11% 2011/05/01 00:00:01
O  192.168.221.1:1080    192.168.221.1:1080    CIFS     0% 2011/05/01 00:20:01
O  192.168.221.1:443     192.168.221.1:443     MAPI    99% 2011/05/01 00:21:01
N  [abcd:a:b:c:d:1:1:1]:1009
                         [1bcd:a:b:c:d:2:21:12]:508
                                               TCPv6   99% 2011/05/01 00:00:01
O  [eedc:ba98:54::3210]:34870
                         [eedc:ba98:7011:3221:1111:1120:201:2021]:443
                                               MAPI    97% 2011/05/01 00:21:01
0  [eedc:ba98:765::1]34870
                         [eedc:ba98:54::3210]:443
                                               MAPI    97% 2011/05/01 00:21:01
0  [eedc:ba98:7011:3221:1111:1120:201:2001]:34870
                         [eedc:ba98:7011:3221:1111:1120:201:2001]:443
                                               MAPI    97% 2011/05/01 00:21:01
O  [eedc:ba98:7011:3221:1111:1120:201:2021]:34870
                         [eedc:ba98:54::3210]:443
                                               MAPI    97% 2011/05/01 00:21:01
N  [fbcd::1:1]:12        [5bcd::2:2]:102       TCPv6   99% 2011/04/30 23:56:01
N  [fbcd::1:1]:12        [5bcd::2:2]:103       TCPv6   99% 2011/05/01 00:00:01

--------------------------------------------------------------------------------
                                           All    V4     V6
---------------------------------------------------------------
Established Optimized:                     11     4      7
  RiOS Only (O):                           7      3      4
  SCPS Only (SO):                          0      0      0
  RiOS+SCPS (RS):                          0      0      0
  TCP Proxy (TP):                          0      0      0
  Packet-mode optimized (N):                 4      1      3
Half-opened optimized (H):                   0      0      0
Half-closed optimized (C):                   0      0      0
Establishing:                                0      0      0
Passthrough (unoptimized):                   1      1      0
  Passthrough intentional(PI):               0      0      0
  Passthrough unintentional (PU):            0      0      0
    Terminated:                              0      0      0(
    Packet-mode:                             0      0      0
Forwarded (F):                               0      0      0
Discarded(terminated):                       0
Denied (terminated):                         0
---------------------------------------------------------------
Total:                                       11     4      7
```

Product

Steelhead appliance

Related Topics

"packet-mode enable,""show flow," "Path Selection Commands"

show hardware error-log

Description

Displays IPMI system event log entries.

Syntax

show hardware error-log {all | new}

Parameters

all	Displays all IPMI SEL entries
new	Display IPMI SEL entries since the last **show hardware error-log** command was issued.

Example

```
amnesiac > show hardware error-log all
1 | 11/28/2006 11:55:10 | Event Logging Disabled SEL | Log area reset/cleared |
Asserted = yes.
2 | 01/04/2007 21:09:07 | Slot/Connector Drive | Fault Status | Asserted = yes.
3 | 01/07/2007 03:24:07 | Slot/Connector Drive | Fault Status | Asserted = yes.
```

Product

CMC Appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"clear hardware error-log"

show hardware nic slots

Description

Displays network interface slot information.

Syntax

show hardware nic slots

Parameters

None

Example

```
amnesiac # show hardware nic slots
Slot Current Mode (Configured)
---- -------------------------
2    inpath (inpath)
0    inpath (inpath)
```

Product

Granite Edge-enabled Steelhead EX appliance

Related Topics

"hardware nic slot"

---

show hardware spec

Description

Displays the hardware specifications that are available for the platform. Includes an indicator that displays what model specification is active and which specifications are available.

Syntax

show hardware spec

Parameters

None

Example

```
amnesiac > show hardware spec
Spec Description
- ---- -------------------------------------
  50   BW Limit: 256 KB/s       Connection Limit: 250
* 100  BW Limit: 1000 KB/s      Connection Limit: 30
  200  BW Limit: 1000 KB/s      Connection Limit: 110
        (unavailable)
  300  BW Limit: 2000 KB/s      Connection Limit: 165
         (unavailable)
* = active
```

Product

Steelhead appliance

Related Topics

"clear hardware error-log"

---

show history

Description

Displays event history.

Syntax

show history [category <category>] [severity <level>]

Parameters

category <category>	Displays event history for the specified event category: • **alarm** • **cli** • **config** • **mgmt** • **web**
severity <level>	Displays the minimum syslog severity threshold for the event category: • **emer** - System unusable • **alert -** Immediate action • **crit** - Critical conditions • **err** - Error conditions • **warning** - Warning conditions • **notice** - Normal but significant condition • **info** - Informational messages • **debug -** Debug-level messages

Usage

Alarms leave no record other than the message log, which is unstructured and not always helpful. Use the **show history** command to help diagnose problems by viewing the event history (an alarm is an example of an event). Other examples of events include a login or a configuration change. An event history displays all events at a glance, allows for the search of alarms according to several criteria, and puts the alarms in the context of other time-based statistical information.

Example

```
amnesiac > show history
Enable: yes
Last Ping:  2013-02-12 14:31:49.412973153 -0700
Saved Ping:  2013-03-21 07:25:51.000000000 -0700
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Alarm Commands"

show hardware watchdog

Description

Displays hardware watchdog information.

Syntax

show hardware watchdog

Parameters

None

Example

```
amnesiac > show hardware watchdog
Enable: yes
Last Ping:  2006-05-12 14:31:49.412973153 -0700
Saved Ping:  2006-04-21 07:25:51.000000000 -0700
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"hardware watchdog enable"

show hosts

Description

Displays system hosts.

Syntax

show hosts

Parameters

None

Example

```
amnesiac > show hosts
Hostname: amnesiac
Name server: 10.0.0.2 (configured)
Domain name: domain.com (configured)
Domain name: domain.com (configured)
IP 107.0.0.1 maps to hostname localhost
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Host Setup Commands"

show host-label

Description

Displays information about the specified host label.

Syntax

show host-label <name> [detailed]

Parameters

<name>	Specify the name of the host label.
detailed	Displays detailed hostname and subnet status information.

Example

```
amnesiac # show host-label test
10.0.0.0/8, 192.168.0.1/32, 192.168.0.2/32, example.com, riverbed.com

amnesiac # show host-label test detailed

Subnets:
10.0.0.0/8, 192.168.0.1/32, 192.168.0.2/32

Host example.com:
192.0.43.10/32
Resolved: 2013/03/12 18:54:14
```

```
Host riverbed.com:
192.0.43.10/32
Resolved: 2013/03/12 18:54:14

Next scheduled resolve: 2013/03/13 18:54:09
```

Product

CMC, Steelhead appliance

Related Topics

"Host Label Commands"

show images

Description

Displays the available software images and which partition the appliance boots the next time the appliance is restarted.

Syntax

show images [checksum]

Parameters

checksum	Displays the Message-Digest 5 algorithm (MD5) checksum of the system images.

Example

```
amnesiac > show images
Images available to be installed:
webimage.tbz
rbtsh/linux 4.0 #12 2007-05-15 11:54:52 root@test:CVS_TMS/HEAD
image.img
rbtsh/linux 4.0 #17 2007-05-22 16:39:32 root@test:CVS_TMS/HEAD
Installed images:
Partition 1:
rbtsh/linux 4.0-HEAD-2007-06-15-07:19:19 #0 2007-06-15 07:19:19 root@test:CVS_TMS/HEAD
Partition 2:
rbtsh/linux 4.0 2007-05-15 11:54:52 root@test:CVS_TMS/HEAD
Last boot partition: 2
Next boot partition: 2
```

Product

CMC Appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"License and Hardware Upgrade Commands"

show info

Description

Displays the system information, including the current state of the system.

Syntax

show info

Parameters

None

Example

```
amnesiac > show info
Status:            Healthy
Config:            working
Appliance Up Time: 15d 1h 14m 4s
Service Up Time:   15d 1h 12m 25s
Serial:            H180000697a
Model:             8800
Revision:          A
Version:           spitfire-1.0
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

"show connection"

show in-path

Description

Displays in-path interface settings.

Syntax

show in-path

Parameters

None

Example

```
amnesiac > show in-path
Enabled: yes
Kickoff: no
L4/PBR/WCCP: no
Main Interface: inpath1_0
Optimizations Enabled On:
  inpath1_0
VLAN Tag IDs:
  inpath1_0: 0
  inpath1_1: 0
```

Product

Steelhead appliance

Related Topics

"In-Path and Virtual In-Path Support Commands"

show in-path ar-circbuf

Description

Displays the asymmetric routing table.

Syntax

show in-path ar-circbuf

Parameters

None

Example

```
amnesiac > show in-path ar-circbuf
```

Product

Steelhead appliance

Related Topics

"Asymmetric Route Detection Commands"

show in-path asym-route-tab

Description

Displays the asymmetric route table. The table contains any asymmetric routes that currently exist. It includes the source IP, destination IP, reason code, and time-out.

Syntax

show in-path asym-route-tab

Parameters

None

Usage

The following types of asymmetry are displayed in the asymmetric routing table:

- **bad RST** - Complete Asymmetry: packets traverse both Steelhead appliances going from client to server but bypass both Steelhead appliances on the return path.
- **bad SYN/ACK** - Server-Side Asymmetry: Packets traverse both Steelhead appliances going from client to server but bypass the server-side Steelhead appliance on the return path.
- **no SYN/ACK** - Client-Side Asymmetry: Packets traverse both Steelhead appliances going from client to server but bypass the client-side Steelhead appliance on the return path.
- **probe-filtered (not-AR)** - Probe-Filtered: Occurs when the client-side Steelhead appliance sends out multiple SYN+ frames and does not get a response.
- **probe-filtered (not-AR)** - SYN-Rexmit: Occurs when the client-side Steelhead appliance receives multiple SYN retransmits from a client and does not see a SYN/ACK packet from the destination server.

Example

```
amnesiac > show in-path asym-route-tab
Format: [IP 1] [IP 2] [reason] [timeout(
10.111.111.19 10.111.25.23 no-SYNACK 770
```

Product

Steelhead appliance

Related Topics

"Asymmetric Route Detection Commands"

show in-path cdp

Description

Displays Cisco Discovery Protocol (CDP) settings for failover deployments using PBR to redirect traffic to the backup appliance.

Syntax

show in-path cdp

Parameters

None

Example

```
amnesiac > show in-path cdp
CDP Enabled: no
Interval: 10 seconds
Hold Time: 180 seconds
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

"Asymmetric Route Detection Commands"

show in-path cf-timer

Description

Displays connection forwarding timer settings.

Syntax

show in-path cf-timer

Parameters

None

Example

```
amnesiac > show in-path cf-timer
ACK Timer Count:        3
ACK Timer Interval:     1000
Read Timeout:           10000
Reconnect Timeout:      10000
```

Product

Steelhead appliance

Related Topics

"Asymmetric Route Detection Commands"

show in-path drop-when-flap

Description

Displays dropped packets if the system detects route flapping.

Syntax

show in-path drop-when-flap

Parameters

None

Usage

Route flapping occurs when a router alternately advertises a destination network through one route then another (or as unavailable, and then available again) in quick sequence.

Example

```
amnesiac > show in-path drop-when-flap
```

```
Drop packets on flap: no
```

Product

Steelhead appliance

Related Topics

"Asymmetric Route Detection Commands"

show in-path hw-assist rules

Description

Displays the hardware assist rules.

Syntax

show in-path hw-assist rules

Parameters

None

Example

```
amnesiac >  show in-path hw-assist rules
Hardware passthrough UDP packets on 10G: no
Hardware passthrough TCP packets on 10G: no

Hardware assist rules for TCP traffic:
#   Action        Subnet-A          Subnet-B          VLAN
--- ------------- ----------------- ----------------- -----------
1   Accept        all               all               all
       Desc: wibble

def Accept        all               all               all
-------------------------------------------------------------------------------
1 user added rule(s)
```

Usage

On Steelhead appliance and Interceptor appliances equipped with one or more Two-Port SR Multimode Fiber 10 Gigabit-Ethernet PCI-E or Two-Port LR Single Mode Fiber 10 Gigabit-Ethernet PCI-E cards, you can configure the system to automatically bypass all UDP (User Datagram Protocol) connections.

You can also configure rules for bypassing specific TCP (Transmission Control Protocol) connections. By automatically bypassing these connections, you can decrease the work load on the local Steelhead appliances.

If the system is not equipped with the necessary card, an error message displays.

Product

Interceptor appliance, Steelhead appliance

Related Topics

"in-path hw-assist rule", "in-path hw-assist edit-rule", "in-path hw-assist move-rule rulenum"

show in-path lsp

Description

Displays whether link state propagation is enabled. When LSP is enabled, if the LAN interface drops the link then the WAN also drops the link.

Syntax

show in-path lsp

Parameters

None

Example

```
amnesiac > show in-path lsp
Link State Propagation Enabled: no
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

"in-path lsp enable"

show in-path mac-except-locl

Description

Displays whether non-local peer Steelhead appliance MAC has been configured for simplified routing. For detailed information, see the *Steelhead Appliance Deployment Guide*.

Syntax

show in-path mac-except-locl

Parameters

None

Example

```
amnesiac > show in-path mac-except-locl
Disallow non-local peer SH MAC for SR: yes
```

Product

Steelhead appliance

Related Topics

"WAN Visibility (Transparency) Commands"

show in-path mac-match-vlan

Description

Displays in-path settings if VLAN IDs are used in simplified routing table look ups for WAN visibility. For detailed information, see the *Steelhead Appliance Deployment Guide*.

Syntax

show in-path mac-match-vlan

Parameters

None

Example

```
amnesiac > show in-path mac-match-vlan
Use VLAN IDs in simplified routing table lookups: no
```

Product

Steelhead appliance

Related Topics

"WAN Visibility (Transparency) Commands"

show in-path macmap-except

Description

Displays the MAC map exception table.

Syntax

show in-path macmap-except

Parameters

None

Example

```
amnesiac > show in-path macmap-except
00:0e:b6:84:11:16 10.10.10.255
```

Product

Steelhead appliance

Related Topics

"WAN Visibility (Transparency) Commands"

show in-path macmap-tables

Description

Displays the MAC-map tables for WAN visibility. For detailed information, see the *Steelhead Appliance Deployment Guide*.

Syntax

show in-path macmap-tables

Parameters

None

Example

```
amnesiac > show in-path macmap-tables
```

Product

Steelhead appliance

Related Topics

"WAN Visibility (Transparency) Commands"

show in-path neighbor

Description

Displays connection forwarding settings. For detailed information about connection forwarding alarms, see the *Steelhead Appliance Management Console User's Guide*.

Syntax

show in-path neighbor

Parameters

None

Example

```
amnesiac > show in-path neighbor
In-path Neighbor Enabled:   no
In-path Neighbor Port:      7850
Keepalive Count:            3
Keepalive Interval:         1
Allow Failure:              no
Advertise Resync:           yes

Use the VLAN & destination
MAC address as forwarded
by the neighbor:            no

Multi-interface support:
  Enabled:                  no

 Neighbor Name         Main Address     Port
 --------------------  ---------------  -----
 No neighbors.
```

Product

Steelhead appliance

Related Topics

"Asymmetric Route Detection Commands," "Connection Forwarding"

show in-path neighbor-detail

Description

Displays connection forwarding settings. For detailed information, see the *Steelhead Appliance Management Console User's Guide*.

Syntax

show in-path neighbor-detail

Parameters

None

Example

```
amnesiac > show in-path neighbor-detail
Neighbor 1 : 172.1.34.4
State                        : Reading message header
NAT requests sent            : 64
NAT DEL messages sent        : 64
NAT ACKs received            : 64
NAT requests received        : 0
NAT DEL messages received    : 0
NAT ACKs sent                : 0
DYN requests sent            : 0
DYN DEL messages sent        : 0
DYN ACKs received            : 0
DYN requests received        : 0
DYN DEL messages received    : 0
DYN ACKs sent                : 0
REDIR requests sent          : 64
REDIR DEL messages sent      : 64
REDIR ACKs received          : 64
REDIR requests received      : 0
REDIR DEL messages received : 0
REDIR ACKs sent              : 0
```

```
Connection failures          : 0
Keepalive timeouts           : 0
Request timeouts             : 0
Max latency seen             : 26 ms
```

Product

Steelhead appliance

Related Topics

"Asymmetric Route Detection Commands," "Connection Forwarding"

show in-path neighbor advertiseresync

Description

Displays advertisements on synchronize settings.

Syntax

show in-path neighbor advertiseresync

Parameters

None

Example

```
amnesiac > show in-path neighbor advertiseresync
Advertise Resync: yes
```

Product

Steelhead appliance

Related Topics

"Asymmetric Route Detection Commands,"

show in-path peer-probe-cach

Description

Displays the peer probe cache.

Syntax

show in-path peer-probe-cach

Parameters

None

Example

```
amnesiac > show in-path peer-probe-cach
Peer probe cache: no
```

Product

Steelhead appliance

Related Topics

"in-path peer-probe-cach"

show in-path peering auto

Description

Displays whether or not automatic in-path peer (Enhanced Auto-Discovery) detection is enabled.

Syntax

show in-path peering auto

Parameters

None

Example

```
amnesiac > show in-path peering auto
Enhanced Auto-Discovery Enabled:   yes
```

Product

Steelhead appliance

Related Topics

"in-path peering auto"

show in-path peering disc-outer-acpt

Description

Displays outer connection for the accept rules.

Syntax

show in-path peering disc-outer-acpt

Parameters

None

Example

```
amnesiac > show in-path peering disc-outer-acpt
```

Product

Steelhead appliance

Related Topics

"in-path peering rule"

show in-path peering rules

Description

Displays in-path peering rules.

Syntax

show in-path peering rules

Parameters

None

Example

```
amnesiac > show in-path peering rules
```

```
Rule Type   Source Network     Dest Network       Port Peer Addr
----- ------ ------------------ ------------------ ----- -------------
    1 pass   *                  *                  *     10.0.1.3
    2 pass   *                  *                  *     10.0.1.
    def auto *                  *                  *     *
```

Product

Steelhead appliance

Related Topics

"in-path peering rule"

show in-path peering oobtransparency

Description

Displays out-of-band transparency settings.

Syntax

show in-path peering oobtransparency

Parameters

None

Example

```
amnesiac > show in-path peering oobtransparency
Mode:   none
Port:   708
```

Product

Steelhead appliance

Related Topics

"WAN Visibility (Transparency) Commands", "in-path peering oobtransparency mode"

show in-path probe-caching

Description

Displays probe caching settings for WAN visibility. For detailed information, see the *Steelhead Appliance Deployment Guide*.

Syntax

show in-path probe-caching

Parameters

None

Example

```
amnesiac > show in-path probe-caching
Probe Caching Enabled: no
```

Product

Steelhead appliance

Related Topics

"WAN Visibility (Transparency) Commands"

show in-path probe-ftp-data

Description

Displays whether or not FTP connections are probed to learn VLAN information. For detailed information, see the *Steelhead Appliance Deployment Guide*.

Syntax

show in-path probe-ftp-data

Parameters

None

Example

```
amnesiac > show in-path probe-ftp-data
Probe FTP connections to learn VLAN info: no
```

Product

Steelhead appliance

Related Topics

"in-path probe-ftp-data"

show in-path probe-mapi-data

Description

Displayswhether or not MAPI data connections are probed to learn VLAN information. For detailed information, see the *Steelhead Appliance Deployment Guide*.

Syntax

show in-path probe-mapi-data

Parameters

None

Example

```
amnesiac > show in-path probe-mapi-data
Probe MAPI connections to learn VLAN info: no
```

Product

Steelhead appliance

Related Topics

"in-path simplified routing"

show in-path rules

Description

Displays current in-path rules and VLAN identification numbers.

Syntax

show in-path rules

Parameters

None

Example - Steelhead appliance

```
amnesiac > show in-path rules
 Rule Type P O L N W K VLAN Source Addr        Dest Addr          Port
----- ---- - - - - - - ---- ------------------ ------------------ ---------------
    1 pass - - - - - - all  all                all                Secure
    2 pass - - - - - - all  all                all                Interactive
    3 pass - - - - - - all  all                all                RBT-Proto
  def auto N F F A C N all  all                all                all

3 user-defined rule(s)

(P) Preoptimization Policy: O=Oracle-Forms S=SSL +=Oracle-Forms-over-SSL N=None
(O) Optimization Policy:    F=Full S=SDR-only C=Compression-only M=SDR-M N=None
(L) Latency Optimizations:  F=Full H=HTTP-only N=None
(N) Neural Framing:         A=Always D=Dynamic T=TCP hints N=Never
(W) WAN Visibility Mode:    C=Correct-Addressing
                            P=Port-Transparency
                            F=Full-Transparency
                            R=Full-Transparency w/Reset
(K) Auto Kickoff:           Y=Enabled
                            N=Disabled
```

Product

Interceptor appliance, Steelhead appliance

Related Topics

"In-Path and Virtual In-Path Support Commands"

show in-path send-storeid

Description

Displays the send-store ID setting.

Syntax

show in-path send-storeid

Parameters

None

Example

```
amnesiac > show in-path send-storeid
Send Storeid: no
```

Product

Steelhead appliance

Related Topics

"in-path send-storeid enable"

show in-path simplified routing

Description

Displays simplified routing settings.

Syntax

show in-path simplified routing

Parameters

None

Example

```
amnesiac > show in-path simplified routing
Collect mappings from destination MAC data: no
Collect mappings from source MAC data:      no
Collect data from un-natted connections:    no
```

Product

Steelhead appliance

Related Topics

"Simplified Routing Support Commands"

show in-path vlan-conn-based

Description

Displays if VLAN connection based mapping is in use. For detailed information, see the *Steelhead Appliance Deployment Guide*.

Syntax

show in-path vlan-conn-based

Parameters

None

Example

```
amnesiac > show in-path vlan-conn-based
```

Product

Steelhead appliance

Related Topics

"WAN Visibility (Transparency) Commands"

show ip

Description

Displays the IP settings.

Syntax

show ip {flow-export <cr> | destination <ip-addr> port <port> <cr> | filter <cr>| [flow-setting <cr> | lan-subnets] | [in-path route <interface> <cr> | static]| [in-path-gateway <interface> <cr> | static] | [security <cr> | peers]}

Parameters

flow-export <cr> | destination <ip-addr> port <port> <cr> | filter <cr>	Displays NetFlow export settings.
flow-setting <cr> | lan-subnets	Displays NetFlow settings. Optionally, display LAN subnets.
in-path route <interface> <cr> | static	Displays in-path route settings for interfaces, such as **inpath0_0**, and **inpath1_1**.
in-path-gateway <interface> <cr> | static	Displays in-path gateway settings for interfaces, such as **inpath0_0**, and **inpath1_1**.
security <cr> | peers	Displays IPSec connections to other appliances.

Example

```
amnesiac > show ip flow-setting
Configured active flow timeout:  1800
In-use active flow timeout:      1800
Inactive flow timeout:           15

The in-use active flow timeout can be different from the
configured active flow timeout when Top Talkers is enabled.
amnesiac-sh75 > show ip flow-setting
Configured active flow timeout:  1800
In-use active flow timeout:      1800
Inactive flow timeout:           15

The in-use active flow timeout can be different from the
configured active flow timeout when Top Talkers is enabled.
```

Product

Interceptor appliance, Steelhead appliance

Related Topics

"Data Flow Support Commands,""Host Setup Commands"

show legacy-rsp

Description

Displays RSP v5.0.x information.

Syntax

show legacy-rsp

Parameters

None

Example

```
amnesiac > show legacy-rsp
Present and reserving 12288 bytes from PFS store
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show limit bandwidth

Description

Displays bandwidth limit settings.

Syntax

show limit bandwidth

Parameters

None

Example

```
amnesiac > show limit bandwidth
Max rate:  10000 kb/s
Max burst: 750000 bytes
```

Product

Steelhead appliance

Related Topics

"Host Setup Commands"

show limit connection

Description

Displays the connection limit setting.

Syntax

show limit connection

Parameters

None

Example

```
amnesiac > show limit connection
Per source IP connection limit: 4096
```

Product

Steelhead appliance

Related Topics

"Host Setup Commands"

show logging

Description

Displays logging and logging filter settings.

Syntax

show logging [filter]

Parameters

filter	Displays per-process logging configuration information.

Example

```
amnesiac > show logging filter
Local logging level: info
amnesiac > show logging
Local logging level: info
Default remote logging level: notice
Remote syslog receiver: 10.10.10.2 (logging level: info)
Number of archived log files to keep: 10
Log rotation frequency: daily
```

Product

CMC, Steelhead appliance, Interceptor appliance

Related Topics

"Logging Commands"

show nettest

Description

Displays network health test results.

Syntax

show nettest {cable-swap | duplex | ip-port-reach | net-gateway | peer-reach}

Parameters

cable-swap	Displays the results of the cable swap test. If the test fails, ensure you are not using a straight-through cable between an appliance port and a router, or a crossover cable between an appliance port and a switch.
duplex	Displays the results of the duplex matching test. If one side is different from the other, then traffic is sent at different rates on each side, causing a great deal of collision.
ip-port-reach	Displays the results of the IP port reachability test.
net-gateway	Displays the results of the network gateway test.
peer-reach	Displays the results of the peer reachability test.

Example

```
amnesiac > show nettest net-gateway
Gateway Test                  Last Run: 2009/08/16 09:43:32
Passed

Interface       Address         Packet Loss     Result
======================================================
Default         10.0.0.1        0%              Passed
amnesiac-sh75 (config) # show nettest net-gateway
Gateway Test                  Last Run: 2009/08/16 09:43:32
Passed

Interface       Address         Packet Loss     Result
======================================================
Default         10.0.0.1        0%              Passed
```

Product

Steelhead appliance

Related Topics

“Network Test Commands”

show ntp

Description

Displays NTP settings.

Syntax

show ntp [all]

Parameters

all	Display NTP settings and active peers.

Example

```
amnesiac > show ntp
NTP enabled: yes
No NTP peers configured.
NTP server: 190.6.38.127 (version 4)
NTP server: 46.187.224.4 (version 4)
NTP server: 46.187.233.4 (version 4)

amnesiac > show ntp all
NTP enabled: yes

NTP peers:
chief-sh158 (version 4) Enabled: yes Key: 10

NTP servers:
0.riverbed.pool.ntp.org (version 4)     Enabled: yes
1.riverbed.pool.ntp.org (version 4)     Enabled: yes
2.riverbed.pool.ntp.org (version 4)     Enabled: yes
208.70.196.25 (version 4)       Enabled: yes
3.riverbed.pool.ntp.org (version 4)     Enabled: yes Key: 11

     remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
-tick.tadatv.com 10.0.22.49       2 u  874 1024  377    5.810   11.252  13.031
*wwwco1test12.mi 64.236.96.53     2 u  817 1024  377   83.799    1.636  52.182
-thor.netservice 64.113.32.5      2 u  865 1024  377   75.838   -4.941   6.927
+ftp1.riverbed.c 10.16.0.15       3 u  839 1024  377    1.740    2.610   6.121
-4.53.160.75     220.183.68.66    2 u  820 1024  377   48.183    8.513   1.116
+chief-sh158.lab 108.59.14.130    3 u  127 1024  373    1.560    5.737  13.369

     remote       conf  auth  key
===================================
tick.tadatv.com   yes   ok    12
wwwco1test12.mi   yes   none  none
thor.netservice   yes   none  none
ftp1.riverbed.c   yes   none  none
4.53.160.75       yes   ok    11
chief-sh158.lab   yes   ok    10
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"Host Setup Commands"

show ntp active-peers

Description

Displays active NTP peers.

Syntax

show ntp active-peers

Parameters

None

Example

```
amnesiac > show ntp active-peers

remote           refid      st t when poll reach   delay   offset  jitter
==============================================================================
-tick.tadatv.com 10.0.22.49       2 u  874 1024  377    5.810   11.252  13.031
*wwwco1test12.mi 64.236.96.53     2 u  817 1024  377   83.799    1.636  52.182
-thor.netservice 64.113.32.5      2 u  865 1024  377   75.838   -4.941   6.927
+ftp1.riverbed.c 10.16.0.15       3 u  839 1024  377    1.740    2.610   6.121
-4.53.160.75     220.183.68.66    2 u  820 1024  377   48.183    8.513   1.116
+chief-sh158.lab 108.59.14.130    3 u  127 1024  373    1.560    5.737  13.369

     remote       conf  auth  key
===================================
tick.tadatv.com   yes   ok    12
wwwco1test12.mi   yes   none  none
thor.netservice   yes   bad   42
ftp1.riverbed.c   yes   none  none
4.53.160.75       yes   ok    11
chief-sh158.lab   yes   ok    10
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"Host Setup Commands"

show ntp authentication

Description

Displays NTP authentication settings.

Syntax

show ntp authentication

Parameters

None

Example

```
amnesiac > show ntp authentication
Trusted Keys: 5, 10
```

```
KeyID  KeyType   Encrypted Secret
-------------------------------------------------
5      MD5       rP1LTiIVk7QlMyFiLSpAKA==
65534  MD5       2Ovzk2RGghrBJLp6BX+BpSxo1pvz+5CM
```

Product

CMC, Steelhead appliance

Related Topics

"Host Setup Commands"

show out-of-path

Description

Displays out-of-path configuration settings.

Syntax

show out-of-path

Parameters

None

Example

```
amnesiac > show out-of-path
Enabled:    no
Inner Port: 7810
```

Product

Steelhead appliance

Related Topics

"Out-of-Path Support"

show packet-mode ip-channels

Description

Displays information about the setup of IP channels between Steelhead appliance peers.

Syntax

show packet-mode ip-channels [filter <filter-string> | sort-by <field> | brief]

Parameters

filter <filter-string>	Displays a filtered list of IP channel information. For example, to filter by source IP address (**srcip**), enter the source IP address as the filter string.
sort-by <field>	Displays IP channel information sorted by the following fields: • **id** - Channel ID • **srcip** - IP address of the originating Steelhead appliance • **srcport** - Port of the originating Steelhead appliance • **destip** - IP address of the destination Steelhead appliance • **destport** - Port of the destination Steelhead appliance • **lan** - LAN bytes • **wan** - WAN bytes • **reduction** - Percentage of reduction • **starttime** - Start time
filter <filter-string>	Displays a filtered list of IP channel information. For example, to filter by source IP address (**srcip**), enter the source IP address as the filter string.

Example

```
amnesiac > show packet-mode ip-channels
```

Product

Steelhead appliance

Related Topics

"packet-mode enable," "show packet-mode status"

show packet-mode status

Description

Displays whether or not packet-mode optimization is enabled.

Syntax

show packet-mode status

Parameters

None

Example

```
amnesiac > show packet-mode status
Enable packet mode: yes
```

Product

Steelhead appliance

Related Topics

"packet-mode enable," "show packet-mode ip-channels"

show path-selection

Description

Displays the path selection configuration, state, and statistics.

Syntax

show path-selection {path <path-name> | paths} {config | state | stats}

Parameters

path <pathname> | paths	Displays the path configuration for the specified path or for all paths.
config	Displays the path configuration.
state	Displays the path configuration and state.
stats	Displays statistics about the specified path.

Example

```
amnesiac > show path-selection path first config
Name:                    First
ID:                      0
Status:                  Up
Interface:               inpath0_0
Gateway IP:              172.16.56.4
Remote IP:               172.16.95.3
Probe DSCP:              1
Probe Timeout:           2 seconds
Probe Threshold:         3

amnesiac > show path-selection path first state
Name:                    First
ID:                      0
Status:                  Up
Interface:               inpath0_0
Gateway IP:              172.16.56.4
Remote IP:               172.16.95.3
Probe DSCP:              1
Probe Timeout:           2 seconds
Probe Threshold:         3
Priority:                0x20002
VLAN:                    65535
Source MAC:              00:0e:b6:90:dc:27
Destination MAC:         00:0a:8a:17:17:81

amnesiac > show path-selection path first stats
Name:                          First
ID:                            0
Bytes:                         0
Probe Requests:                467
Probe Request Relay Mismatch:  0
Probe Response Relay Mismatch: 0
```

Product

Steelhead appliance

Related Topics

"Path Selection Commands"

show path-selection interface stats

Description

Displays statistics about relay interfaces for the path selection feature.

Syntax

show path-selection interface [<interface-name>] stats

Parameters

<interface-name>	Displays path selection statistics about the specified relay interface.

Example

The following example shows statistics about the inpath0_0 interface:

```
amnesiac > show path-selection interface inpath0_0 stats
```

The following example shows statistics about all interfaces:

```
amnesiac > show path-selection interface stats
```

Product

Steelhead appliance

Related Topics

"Path Selection Commands"

show path-selection settings

Displays path-selection settings.

Syntax

show path selection settings

Parameters

None

Example

```
amnesiac > show path-selection settings
Learn behavior during path selection probe ricochet: first-on-cfg
Reflect path for probe responses:                    yes
Reflect path for optimized connection setup packets: yes
```

Product

Steelhead appliance

Related Topics

"Path Selection Commands"

show path-selection status

Displays path selection status.

Syntax

show path selection status

Parameters

None

Example

```
amnesiac > show path-selection status
Enabled: yes
```

Product

Steelhead appliance

Related Topics

"Path Selection Commands"

show peer version

Description

Displays the peer protocol version settings.

Syntax

show peer version

Parameters

None

Example

```
amnesiac > show peer version
No peer setting defined.
```

Product

Steelhead appliance

Related Topics

"Peering Commands"

show peers

Description

Displays information about connected peers.

Syntax

show peers [online-only]

Parameters

online-only	Displays connected peer appliances that are online.

Example

```
amnesiac > show peers
S IP              Name             Model   Version Licenses
- --------------- ---------------- ------- -------
-----------------------------
O 10.11.3.145     gen1-sh30        2020    6.0.0   CIFS/MAPI/SSL/ORACLE-FORMS

O = online, U = unknown
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

"Peering Commands"

show pfs all-info shares

Description

Displays PFS share settings.

Syntax

show pfs all-info shares [local-name <localname>]

Parameters

local-name <localname>	Displays the PFS settings for the specified local share.

Example

```
amnesiac > show pfs all-info shares
no registered shares
```

Product

Steelhead appliance

Related Topics

"PFS Support Commands"

show pfs status

Description

Displays the status of local shares.

Syntax

show pfs status [shares [local-name <localname>]]

Parameters

shares	Displays the status of all PFS shares.
local-name <localname>	Displays the status for the specified local share.

Example

```
amnesiac > show pfs status shares
+==============================
| Information for PFS share lshare1
|
| ----- Status -----
|   Last Sync Status:  true
|   Share Ready:  true
|   Status:  START_SYNC in progress since Fri Mar  9 17:04:26 2007
|   Size (MB):  39
|   Last Synced:  Fri Mar  9 17:05:30 2007
```

Product

Steelhead appliance

Related Topics

"PFS Support Commands"

show pfs configuration

Description

Displays PFS configuration settings.

Syntax

show pfs configuration shares [local-name <localname>]

Parameters

local-name <localname>	Displays the PFS settings for the specified local share.

Example

```
amnesiac > show pfs configuration shares
```

Product

Steelhead appliance

Related Topics

"PFS Support Commands"

show pfs settings

Description

Displays PFS general settings.

Syntax

show pfs settings

Parameters

None

Example

```
amnesiac > show pfs settings
% PFS not enabled
```

Product

Steelhead appliance

Related Topics

"PFS Support Commands"

show pfs stats shares

Description

Displays PFS share statistics.

Syntax

show pfs stats shares [local-name <localname>]

Parameters

local-name <localname>	Specify the name of the local share for which to display statistics.

Example

```
amnesiac > show pfs stats shares
+==============================
| Information for PFS share field_kit
|
| ----- Statistics -----
+==============================
| Information for PFS share internal-test
|
| ----- Statistics -----
+==============================
| Information for PFS share internal-townsend
|
| ----- Statistics -----
+==============================
```

Product

Steelhead appliance

Related Topics

"PFS Support Commands"

show prepop

Description

Displays prepopulation settings information.

Syntax

show prepop {all-info shares [remote-path <remote-path>] | configuration shares [remote-path <remote-path>] | stats shares [remote-path <remote-path>] | status shares [remote-path <remote-path>]}

Parameters

all-info shares [remote-path <remote-path>]	Displays all information for the prepopulation share or the specified share.
configuration shares [remote-path <remote-path>]	Displays configuration of the prepopulation share or the specified share.
stats shares [remote-path <remote-path>]	Displays prepopulation statistics for all shares or the specified share.
status shares [remote-path <remote-path>]	Displays status for the prepopulation shares or the specified share.

Example

```
amnesiac > show prepop all-info shares
No registered shares
```

Product

Steelhead appliance

Related Topics

"CIFS Prepopulation Support Commands"

show prepop log dry-run

Description

Displays the dry run log for a prepopulated share.

Syntax

show prepop log dry-run remote-path <remote-path>

Parameters

remote-path <remote-path>	Specify the remote path of the share to be displayed. Use the format `'\\server\share'`.

Example

```
amnesiac > show prepop log dry-run remote-path '\\10.11.61.66\prepop_share'
```

Product

Steelhead appliance

Related Topics

"CIFS Prepopulation Support Commands"

show prepop log sync

Description

Displays the prepopulation synchronization log for the prepopulated share.

Syntax

show prepop log sync remote-path <remote-path>

Parameters

remote-path <remote-path>	Specify the remote path of the share to be displayed. Use the format `'\\server\share'`.

Example

```
amnesiac > show prepop log sync remote-path '\\10.11.61.66\prepop_share'
```

Product

Steelhead appliance

Related Topics

"CIFS Prepopulation Support Commands"

show prepop share policy

Description

Displays policy information.

Syntax

show prepop share policy remote-path <remote-path> [policy <policy-name>]

Parameters

remote-path <remote-path>	Specify the remote path of the share. Use the format `'\\server\share'`.
policy <policy-name>	Specify a policy name.

Example

```
amnesiac # show prepop share policy remote-path '\\10.11.61.66\prepop_share'
```

Product

Steelhead appliance

Related Topics

"CIFS Prepopulation Support Commands"

show protocol cifs

Description

Displays CIFS settings.

Syntax

show protocol cifs

Parameters

None

Example

```
amnesiac > show protocol cifs
Enable Transparent Prepopulation Support: no
Disable CIFS Write Optimization:          no
Security Signature Optimization:          yes
Overlapping Open Enabled: yes
```

Product

Steelhead appliance

Related Topics

"CIFS, SMB, SMB2, and SMB3 Support Commands"

show protocol cifs applock

Description

Displays CIFS applock settings.

Syntax

show protocol cifs applock

Parameters

None

Example

```
amnesiac > show protocol cifs applock
Enabled:         no
```

Product

Steelhead appliance

Related Topics

"CIFS, SMB, SMB2, and SMB3 Support Commands"

show protocol cifs ext-dir-cache

Description

Displays whether or not CIFS extended directory caching is enabled.

Syntax

show protocol cifs ext-dir-cache

Parameters

None

Example

```
amnesiac > show protocol cifs ext-dir-cache
  CIFS extended directory cache
    Enabled:   no
```

Product

Steelhead appliance

Related Topics

"CIFS, SMB, SMB2, and SMB3 Support Commands," "protocol cifs ext-dir-cache enable"

show protocol cifs nosupport client

Description

Displays the client operating systems not supported by optimization

Syntax

show protocol cifs nosupport client

Parameters

None

Example

```
amnesiac > show protocol cifs nosupport client
Operating systems without optimization support:
macunk
novell
winunk
wnt3
```

Product

Steelhead appliance

Related Topics

"CIFS, SMB, SMB2, and SMB3 Support Commands"

show protocol cifs nosupport server

Description

Displays the server operating systems not supported by optimization

Syntax

show protocol cifs nosupport server

Parameters

None

Example

```
amnesiac > show protocol cifs nosupport server
Operating systems without optimization support:
bsd
win7
winunk
wnt3
```

Product

Steelhead appliance

Related Topics

"CIFS, SMB, SMB2, and SMB3 Support Commands"

show protocol cifs oopen

Description

Displays CIFS overlapping open sessions.

Syntax

show protocol cifs oopen

Parameters

None

Example

```
amnesiac > show protocol cifs oopen
Enabled:              yes
Optimization Policy:  deny first
Extensions to always allow:
doc, pdf, ppt, sldasm, slddrw, slddwg, sldprt, txt, vsd, xls
Extensions to always deny:
ldb, mdb
```

Product

Steelhead appliance

Related Topics

"CIFS, SMB, SMB2, and SMB3 Support Commands"

show protocol cifs smb signing status

Description

Displays SMB signing status.

Syntax

show protocol cifs smb signing status

Parameters

None

Example

```
amnesiac > show protocol cifs smb signing status
SMB Signing Enabled: no
Mode Type:           transparent
```

Product

Steelhead appliance

Related Topics

"CIFS, SMB, SMB2, and SMB3 Support Commands"

show protocol cifs spoolss

Description

Displays CIFS print spool settings.

Syntax

show protocol cifs spoolss

Parameters

None

Example

```
amnesiac > show protocol cifs spoolss
```

Product

Steelhead appliance

Related Topics

"protocol cifs spoolss enable"

show protocol citrix

Description

Displays Citrix status.

Syntax

show protocol citrix [cdm | smallpkts]

Parameters

cdm	Displays whether Citrix client device mapping (CDM) is enabled or disabled and other CDM information.
smallpkts	Displays whether Citrix small packets optimization is enabled or not.

Example

```
amnesiac > show protocol citrix
Citrix Enabled:                 no
Secure ICA Enabled:             no
ICA Port:                       1494
Session Reliability Port:       2598

amnesiac > show protocol citrix smallpkts
Citrix small packets optimization enabled = : no
Citrix small packets optimization threshold = : 64
```

Product

Steelhead appliance

Related Topics

"Citrix Support Commands"

show protocol connection

Description

Displays the HS-TCP settings.

Syntax

show protocol connection

Parameters

None

Example

```
amnesiac > show protocol connection
LAN:
Send socket buffer size:            81920 bytes
Receive socket buffer size:         32768 bytes
WAN:
Default send socket buffer size:    262140 bytes
Default receive socket buffer size: 262140 bytes
```

Product

Steelhead appliance

Related Topics

"High-Speed TCP and Satellite Optimization Commands"

show protocol domain-auth restricted-krb

Description

Displays whether or not the Kerberos restricted trust model is enabled.

Syntax

show protocol domain-auth restricted-krb

Parameters

None

Example

```
amnesiac > show protocol domain-auth restricted-krb
Kerberos Restricted Trust Model Mode Enabled: yes
```

Product

Steelhead appliance

Related Topics

"protocol domain-auth restricted-krb enable"

show protocol domain-auth credentials location

Description

Displays the location of the domain authentication credentials.

Syntax

show protocol domain-auth credentials location

Parameters

None

Example

```
amnesiac > show protocol domain-auth credentials location
Domain Authentication credentials location: In secure vault
```

Product

Steelhead appliance

Related Topics

"Windows Domain Authentication Delegation Commands"

show protocol domain-auth delegation auto-mode

Description

Displays whether the auto-delegation mode is enabled or disabled.

Syntax

show protocol domain-auth delegation auto-mode

Parameters

None

Usage

Auto-delegation mode is enabled by the "protocol domain-auth delegation auto-mode enable" command.

Example

```
amnesiac > show protocol domain-auth delegation auto-mode
   Auto Delegation Mode Enabled: no
```

Product

Steelhead appliance

Related Topics

"Windows Domain Authentication Delegation Commands"

show protocol domain-auth delegation delegate-user

Description

Displays delegate user accounts.

Syntax

show protocol domain-auth delegation delegate-user

Parameters

None

Usage

Auto-delegation mode is enabled by the "protocol domain-auth delegation auto-mode enable" command.

Example

```
amnesiac > show protocol domain-auth delegation delegate-user
No domains configured.
```

Product

Steelhead appliance

Related Topics

"Windows Domain Authentication Delegation Commands"

show protocol domain-auth delegation rules

Description

Displays the Windows domain delegated authentication server rules.

Syntax

show protocol domain-auth delegation rules

Parameters

None

Usage

Windows domain delegated authentication server rules are configured by the "protocol domain-auth delegation rule dlg-all-except" and "protocol domain-auth delegation rule dlg-only"commands.

Example

```
amnesiac > show protocol domain-auth delegation rules
    Active List for Delegation Rules: Delegation-Only List
    No Rules configured for the Delegation-Only List
    No Rules configured for the Delegation-All-Except List
```

Product

Steelhead appliance

Related Topics

"Windows Domain Authentication Delegation Commands"

show protocol domain-auth native-krb

Description

Displays the native Kerberos mode setting, yes or no.

Syntax

show protocol domain-auth native-krb

Parameters

None

Example

```
amnesiac > show protocol domain-auth native-krb
```

```
Native Kerberos Mode Enabled: yes
```

Product

Steelhead appliance

Related Topics

"protocol domain-auth oneway-trust"

show protocol domain-auth oneway-trust

Description

Displays the configurations in the one-way trust list for delegated authentication.

Syntax

show protocol domain-auth oneway-trust

Parameters

None

Usage

Configure the one-way trust list for delegated authentication with the "protocol domain-auth oneway-trust" command.

Example

```
amnesiac > show protocol domain-auth oneway-trust
No Configurations in Domain One-way Trust List
```

Product

Steelhead appliance

Related Topics

"Windows Domain Authentication Delegation Commands"

show protocol domain-auth replication replicate-user

Description

Displays replication user accounts.

Syntax

show protocol domain-auth replication replicate-user

Parameters

None

Example

```
amnesiac > show protocol domain-auth replication replicate-user
```

Product

Steelhead appliance

Related Topics

"protocol domain-auth auto-conf replication"

show protocol fcip rules

Description

Displays FCIP (Fiber Channel over IP) optimization ports.

Syntax

show protocol fcip rules

Parameters

None

Example

```
amnesiac > show protocol fcip rules
Src IP          Dst IP          DIF Enabled  DIF Blocksize
------          ------          -----------  -------------
all (0.0.0.0)   all (0.0.0.0)   false        N/A
```

Product

Steelhead appliance

Related Topics

"FCIP Support Commands"

show protocol fcip settings

Description

Displays FCIP (Fiber Channel over IP) optimization settings.

Syntax

show protocol fcip settings

Parameters

None

Example

```
amnesiac > show protocol fcip settings
Enabled: no
Ports  : 3225,3226,3227,3228
```

Product

Steelhead appliance

Related Topics

"FCIP Support Commands"

show protocol ftp

Description

Displays FTP settings.

Syntax

show protocol ftp

Parameters

None

Example

```
amnesiac > show protocol ftp
FTP Port  Enable
--------  ------
21        true
```

Product

Steelhead appliance

Related Topics

"FTP Support Commands"

show protocol http

Description

Displays HTTP settings.

Syntax

show protocol http

Parameters

None

Example

```
amnesiac > show protocol http
Enabled: yes
NTLM Authentication Settings:
  Default              Reuse Auth: no
Pre-Fetch Objects with Extensions:
  css
  gif
  jpg
  js
```

Product

Steelhead appliance

Related Topics

"HTTP Support Commands"

show protocol http auto-config selection

Description

Displays HTTP auto configuration selection settings.

Syntax

show protocol http auto-config selection

Parameters

None

Example

```
amnesiac > show protocol http auto-config selection
```

```
Cache:                        yes
Parse and Prefetch:           yes
URL Learning:                 yes
NTLM Auth Srv:                yes
Force NTLM Negotiation:       yes
Strip Authentication Header: yes
Authenticate Cache:           yes
Strip Compression:            yes
Insert Cookie:                yes
Insert Keep Alive:            yes
Sharepoint FPSE:              no
Sharepoint WebDAV:            no
Sharepoint FSSHTTP:           yes
```

Product

Steelhead appliance

Related Topics

"protocol http auto-config selection"

show protocol http metadata-resp

Description

Displays HTTP metadata response settings.

Syntax

show protocol http metadata-resp

Parameters

None

Example

```
amnesiac > show protocol http metadata-resp
Minimum Metadata Response Time (seconds):  60
Maximum Metadata Response Time (seconds):  86400

Metadata Response Extensions:
-----------------------------
  css
  gif
  jpg
  js
  png
```

Product

Steelhead appliance

Related Topics

"HTTP Support Commands"

show protocol http prefetch extensions

Description

Displays HTTP prefetched extensions through URL learning.

Syntax

show protocol http prefetch extensions

Parameters

None

Example

```
amnesiac > show protocol http prefetch extensions
Pre-Fetch Objects with Extensions through URL-learning:
  css
  gif
  jpg
  js
  png
```

Product

Steelhead appliance

Related Topics

"HTTP Support Commands"

show protocol http prefetch tags

Description

Displays HTTP prefeteched tag settings.

Syntax

show protocol http prefetch tags

Parameters

None

Example

```
amnesiac > show protocol http prefetch tags
  Tag                              Attribute
  ------------------------------   ------------------------------
  base                             href
  body                             background
  img                              src
  link                             href
  script                           src
```

Product

Steelhead appliance

Related Topics

"HTTP Support Commands"

show protocol http prepop list

Description

Displays one or more lists of URLs.

Syntax

show protocol http prepop {list <list-name> | lists}

Parameters

list <list-name>	Displays a single list of URLs.
lists	Displays multiple lists of URLs.

Example

```
amnesiac > show protocol http prepop lists
```

Product

Steelhead appliance

Related Topics

"protocol http prepop verify-svr-cert enable," "protocol http prepop verify-svr-cert enable," "show protocol http prepop list"

show protocol http prepop status

Description

Displays the progress and status of a prepopulation operation.

Syntax

show protocol http prepop status {all | list <list-name>}

Parameters

all	Displays prepopulation status for all lists.
list <list-name>	Displays prepopulation status for the specified list. This option displays the last known status of the list.

Example

```
amnesiac > show protocol http prepop status all
```

Product

Steelhead appliance

Related Topics

"protocol http prepop verify-svr-cert enable," "show protocol http prepop list"

show protocol http prepop verify-svr-cert

Description

Displays server verification settings for HTTP prepopulation operations.

Syntax

show protocol http prepop verify-svr-cert

Parameters

None

Example

```
amnesiac > show protocol http prepop verify-svr-cert
Server verification: yes
```

Product

Steelhead appliance

Related Topics

"protocol http prepop verify-svr-cert enable"

show protocol http server-table

Description

Displays HTTP optimization settings for the hostnames and subnets in the server table.

Syntax

show protocol http server-table [auto-config | default]

Parameters

auto-config	Displays the host autoconfiguration table.
default	Displays the default HTTP server table.

Example

```
amnesiac > show protocol http server-table
UL: URL-Learning       PP: Parse-&-Prefetch
OP: Obj-Prefetch-Table RA: Reuse-Auth
SA: Strip-Auth-Header  GR: Gratuitous-401
FN: Force-Nego-NTLM    SC: Strip-Compression
IC: Insert-Cookie      IK: Insert-Keep-Alive

  Hostname/Subnet     UL   PP   OP   RA   SA   GR   FN   SC   IC   IK
  ------------------  ---  ---  ---  ---  ---  ---  ---  ---  ---  ---
  default             auto configured
```

Product

Steelhead appliance

Related Topics

"protocol http server-table"

show protocol http stream-split

Description

Displays the video stream-splitting configuration or statistics.

Syntax

show protocol http stream-split [stats]

Parameters

stats	Displays current statistics. This option returns the current statistics for: • number of video fragments that were fetched over the WAN. • number of fragments that were served locally.

Example

```
amnesiac > show protocol http stream-split
Live stream-splitting enabled: yes

amnesiac > show protocol http stream-split stats
Fragments fetched over WAN : 85
Fragments served locally   : 683
```

Product

Steelhead appliance

Related Topics

"Oracle Forms Support Commands"

show protocol mapi

Description

Displays MAPI settings.

Syntax

show protocol mapi

Parameters

None

Example

```
amnesiac > show protocol mapi
MAPI Optimization Enabled:      yes
Incoming MAPI Port:             7830
Prepop Enabled:                 yes
Prepop Max Connections:         1500
Prepop Poll Interval:           20 min(s)
Prepop Timeout:                 96 hr(s)
MAPI NSPI Optimization Enabled: yes
NSPI Port:                      7840
MAPI/Exchange 2003 Support:     yes
MAPI Port Remap:                yes
MAPI 2k7 Native:                yes
MAPI Encryption Enabled:        yes
MAPI 2k7 Force NTLM Auth:       yes
```

Product

Steelhead appliance

Related Topics

"protocol mapi enable"

show protocol ms-sql

Description

Displays MS SQL settings.

Syntax

show protocol ms-sql

Parameters

None

Example

```
amnesiac > show protocol ms-sql
Enable entire MS-SQL blade:          yes
MS-SQL server port:                  1433
MS-SQL number of preacknowledgement: 5
MS-SQL prefetch fetch-next:          yes
```

Product

Steelhead appliance

Related Topics

"MS-SQL Blade Support Commands"

show protocol ms-sql rules

Description

Displays MS SQL rules.

Syntax

show protocol ms-sql rules [default-cmds | default-config]

Parameters

default-cmds	Displays only the MS-SQL default commands.
default-config	Displays only the MS-SQL default configuration.

Example

```
amnesiac > show protocol ms-sql rules default-config
MS-SQL RPC Rule
MS-SQL RPC Rule
   Rule ID  Enable
   -------  ------
   1        true
     MS-SQL RPC Action
     Action ID  Enable
     ---------  ------
     1        true
       MS-SQL RPC Arg Action
       Arg Offset  Enable
       ----------  ------
       5        true
     Action ID  Enable
     ---------  ------
     2        true
       MS-SQL RPC Arg Action
       Arg Offset  Enable
       ----------  ------
       5        true
     Action ID  Enable
     ---------  ------
     3        true
(this is a partial example)
```

Product

Steelhead appliance

Related Topics

"MS-SQL Blade Support Commands"

show protocol nfs

Description

Displays NFS server and volume settings.

Syntax

show protocol nfs server | servers <name> <cr> [full | lookup-volumes | volume id <fsid>]

Parameters

server | servers <name> full | lookup-volumes | volume id <fsid>	Displays information for the NFS server specified by **<name>**. You can specify the following levels of detail: • **full** - Displays full details. • **lookup-volumes** - Displays a list of NFS server volumes that have been exported. • **volume id <fsid>** - Displays details for the NFS server volume.
servers <cr> | full	Displays NFS server settings.

Example

```
amnesiac > show protocol nfs server example
Global:
NFS Enabled: yes
V2/V4 Alarm Enabled: yes
Memory Soft Limit: 10000000
Memory Hard Limit: 12000000
Max Directory Count: 5242880 bytes
Max Symlink Count: 524288 bytes

Default NFS Server Settings:
Policy: Global Read-Write

Default NFS Volume Settings:
Policy: Global Read-Write
```

Product

Steelhead appliance

Related Topics

"NFS Support Commands"

show protocol notes

Description

Displays Lotus notes settings.

Syntax

show protocol notes

Parameters

None

Example

```
amnesiac > show protocol notes
Enable Notes Blade: no
Notes Port Number:  1352
Enable Notes Attach Compression Option: yes
Pull Replication Optimization enabled: no
```

Product

Steelhead appliance

Related Topics

"Lotus Notes Commands"

show protocol oracle-forms

Description

Displays Oracle Forms settings.

Syntax

show protocol oracle-forms

Parameters

None

Example

```
amnesiac > show protocol oracle-forms
Enabled: yes
HTTP mode enabled: no
```

Product

Steelhead appliance

Related Topics

"Oracle Forms Support Commands"

show protocol smb2

Description

Displays SMB2 signing status and whether or not SMB2 is enabled.

Syntax

show protocol smb2 {status | signing status}

Parameters

status	Is the SMB2 protocol enabled or disabled.
signing status	Is SMB2 signing enabled (yes or no) and which SMB2 signing mode is configured (transparent or delegation).

Example

```
amnesiac > show protocol smb2 status
SMB2 Enabled: yes

amnesiac > show protocol smb2 signing status
SMB2 Signing Enabled: no
Mode Type:           delegation
```

Product

Steelhead appliance

Related Topics

"protocol smb2 signing enable", "protocol smb2 signing mode-type"

show protocol snapmirror

Description

Displays the filer configuration settings for one or all filers.

Syntax

show protocol snapmirror [filer <name> [volume <volume name>]]

Parameters

filer <name>	Optionally, specify the name of the filer.
volume <volume name>	Optionally, specify the volume name.

Usage

The **show protocol snapmirror** command displays configuration settings for all filers.

Example

```
amnesiac > show protocol snapmirror
Addresses:

filer    Source IP
-------- -----------
server-1 10.12.200.1

volume policies:

filer    volume Opt policy  Description
-------- ------ ----------- -----------
server-1 vol0   sdr-default
```

Product

Steelhead appliance

Related Topics

"SnapMirror Support Commands"

show protocol snapmirror stats

Description

Displays statistics for SnapMirror selective optimization.

Syntax

show protocol snapmirror [filer <name> [volume <volume-name>]] stats [brief] [live [interval <seconds>]]

Parameters

filer <name>	Specify the name of the filer.
volume <volume-name>	Specify the volume name.
[brief] [live [interval <seconds>]]	Displays optimization statistics. Statistics are refreshed periodically, as specified by the time interval (in seconds). If **brief** is specified, the output is displayed with a minimum amount of detail.

Example

```
amnesiac > show protocol snapmirror stats live

Time                Filer  Volume  Opt policy  Reduction LAN Mbps WAN Mbps LAN  KB WAN KB  Desc
------------------- ------ ------- ----------- --------- -------- -------- ------- ------- ------
01/07/2013 16:39:17 ksnap1 vol2    lz-only     78.76%             73,782  15,672
01/07/2013 16:39:17 ksnap1 vol3    none        0.00%              74,102  84,072
01/07/2013 16:39:17 ksnap1 vol4    sdr-default 79.25%             74,030  15,361
01/07/2013 16:39:17 ksnap1 *       -           57.49%            278,274 118,294           None
```

Product

Steelhead appliance

Related Topics

"SnapMirror Support Commands"

show protocol snapmirror settings

Description

Displays global settings for SnapMirror optimization.

Syntax

show protocol snapmirror settings

Parameters

None

Example

```
amnesiac > show protocol snapmirror settings
Enabled: yes
Ports  : 10566
```

Product

Steelhead appliance

Related Topics

"SnapMirror Support Commands"

show stats protocol snapmirror

Description

Displays SnapMirror protocol statistics for a specified time period.

Syntax

show stats protocol snapmirror [filer <name>] [volume <volume-name>] [total] {interval <interval-time> | start-time <"YYYY/MM/DD HH:MM:SS"> end-time <"YYYY/MM/DD HH:MM:SS">}

Parameters

filer <name>	Specify the name of the filer.
volume <volume-name>	Specify the volume name.
total	Displays the total bytes transferred instead of throughput.
interval <time-interval>	Specify the time interval in which to process statistics. Choices are the most recent of the following values: • 1min • 5min • hour • day • week • month Statistics are refreshed periodically, as specified by the time interval.
start-time <YYYY/MM/DD HH:MM:SS>	Specify the start time to collect SnapMirror statistics. Use the format "YYYY/MM/DD HH:MM:SS" (enclosed in double quotes).
end-time <YYYY/MM/DD HH:MM:SS>	Specify the end time to stop collecting SnapMirror statistics. Use the format "YYYY/MM/DD HH:MM:SS" (enclosed in double quotes).

Example

```
amnesiac > show stats protocol snapmirror interval week
```

Product

Steelhead appliance

Related Topics

"SnapMirror Support Commands"

show protocol srdf rules

Description

Displays rules for isolating DIF headers within the SRDF data stream.

Syntax

show protocol srdf rules

Parameters

None

Example

```
amnesiac > show protocol srdf rules
Src IP          Dst IP          DIF Enabled  DIF Blocksize
------          ------          -----------  -------------
10.12.203.1     10.12.203.2     true         520
all (0.0.0.0)   all (0.0.0.0)   true         512
```

Product

Steelhead appliance

Related Topics

"SRDF Support Commands"

show protocol srdf settings

Description

Displays Symmetrix Remote Data Facility (SRDF) optimization settings.

Syntax

show protocol srdf settings

Parameters

None

Example

```
amnesiac > show protocol srdf settings
Enabled: yes
Ports   : 1748
```

Product

Steelhead appliance

Related Topics

"SRDF Support Commands"

show protocol srdf symm

Description

Displays Symmetrix Remote Data Facility (SRDF) selective optimization statistics.

Syntax

show protocol srdf symm <cr> | id <Symmetrix ID> [base_rdf_group <RDF number base> | rdf_group <RDF group> |stats <cr> | [brief | live <cr> | interval <seconds>]]

Parameters

id <Symmetrix ID>	Specify a Symmetrix ID. The Symmetrix ID is an alphanumeric string that can contain hyphens and uderscores (for example, a standard Symmetrix serial number: 000194900363). Do not use spaces or special characters.
base_rdf_group <RDF number base>	Specify the Remote Data Facility (RDF) base type: • **0** - Specify if your RDF group is a 0-based group type. • **1** - Specify if your RDF group is a 1-based group type. This is the default value of RDF groups.
rdf_group <RDF group>	Specify an IP address for the RDF group. The RDF group number can begin with either a 0 or 1. The default value is 1.
stats <cr> | [brief | live <cr> |[interval <seconds>]	Displays optimization statistics. Statistics are refreshed periodically as specified by the time interval (in seconds). If the Symmetrix ID is omitted, the statistics for all Symmetrix IDs on this Steelhead appliance are displayed. If **brief** is specified, the output is displayed with a minimum amount of detail.

Usage

SRDF selective optimization enables you to set different optimization levels for RDF groups.

Example

```
amnesiac > show protocol srdf symm 0123 stats brief
SYMM RDF group opt policy Reduction LAN Mbps WAN Mbps description
---- --------- ---------- --------- -------- -------- -----------
0123   1        none        100%       20      20      Oracle1 DB
0123   2        lz-only      80%      200      40      Oracle2 DB
0123   3        sdr-default  90%      200      20      Homedirs
0123   4        sdr-default  90%      200      20      Oracle3 DB
```

Product

Steelhead appliance, CSH

Related Topics

"SRDF Support Commands"

show protocol ssl

Description

Displays SSL configuration settings and certificates.

Syntax

show protocol ssl

Parameters

None

Example

```
amnesiac > show protocol ssl
Enabled: no
Fail handshakes if a relevant CRL cannot be found: no

CA certificates:
  AOL_Time_Warner_1
  AOL_Time_Warner_2
  Actalis
  AddTrust_Class_1
  AddTrust_External
  AddTrust_Public
<<partial list>>
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl backend

Description

Displays SSL back-end settings.

Syntax

show protocol ssl backend

Parameters

None

Example

```
amnesiac > show protocol ssl backend
Bypass interval when handshakes fail:                    300 seconds
Bypass interval when no suitable certificate is found: 3600 seconds
Bypass table maximum size:                               9000
Renegotiation with NULL certificates enabled:            no
Certificate chain caching enabled:                       no
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl backend bypass-table

Description

Displays the list of bypassed servers.

Syntax

show protocol ssl backend bypass-table [client-ip <ip-addr>] [server-ip <ip-addr> [server-port <port>]]

Parameters

client-ip <ip-addr>	Specify the client IPv4 or IPv6 address.
server-ip <ip-addr>	Specify the server IPv4 or IPv6 address.
server-port <port>	Specify the server port.

Example

```
amnesiac > show protocol ssl backend bypass-table client-ip 10.0.0.1
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl backend client cipher-strings

Description

Displays SSL cipher strings for use with clients.

Syntax

show protocol ssl backend client cipher-strings [verbose]

Parameters

verbose	Displays the verbose list of ciphers.

Example

```
amnesiac > show protocol ssl backend client cipher-strings verbose

  # Cipher String/Suite Name
--- ------------------------------
  1 DEFAULT
```

```
                                 KeyExch(*):  Auth:  Enc(*):    Mac:      (+)
    AES256-SHA                   RSA          RSA    AES(256)   SHA1
    DES-CBC3-SHA                 RSA          RSA    3DES(168)  SHA1
    AES128-SHA                   RSA          RSA    AES(128)   SHA1
    RC4-SHA                      RSA          RSA    RC4(128)   SHA1
    RC4-MD5                      RSA          RSA    RC4(128)   MD5
    DES-CBC-SHA                  RSA          RSA    DES(56)    SHA1
    EXP-DES-CBC-SHA              RSA(512)     RSA    DES(40)    SHA1   export
    EXP-RC2-CBC-MD5              RSA(512)     RSA    RC2(40)    MD5    export
    EXP-RC4-MD5                  RSA(512)     RSA    RC4(40)    MD5    export

    (*) Numbers in parentheses are key size restrictions.
    (+) "export" denotes an "export" classification.
<<this is a partial list>>
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl backend disc-table

Description

Displays the list of discovered servers.

Syntax

show protocol ssl backend disc-table [full]

Parameters

full	Displays the table settings for all discovered servers.

Example

```
amnesiac > show protocol ssl backend disc-table
Discovered servers:
  No discovered servers.
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl backend server cipher-strings

Description

Displays SSL cipher strings for use with servers.

Syntax

show protocol ssl backend server cipher-strings | [verbose]

Parameters

verbose	Displays the verbose list of ciphers.

Example

```
amnesiac > show protocol ssl backend server cipher-strings verbose
```

```
Discovered servers:
  No discovered servers.
amnesiac > show protocol ssl backend server cipher-strings
  # Cipher String/Suite Name
--- ------------------------------
  1 DEFAULT
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl ca

Description

Displays a CA certificate.

Syntax

show protocol ssl ca <ca name> <cr> | certificate [raw | text]

Parameters

ca <ca name>	Specify the CA name.
certificate [raw | text]	Displays SSL CA certificate in raw or text format.

Example

```
amnesiac > show protocol ssl ca Actalis certificate text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 1034588298 (0x3daa908a)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=IT, O=Actalis S.p.A., OU=Certification Service Provider, CN=Ac
talis Root CA
        Validity
            Not Before: Oct 14 09:38:38 2002 GMT
            Not After : Oct 14 08:38:38 2022 GMT
        Subject: C=IT, O=Actalis S.p.A., OU=Certification Service Provider, CN=A
ctalis Root CA
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:bc:54:63:8a:98:15:48:be:6a:ae:e1:70:90:4a:
                    a4:55:00:26:8b:6e:8d:4f:eb:b3:df:ca:c8:53:6c:
                    84:e4:30:ba:3d:bb:fb:f3:c0:40:8c:c1:62:ce:ae:
                    20:4e:37:1f:5c:36:fe:7a:88:5e:00:e2:a9:8a:1e:
                    5d:a6:ca:d3:81:c9:f5:74:33:62:53:c2:28:72:2b:
                    c2:fb:b7:c1:81:d3:c3:fa:d7:eb:a9:62:05:94:1e:
                    ac:1f:53:69:2b:ca:39:1c:36:8f:63:38:c5:31:e4:
<<partial listing>>
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl cas

Description

Displays the CA certificates.

Syntax

show protocol ssl cas

Parameters

None

Example

```
amnesiac > show protocol ssl cas ca Actalis certificate text
  Name  (Issued To)
  AC_RaEDz_CerticE1mara_S.A.  (AC Ra<C3><AD>z Certic<C3><A1>mara S.A.)
  AOL_Time_Warner_1  (AOL Time Warner Root Certification Authority 1)
  AOL_Time_Warner_2  (AOL Time Warner Root Certification Authority 2)
  AddTrust_Class_1  (AddTrust Class 1 CA Root)
  AddTrust_External  (AddTrust External CA Root)
  AddTrust_Public  (AddTrust Public CA Root)
  AddTrust_Qualified  (AddTrust Qualified CA Root)
  America_Online_1  (America Online Root Certification Authority 1)
  America_Online_2  (America Online Root Certification Authority 2)
  Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068  (Autoridad de Certi
ficacion Firmaprofesional CIF A62634068)
  Baltimore_CyberTrust  (Baltimore CyberTrust Root)
  COMODO  (COMODO Certification Authority)
  COMODO_ECC  (COMODO ECC Certification Authority)
  Certisign_Autoridade_Certificadora_AC1S  ()
  Certisign_Autoridade_Certificadora_AC2  ()
  Certisign_Autoridade_Certificadora_AC3S  ()
  Certisign_Autoridade_Certificadora_AC4  ()
  Certplus_Class_1_Primary  (Class 1 Primary CA)
  Certplus_Class_2_Primary  (Class 2 Primary CA)
  Certplus_Class_3P_Primary  (Class 3P Primary CA)
<<partial listing>>
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl client-cer-auth

Description

Displays Client Certificate Authentication settings.

Syntax

show protocol ssl client-cer-auth

Parameters

None

Example

```
amnesiac > show protocol ssl client-cer-auth
Enabled: yes
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl client-side session-reuse

Description

Displays the CA certificates.

Syntax

show protocol ssl client-side session-reuse

Parameters

None

Example

```
amnesiac > show protocol ssl client-side session-reuse
Enabled:                     no
Timeout:                     36000 secs (10.0 hours)
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl crl

Description

Displays current status of CRL polling.

Syntax

show protocol ssl crl {ca <ca name>| cas [crl-file <string> text] | report ca <string>}

Parameters

ca <ca name>	Displays the current state of CRL polling of a CA
cas [crl-file <string> text]	Displays the CRL in text format version.
report ca <string>	Displays the reports of CRL polling from CA or display reports of CRL polling from the peer.

Example

```
amnesiac > show protocol ssl crl ca Actalis
Automatically Discovered CDPs:
(can be overriden by manually configured CDP URIs):
  CA: Actalis
   CDP Index: 1
     DP Name 1: URI:ldap://ldap.actalis.it/cn%3dActalis%20Root%20CA,ou%3dCertifi
cation%20Service%20Provider,o%3dActalis%20S.p.A.,c%3dIT?certificateRevocationLis
t;binary
     Last Query Status: unavailable
   CDP Index: 2
     DP Name 1: URI:http://ca.actalis.it/crl/root/getCRL
     Last Query Status: unavailable
```

```
Manually Configured CDP URIs:
(Dangling manually configured CDP URIs for certificates that do
not exist will NOT be updated.)
  No manually configured CDP URIs.
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl expiring-certs

Description

Displays expiring or expired SSL certificates.

Syntax

show protocol ssl expiring-certs

Parameters

None

Usage

This command displays any certificates with impending expiration dates (60 days) and expired dates.

Example

```
amnesiac > show protocol ssl expiring-certs
Peering certificate is OK.
All server certificates are OK.
All server chain certificates are OK.
All CA certificates are OK.
All peering trust certificates are OK.
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl midsession-ssl

Description

Displays midsession SSL settings.

Syntax

show protocol ssl midsession-ssl

Parameters

None

Example

```
amnesiac > show protocol ssl midsession-ssl
Enabled: yes
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl proxy-support

Description

Displays SSL proxy settings.

Syntax

show protocol ssl proxy-support

Parameters

None

Example

```
amnesiac > show protocol ssl proxy-support
Enabled: yes
```

Product

Steelhead appliance

Related Topics

"protocol ssl proxy-support enable"

show protocol ssl server-cert name

Description

Displays an SSL server certificate.

Syntax

show protocol ssl server-cert name <name>

Parameters

<name>	Specify the server certificate name.

Example

```
amnesiac > show protocol ssl server-cert name Go_Daddy_Class_2
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl server-cert name certificate

Description

Displays a SSL server certificate.

Syntax

show protocol ssl server-cert name <name> certificate <cr> | [raw | text]

Parameters

<name>	Specify the server certificate name.
[raw | text]	Specify the format type for the certificate.

Example

```
amnesiac > show protocol ssl server-cert name Go_Daddy_Class_2 certificate raw
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl server-cert name chain-cert

Description

Displays a SSL server certificate.

Syntax

show protocol ssl server-cert name <name> chain-cert <cert-name> certificate

Parameters

<name>	Specify the server certificate name.
<cert-name>	Specify the certificate name.

Example

```
amnesiac > show protocol ssl server-cert name Go_Daddy_Class_2 chain-cert certexample certificate
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl server-cert name chain-certs

Description

Displays the SSL server certificate.

Syntax

show protocol ssl server-cert name <name> chain-certs <cert-name> certificate

Parameters

<name>	Specify the server certificate name.
<cert-name>	Specify the certificate name.
certificate	Displays the certificate.

Example

```
amnesiac > show protocol ssl server-cert name Go_Daddy_Class_2 chain-certs certexample certificate
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl server-certs

Description

Displays the SSL server certificate.

Syntax

show protocol ssl server-certs

Parameters

None

Example

```
amnesiac > show protocol ssl server-certs
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show protocol ssl server

Description

Displays SSL servers and certificates.

Syntax

show protocol ssl server <cr> {ip <ip-addr> <cr> port <port> [certificate | chain-cert <name> certificate | chain-certs <cr>]}

Parameters

{ip <ip-addr> <cr> port <port> [certificate | chain-cert <name> certificate | chain-certs <cr>]}		Specify the IP address and the port of the SSL server you want to display.
	certificate	Displays the SSL server certificate.
	chain-cert <name> certificate	Specify the name of the chain certificate that you want to display.
	chain-certs <cr>	Displays all chain certificates.

Example

```
amnesiac > show protocol ssl server
SSL servers:
  1.1.1.1:443 (Enabled: yes)
  2.2.2.2:443 (Enabled: yes)
tcfe51 (config) # show protocol ssl server ip 1.1.1.1 chain-certs
No chain certificates.
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands"

show qos basic classification

Description

Displays Basic QoS settings.

Syntax

show qos basic classification {wan-oversub | global-app(s) | interface | policy(s) | site(s)}

Parameters

wan-oversub	Displays the basic QoS bandwidth oversubscription setting.
global-app(s)	Displays the configured global applications. For a complete list of supported global applications use **show qos basic classification global-app ?** to print help information on the command line.
interface	Shows interface settings.
policy(s)	Displays configured QoS service policy(s).
site(s)	Display the configured site(s).

Example

```
amnesiac # show qos basic classification
QoS Classification: Disabled
QoS Marking: Disabled
Mode: Basic
  Interface State       Burst (kbit) LinkRate (kbps)
  --------- ----------- ------------ ---------------
  wan0_0    Enabled     250          1000
  primary   Disabled    0            0
```

Product

Steelhead appliance

Related Topics

"QoS Support Commands"

show qos classification

Description

Displays advanced QoS classification settings.

Syntax

show qos classification {classes | interfaces | rules | site(s)}

Parameters

classes	Displays QoS classification class settings.
interfaces	Shows interface settings.
rules	Displays QoS classification rules.
site(s)	Displays the configured site(s).

Usage

Use the **show qos classification** command to verify that QoS is enabled and properly configured. For detailed information, see the *Steelhead Appliance Management Console User's Guide* and *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac > show qos classification classes
QoS Classification: Enabled
QoS Marking: Enabled
Mode: Advanced (Hierarchy)
  Interface State       Burst (kbit) LinkRate (kbps)
  --------- ----------- ------------ ---------------
  wan0_0    Enabled     25000        100000
  wan0_1    Disabled    0            0
  primary   Disabled    0            0
```

Product

Steelhead appliance

Related Topics

"QoS Support Commands"

show qos control-packets dscp

Description

Displays the global DSCP marking.

Syntax

show qos control-packets dscp

Parameters

None

Example

```
amnesiac > show qos control-packets dscp
Default DSCP marking: 255
```

Product

Steelhead appliance

Related Topics

"qos control-packets"

show qos inbound

Description

Displays inbound QoS settings.

Syntax

show qos inbound

Parameters

None

Example

```
amnesiac > show qos inbound
Inbound QoS Enabled: no
  Interface State       LinkRate (kbps)
  --------- ----------- ---------------
  wan0_0    Disabled    0
  wan0_1    Disabled    0
  wan1_0    Disabled    0
  wan1_1    Disabled    0
  wan2_0    Disabled    0
```

Product

Steelhead appliance

Related Topics

"Inbound QoS Commands"

show qos inbound classes

Description

Displays the summary of configured inbound QoS classes and their parameters.

Syntax

show qos inbound classes

Parameters

None

Example

```
amnesiac > show qos inbound classes
Class              Priority      GBW %  UBW %  LW     Class ID
------------------ ------------- ------ ------ ------ --------
Default            low           10.00  100.00 100.00 2
```

Product

Steelhead appliance

Related Topics

"Inbound QoS Commands"

show qos inbound rules

Description

Displays the summary of configured inbound QoS rules and their matching parameters.

Syntax

show qos inbound rules

Parameters

None

Example

```
amnesiac > show qos inbound rules

Rule Name    Desc         Remote           Local           Prt DSCP VLAN Type L7    Class
---- ------  ------------ ---------------  --------------  --- ---- ---- ---- ----- -------
1    bus_app Default Rule 0.0.0.0/0:all    0.0.0.0/0:all   all all  all  all  None  Default
```

Product

Steelhead appliance

Related Topics

"Inbound QoS Commands"

show qos l7protocol

Description

Displays information about a supported Layer 7 protocol or protocols.

Syntax

show qos l7protocol(s) <protocol> description

Parameters

<protocol>	Specify the protocol.
description	Describes the protocol or protocol family.

Usage

For detailed information about QoS, see the *Steelhead Appliance Management Console User's Guide* and *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac > show qos l7protocol ICA description
L7 Protocol   :  ICA
Description   : Citrix protocol family. This includes Citrix-CGP, ICA-Protocol, Citrix-IMA, Citrix-
Jedi, Citrix-Licensing, Citrix-Online, Citrix-RTMP, Citrix-SLG and Citrix-WANScaler protocols.

amnesiac > show qos l7protocol Youtube description
L7 Protocol   :  Youtube
Description   :  A video-sharing website on which users can upload, share, and view videos.
```

Product

Steelhead appliance

Related Topics

"QoS Support Commands"

show raid configuration

Description

Displays RAID configuration information.

Syntax

show raid configuration [detail]

Parameters

detail	Displays RAID configuration details.

Example

```
amnesiac > show raid configuration
UnitType  Status      Stripe       Size(GB)
-------------------------------------------
RAID-10     ONLINE      064KB       931.52
RAID-1      ONLINE         -           -
DISK 01     ONLINE         -         232.00
DISK 02     ONLINE         -         232.00
RAID-1      ONLINE         -           -
DISK 03     ONLINE         -         232.00
DISK 04     ONLINE         -         232.00
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Raid Commands"

show raid diagram

Description

Displays the physical layout of the RAID disks and the state of each drive: Online, Offline, Fail, Rebuild, Missing, and Spare.

Syntax

show raid diagram

Parameters

None

Example

```
amnesiac > show raid diagram

[      0 : online        ][      1 : online        ][      2 : online        ]
[      3 : online        ][      4 : online        ][      5 : online        ]
[      6 : online        ][      7 : online        ][      8 : online        ]
[      9 : online        ][     10 : online        ][     11 : online        ]
[     12 : online        ][     13 : online        ][     14 : online        ]
[     15 : online        ]
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Raid Commands"

show raid error-msg

Description

Displays RAID error messages.

Syntax

show raid error-msg

Parameters

None

Example

```
amnesiac > show raid error-msg
Alarm raid_error:  ok
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Raid Commands"

show raid info

Description

Displays RAID information.

Syntax

show raid info [detail]

Parameters

detail	Displays detailed RAID information.

Example

```
amnesiac > show raid info
Firmware            =>  713R
Bios                =>  G121
Memory              =>  64MB
Raid type           =>  Raid 10
Auto rebuild        =>  Enabled
Raid status         =>  OK
Stripe size         =>  64K
Num of drives       =>  4
Disk Vendor         =>  WDC
Serial Number       =>  ^B33686018
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Raid Commands"

show raid physical

Description

Displays RAID physical details.

Syntax

show raid physical

Parameters

None

Example

```
amnesiac > show raid physical
```

```
Adapter 0, Channel 0, Target ID 0
----------------------------------------
Type: DISK                 Vendor      : WDC
Product: WD2500SD-01KCB0   Revision    : 08.0
Synchronous   : No         Wide-32     : No    Wide-16: No
LinkCmdSupport: No         TagQ support: No    RelAddr: No
Removable     : No         SoftReset   : No    AENC   : No


Adapter 0, Channel 0, Target ID 1
----------------------------------------
Type: DISK                 Vendor      : WDC
Product: WD2500SD-01KCB0   Revision    : 08.0
Synchronous   : No         Wide-32     : No    Wide-16: No
LinkCmdSupport: No         TagQ support: No    RelAddr: No
Removable     : No         SoftReset   : No    AENC   : No

[partial output]
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Raid Commands"

show report

Description

Displays system details.

Syntax

show report {all | system | service}

Parameters

all	Specify to display a complete system detail report.
system	Specify to display system resources.
service	Specify to display system services.

Usage

Use this report to display system summary information for each of your components. Use this command to gather system information for debugging.

Example

```
amnesiac > show report all
System Detail Report
cpu
--------------------------------
status: green
info:   CPU 0, idle time: 20d 16h 20m 6s, system time: 4h 10m 19s, user time: 3h 34m 0s.
        CPU 1, idle time: 20d 16h 48m 28s, system time: 3h 28m 49s, user time: 4 h 1m 15s.
        CPU 2, idle time: 20d 17h 9m 42s, system time: 3h 50m 52s, user time: 3h 25m 9s.
        CPU 3, idle time: 20d 16h 15m 59s, system time: 3h 21m 53s, user time: 4h 46m 52s.
memory
--------------------------------
status: green
info:   Physical memory, total 8174168, used 6257768, free 1916400. Swap memory,
 total 2096472, used 192, free 2096280.
```

```
cifs
--------------------------------
status: green
info:   Optimization is enabled
<<this is a partial example>>
```

Product

Steelhead appliance

Related Topics

"show info," "show stats bandwidth"

show rsp

Description

Displays RSP settings.

Syntax

show rsp

Parameters

None

Example

```
amnesiac > show rsp
  Supported:   Yes
  Installed:   Yes
  Release:     6.0.0
  Enabled:     Yes
  State:       Running
  Disk Space:  5.62 GB used / 92.82 GB free / 98.44 GB total
  Memory:      0 MB used / 128 MB free / 128 MB total
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show rsp backups

Description

Displays RSP backup files.

Syntax

show rsp backups

Parameters

None

Example

```
amnesiac > show rsp backups
Backups:
  No backups
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show rsp clones

Description

Displays RSP clone operations in progress.

Syntax

show rsp clones

Parameters

None

Example

```
amnesiac > show rsp clones
   Clone Transfers:
      No clone transfers
```

Product

Steelhead appliance

Related Topics

"RSP Commands" "show rsp clones server," "show rsp clones status"

show rsp clones server

Description

Displays the settings for listening for remote RSP clones.

Syntax

show rsp clones server

Parameters

None

Example

```
amnesiac > show rsp clones server
   Password set; Incoming clone transfers enabled
```

Product

Steelhead appliance

Related Topics

"RSP Commands" "show rsp clones server," "show rsp clones status"

show rsp clones status

Description

Displays the most recent status by slot for RSP clone operations.

Syntax

show rsp clones status

Parameters

None

Example

```
amnesiac > show rsp clones status
Slot 1:
  Last incoming HA sync status:
    N/A
  Last outgoing HA sync status:
    N/A

Slot 2:
  Last incoming HA sync status:
    Status: 0
    Status String: Slot cloned successfully.
    Time Operation Started: 2010/03/16 16:59:46
    Duration of Operation: 855
    Transfer Host: dugas-sh159
  Last outgoing HA sync status:
    N/A
<<Output continues to show status for each slot>>
```

Product

Steelhead appliance

Related Topics

"RSP Commands," "show rsp clones," "show rsp clones server"

show rsp dataflow

Description

Displays RSP settings.

Syntax

show rsp dataflow <dataflow>

Parameters

dataflow <dataflow>	Specify the dataflow for display. For example, **inpath0_0.**

Usage

Use the dataflow option to display RSP dataflow settings.

Each RSP package uses its own RSP network interfaces to communicate. These network interfaces are matched with the physical intercept points that create VNIs. VNIs are network taps that enable data flow in and out of the RSP packages. VNIs act as the connection points for the LAN, WAN, primary, and auxiliary interfaces on the Steelhead appliance.

Example

```
amnesiac > show rsp
  Supported:   Yes
  Installed:   Yes
  Release:     6.0.0
  Enabled:     Yes
  State:       Running
  Disk Space:  13.54 GB used / 163.64 GB free / 177.18 GB total
  Memory:      0 MB used / 128 MB free / 128 MB total
amnesiac > show rsp inpath0_0
Dataflow inpath0_0:

  #     VNI                             Type
 --     ------------------------------  --------
```

```
      lan0_0
1     RiOS 0_0                        RiOS
      wan0_0

An "X" means the VNI is not in effect. Possible reasons include
the slot is disabled/uninstalled, the VNI is invalid, etc.
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show rsp images

Description

Displays RSP installation images on the disk.

Syntax

show rsp images [checksum]

Parameters

checksum	Displays the Message-Digest 5 algorithm (MD5) checksum of the RSP system image.

Usage

RSP installation images contain the software that must installed before you can enable RSP functionality on the Steelhead appliance. You can download multiple RSP installation images, but you can only install one at any one time.

Example

```
amnesiac > show rsp images
RSP Installation images:
  RSP Image 1
    File:    rsp-image.img
    Version: rbt_sh guam-i386-latest-39316 #0 2008-10-16 04:06:43 i386 root@paris:svn://svn/mgmt/
trunk

RSP Installed image:
  4.0 rbt_sh guam-i386-latest-39316 #0 2008-10-16 04:06:43 i386 root@pa
ris:svn://svn/mgmt/trunk
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show rsp opt-vni

Description

Displays optimization virtual network interfaces (VNIs).

Syntax

show rsp opt-vni <vni name> <cr> | rules

Parameters

<vni name>	Displays the Message-Digest 5 algorithm (MD5) checksum of the RSP system image.
rules	Displays configured rules for the optimization virtual network interface.

Example

```
amnesiac > show rsp opt-vni RiOS0_0
VNI RiOS0_0:

LAN to WAN direction:
  # Type     Source Addr        Source Port Dest Addr          Dest Port   Proto
--- -------- ------------------ ----------- ------------------ ----------- -----
  1 pass     all                all         all                1956        UDP
  2 redirect all                12345-54321 all                all         all
  3 copy     123.123.123.0/24   all         123.123.123.123/32 all         24

WAN to LAN direction:
  # Type     Source Addr        Source Port Dest Addr          Dest Port   Proto
--- -------- ------------------ ----------- ------------------ ----------- -----
  1 redirect 1.1.1.1/32         12-23       4.4.4.4/32         6621        TCP
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show rsp package

Description

Displays a third-party package installed on the Steelhead appliance.

Syntax

show rsp package <package>

Parameters

<package>	Specify the package filename.

Example

```
amnesiac > show rsp package
Package my-package.pkg:
  Valid:                   Yes

  Name:                    my
  Uncompressed size:       1.05MB
  Version:                 1
  Encrypted:               No
  Description:
    My package
[partial output]
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show rsp packages

Description

Displays RSP packages.

Syntax

show rsp packages [checksum]

Parameters

checksum	Displays the Message-Digest 5 algorithm (MD5) of the RSP packages.

Example

```
amnesiac > show rsp packages
Packages:
  my-package.pkg
  his-package.pkg
  another-package.pkg
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show rsp slot

Description

Displays a specified RSP slot.

Syntax

show rsp slot <slot name>

Parameters

<slot name>	Specify the slot name. The default names are **1**, **2**, **3**, **4**, **5.**

Example

```
amnesiac > show rsp slot 1
Slot 1:
  Package:
   Name: Tiny
   Version: 1
   Description:
       Tiny package

  Enabled:                   No
  Priority:                  Normal
  Clone Restore Pending:     No
  Memory Size:               128 (MB)
  Slot Size on Disk:         1.05 MB
  Attached Disks:
    Name                            Size        Adapter  Bus
    ------------------------------  ----------  -------- -----
    tiny                            1.00 MB     IDE      0:0
    Total Attached Disk Space:      1.00 MB

  Watchdog:
    Slot Status:           Not Applicable (Slot is not enabled)
    Timeout:               10 second(s)
    Startup Grace Period:  60 second(s)
    VNI Policy on fail:    Bypass-on-failure
    VM Reboot on fail:     No
    Ping Monitoring:       Disabled
      Ping Interval:       5 second(s)
      IP:                  0.0.0.0
    Heartbeat Monitoring:  Not supported
      Heartbeat Port:      None

  Optimization VNIs:
    Name                            T  I  N  VLAN   MAC
    ------------------------------  -  -  -  -----  -----------------
    1:QALanBridge                   L  R  R  none   00:0C:29:4F:9F:B1
    1:QAWanBridge                   W  R  R  none   00:0C:29:4F:9F:BB

    (T) Type:                  L=Lan  W=Wan  V=V-Inpath
    (I) Default IP Policy:     P=Pass  R=Redirect  C=Copy  L=L2-Switch
    (N) Default Non-IP Policy: P=Pass  R=Redirect  C=Copy  L=L2-Switch

  Management VNIs:
    Name                                 Bridged To  MAC
    -----------------------------------  ----------  -----------------
    1:QABridgeMgmt                       primary     00:0C:29:4F:9F:A7
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show rsp slots

Description

Displays RSP slots.

Syntax

show rsp slots

Parameters

None

Example

```
amnesiac > show rsp slots
Slot 1:
  Vacant.

---------------------------------------------------------------------------
Slot 2:
  Vacant.

---------------------------------------------------------------------------
Slot 3:
  Vacant.

---------------------------------------------------------------------------
Slot 5:
  Vacant.

---------------------------------------------------------------------------
```

```
Slot myslot:
  Vacant.

---------------------------------------------------------------------------
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show rsp vmware

Description

Displays VMware server information.

Syntax

show rsp vmware log hostd [index <index>] | web-access

Parameters

log hostid	Displays VMware Server host agent logs.
index <index>	Optionally, specify the host agent log index. The index is an optional number that requests a numbered virtual machine log.
web-access	Displays the URL for VMware server as it is running on the Steelhead appliance. It also displays the VMware SSL certificate details for the Steelhead appliance.

Example

```
amnesiac > show rsp vmware web-access
URL: http://MyTestSite.MyLab.MyDomain.com:8222

Certificate:
Issued To:
  Common Name:       MyTestSite
  Email:             ssl-certificates@vmware.com
  Organization:      VMware, Inc.
  Organization Unit: VMware Management Interface
  Locality:          Palo Alto
  State:             California
  Country:           US
[partial output]
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show rsp vnis

Description

Displays RSP optimization and management virtual network interfaces (VNIs).

Syntax

show rsp vnis

Parameters

None

Example

```
amnesiac > show rsp vnis
  Optimization VNIs:
    RiOS 0_0    (type: RiOS, VLAN: None)

  Management VNIs:
    No management VNIs.
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show scep service

Description

Displays SCEP service status.

Syntax

show scep service

Parameters

None

Example

```
amnesiac > show scep service
```

Product

Steelhead appliance

Related Topics

"scep service restart"

show secure-peering

Description

Displays secure peering settings.

Syntax

show secure-peering

Parameters

None

Example

```
amnesiac > show secure-peering
Traffic Type To Encrypt: ssl-only

Fallback To No Encryption: Not Applicable for 'ssl-only'

Certificate Details:
Issued To:
  Common Name:        Steelhead D34ST0005C00C
  Organization:       Riverbed Technology, Inc.
  Locality:           San Francisco
  State:              California
  Country:            --
  Serial Number:      cd:XX:e8:30:dd:XX:2c:XX
Issued By:
  Common Name:        Steelhead D34ST0005C00C
  Organization:       Riverbed Technology, Inc.
  Locality:           San Francisco
  State:              California
  Country:            --
Validity:
  Issued On:          Nov 12 22:36:10 2009 GMT
  Expires On:         Nov 12 22:36:10 2011 GMT
Fingerprint:
  SHA1:               3F:XX:C6:27:C5:XX:XX:2B:D4:XX:0C:F6:0F:9E:FA:F2:1A:XX:B7:XX
Key:
  Type:               RSA
  Size (Bits):        1024
<<partial example>>
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering black-lst-peer

Description

Displays self-signed black list peers in secure peering.

Syntax

show secure-peering black-lst-peer <ip-addr>

Parameters

<ip-addr>	Specify the address of the black list peer.

Example

```
amnesiac > show secure-peering black-lst-peer 10.0.0.1
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering black-lst-peers

Description

Displays self-signed black list peers.

Syntax

show secure-peering black-lst-peers

Parameters

None

Example

```
amnesiac > show secure-peering black-lst-peers
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering ca

Description

Displays a specified peering CA certificate.

Syntax

show secure-peering ca <cert-name> certificate [raw | text]

Parameters

<cert-name> certificate	Specify the certificate name.
[raw | text]	Specify the format for the certificate.

Example

```
amnesiac > show secure-peering ca Go_Daddy_Class_2 raw
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering cas

Description

Displays all configured secure peering CA certificates.

Syntax

show secure-peering cas

Parameters

None

Example

```
amnesiac > show secure-peering cas
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering certificate

Description

Displays a certificate.

Syntax

show secure-peering certificate <cr> [raw | text]

Parameters

[raw | text]	Specify the format for the certificate.

Example

```
amnesiac > show secure-peering certificate raw
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering cipher-strings

Description

Displays a cipher.

Syntax

show secure-peering cipher-strings <cr> | verbose

Parameters

verbose	Displays detailed information for the cipher string.

Example

```
amnesiac > show secure-peering cipher-strings
  # Cipher String/Suite Name
--- ------------------------------
  1 DEFAULT
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering crl

Description

Displays a certificate.

Syntax

show secure-peering crl {ca <string> | cas [crl-file <filename> text]}

Parameters

ca <string>	Specify the name of a secure-peering CA certificate.
cas	Displays the CRL polling status of secure-peering CAs.
crl-file <filename> text	Specify the name of the CRL file to display in text format.

Example

```
amnesiac > show secure-peering crl ca Go_Daddy_Class_2 cas
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering crl report ca

Description

Displays a certificate.

Syntax

show secure-peering crl report ca <string>

Parameters

<string>	Specify the name of a secure peering CA certificate.

Example

```
amnesiac > show secure-peering crl report ca Go_Daddy_Class_2
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering gray-lst-peer

Description

Displays self-signed gray list peers.

Syntax

show secure-peering gray-lst-peer <ip-addr>

Parameters

<ip-addr>	Specify the address of the gray list peer.

Example

```
amnesiac > show secure-peering gray-lst-peer 10.0.0.1
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering gray-lst-peers

Description

Displays self-signed gray list peers.

Syntax

show secure-peering gray-lst-peers

Parameters

None

Example

```
amnesiac > show secure-peering gray-lst-peers
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering mobile-trust

Description

Displays a trusted Steelhead Mobile Controller entities that can sign certificates for Steelhead Mobile clients.

Syntax

show secure-peering mobile-trust <cert-name> certificate <cr> | [raw | text]

Parameters

<cert-name> certificate	Specify the certificate name.
[raw | text]	Specify the format for the certificate.

Example

```
amnesiac > show secure-peering mobile-trust Wells_Fargo certificate
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering mobile-trusts

Description

Displays trusted Steelhead Mobile Controller entities that may sign certificates for Steelhead Mobile clients.

Syntax

show secure-peering mobile-trusts

Parameters

None

Example

```
amnesiac > show secure-peering mobile-trusts
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering scep

Description

Displays SCEP information.

Syntax

show secure-peering scep

Parameters

None

Example

```
amnesiac > show secure-peering scep
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering scep auto-reenroll csr

Description

Displays the automatic re-enrollment CSR.

Syntax

show secure-peering scep auto-reenroll csr

Parameters

None

Example

```
amnesiac > show secure-peering scep auto-reenroll csr
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering scep auto-reenroll last-result

Description

Displays the result of the last completed automatic re-enrollment.

Syntax

show secure-peering scep auto-reenroll last-result

Parameters

None

Example

```
amnesiac > show secure-peering scep auto-reenroll last-result
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering scep ca

Description

Displays a specified SCEP peering CA certificate.

Syntax

show secure-peering scep ca <cert-name> certificate

Parameters

<cert-name> certificate	Specify the certificate name.

Example

```
amnesiac > show secure-peering scep ca Go_Daddy_Class_2
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering scep enrollment status

Description

Displays SCEP enrollment status.

Syntax

show secure-peering scep enrollment status

Parameters

None

Example

```
amnesiac > show secure-peering scep enrollment status
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering scep on-demand csr

Description

Displays SCEP on-demand enrollment information.

Syntax

show secure-peering scep on-demand csr

Parameters

None

Example

```
amnesiac > show secure-peering scep on-demand csr
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering scep on-demand last-result

Description

Displays the result of the last completed on-demand enrollment.

Syntax

show secure-peering scep on-demand last-result

Parameters

None

Example

```
amnesiac > show secure-peering scep on-demand last-result
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering white-lst-peer

Description

Displays self-signed white list peers.

Syntax

show secure-peering white-lst-peer <ip-addr>

Parameters

<ip-addr>	Specify the address of the white list peer.

Example

```
amnesiac > show secure-peering white-lst-peer 10.0.0.1
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show secure-peering white-lst-peers

Description

Displays self-signed white list peers.

Syntax

show secure-peering white-lst-peers

Parameters

None

Example

```
amnesiac > show secure-peering white-lst-peers
```

Product

Steelhead appliance

Related Topics

"Secure Peering (Secure Inner Channel) Commands"

show service

Description

Displays whether services are running.

Syntax

show service

Parameters

None

Example

```
amnesiac > show service
Optimization Service: Running
```

Product

Steelhead appliance

Related Topics

"System Administration and Service Commands"

show service connection pooling

Description

Displays connection pooling settings.

Syntax

show service connection pooling

Parameters

None

Example

```
amnesiac >  show service connection pooling
Connection Pooling Max Pool Size: 20
```

Product

Steelhead appliance

Related Topics

"Connection Pooling Commands"

show service neural-framing

Description

Displays neural framing settings.

Syntax

show service neural-framing

Parameters

None

Example

```
amnesiac >  show service neural-framing
Enable Computation of Neural heuristics: no
amnesiac >
```

Product

Steelhead appliance

Related Topics

"In-Path and Virtual In-Path Support Commands"

show service ports

Description

Displays service port settings.

Syntax

show service ports

Parameters

None

Example

```
amnesiac > show service ports
Service ports:
7800 (default)
7810
amnesiac >
```

Product

Steelhead appliance

Related Topics

"System Administration and Service Commands"

show single-ended rules

Description

Displays single-ended transport rules.

Syntax

show single-ended rules

Parameters

None

Example

```
amnesiac > show single-ended rules
Rule Source Address          Dest Address            Port        VLAN T S P R C
---- ----------------------- ----------------------- ----------- ---- - - - - -
   1 all-ipv4                all-ipv4                all         all  O Y Y N C
   2 all-ip                  all-ip                  Interactive all  P - - - -

   3 all-ip                  all-ip                  RBT-Proto   all  P - - - -
 def all-ip                  all-ip                  all         all  O Y N N C
---- ----------------------- ----------------------- ----------- ---- - - - - -
3 user-defined rule(s)

(T) Traffic Type:            O=Optimized  P=Passthrough
(S) SCPS Discovery:          Y=Enabled  N=Disabled
(P) Allow Proxy:             Y=Enabled  N=Disabled
(R) Rate-Pacing:             Y=Enabled  N=Disabled
(C) Congestion Control:      B=BW-EST C=PER-CONN-TCP E=ERR-TOL-TCP
                             H=HSTCP  R=RENO
```

Product

Steelhead appliance

Related Topics

"single-ended rule optimized scps-discover," "single-ended rule optimized tcp-proxy"

show snmp

Description

Displays SNMP server settings.

Syntax

show snmp

Parameters

None

Example

```
amnesiac > show snmp
SNMP enabled: yes
System location:
System contact:
Read-only community: public
Traps enabled: yes
No trap sinks configured.
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"SNMP Commands"

---

show snmp acl-info

Description

Displays SNMP access control list settings.

Syntax

show snmp acl-info

Parameters

None

Example

```
amnesiac > show snmp acl-info
Security Names
--------------
Security name                    Community string         Source address
-------------                    ----------------         --------------
There are no configured security names
Groups
------
Group name                       Security model   Security name
----------                       --------------   -------------
There are no configured groups
Views
-----
There are no configured views
Access control lists
---------------------
Group name                       Security level Read view
----------                       -------------- -------------
```

Product

Interceptor appliance, Steelhead appliance

Related Topics

"SNMP Commands"

show snmp ifindex

Description

Displays the ifindex values for all interfaces.

Syntax

show snmp ifindex

Parameters

None

Example

```
amnesiac > show snmp ifindex
Interface    Ifindex
-----------------------
      aux    1
     eth0    6
     eth1    7
     eth2    8
     eth3    9
     eth4    10
     eth5    11
     eth6    12
     eth7    13
       lo    5
  primary    2
```

Product

Interceptor appliance, Steelhead appliance

Related Topics

"SNMP Commands"

show snmp usernames

Description

Displays SNMP user settings.

Syntax

show snmp usernames

Parameters

None

Example

```
amnesiac > show snmp usernames

Username            Authentication Protocol  Authentication Key
There are no configured users
```

Product

Interceptor appliance, Steelhead appliance

Related Topics

"SNMP Commands"

show ssh client

Description

Displays the client settings.

Syntax

show ssh client [private]

Parameters

private	Display SSH client public and private keys.

Example

```
amnesiac > show ssh client
SSH server enabled: yes
```

Product

CMC Appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Secure Shell Access Commands"

show ssh server

Description

Displays the ssh server.

Syntax

show ssh server [allowed-ciphers | publickey]

Parameters

allowed-ciphers	Display SSH server allowed ciphers.
publickey	Display SSH server-public host key.

Example

```
amnesiac > show ssh server publickey
SSH server public key: ssh-rsa AAAAB3NzaC1yc2XXXXXXXwAAAQEAwz7zKAc1NbTKSp40mRg7J
9YV5CeoGRQoCEPS17ValtEQbepaQygdifueiejht39837482y74982u7ridejbvgiIYZs/E23zmn212kj
dXFda8zJxJm07RIKOxNDEBUbAUp8h8dkeiejgfoeoriu39438598439gfjeNLfhjWgh1dzeGYycaAoEA
K21Igg+Sg0ELGq2cJ8mMzsSsCq5PnOmj63RAMuRgBdrtBdIAd32fy642PQJveqtfl7MBN6IwTDECRpex
F3Ku98pRefc2h0u44VZNT9h4tXCe8qHpuO5k98oA

amnesiac > show ssh server allowed-ciphers
SSH server allowed ciphers:
---------------------------
aes128-ctr
aes192-ctr
aes256-ctr
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Secure Shell Access Commands"

show stats bandwidth

Description

Displays the bandwidth statistics.

Syntax

show stats bandwidth {[<port> | all] [bi-directional |lan-to-wan | wan-to-lan] [1min | 5min | hour | day | week | month]}

Parameters

<port> | all	Specify all ports or a specified port.
bi-directional | lan-to-wan | wan-to-lan	Specify the traffic type.
1min | 5min | hour | day | week | month	Specify the time period.

Example

```
amnesiac > show stats bandwidth all lan-to-wan hour
WAN Data:                  0 Bytes
LAN Data:                  0 Bytes
Data Reduction:            0%
Data Reduction Peak:       0%
Data Reduction Peak Time:
Capacity Increase:         1X
```

Product

Steelhead appliance

Related Topics

"System Administration and Service Commands"

show stats conn-pool

Description

Displays the connection pooling statistics.

Syntax

show stats conn-pool {1min | 5min | hour | day | week | month}

Parameters

1min | 5min | hour | day | week | month	Specify the time period.

Example

```
amnesiac > show stats conn-pool week
Total Connection Pool:              0
Connection Hit :                    0
Connection Hit Ratio:
```

Product

Steelhead appliance

Related Topics

"Connection Pooling Commands"

show stats connections

Description

Displays connection statistics.

Syntax

show stats connections {1min | 5min | hour | day | week | month}

Parameters

1min | 5min | hour | day | week | month	Specify the time period.

Example

```
amnesiac > show stats connections hour
Avg Total Optimized:   0
Peak Total Optimized:  0 (2008/10/17 17:26:23)
   Avg Established:    0
   Peak Established:   0 (2008/10/17 17:26:23)
   Avg Half Opened:    0
   Peak Half Opened:   0 (2008/10/17 17:26:23)
   Avg Half Closed:    0
   Peak Half Closed:   0 (2008/10/17 17:26:23)
Avg Active Optimized:  0
Peak Active Optimized: 0 (2008/10/17 17:26:23)
Avg Pass Through:      0
Peak Pass Through:     0 (2008/10/17 17:26:23)
Avg Forwarded:         0
Peak Forwarded:        0 (2008/10/17 17:26:23)
```

Product

Steelhead appliance

Related Topics

"Connection Pooling Commands"

show stats cpu

Description

Displays connection pooling statistics.

Syntax

show stats cpu

Parameters

None

Example

```
amnesiac > show stats cpu
CPU 1
  Utilization:                3%
  Peak Utilization Last Hour: 10% at 2008/10/17 18:10:03
  Avg. Utilization Last Hour: 4%

CPU 2
  Utilization:                7%
  Peak Utilization Last Hour: 9% at 2008/10/17 17:43:13
  Avg. Utilization Last Hour: 4%
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"show stats memory"

show stats datastore

Description

Displays data store statistics.

Syntax

show stats datastore [1min | 5min | hour | day | week | month]

Parameters

1min | 5min | hour | day | week | month	Specify the time period.

Example

```
amnesiac > show stats datastore hour
Total Hits: 0
Misses:     0
```

Product

Steelhead appliance

Related Topics

"Data Store Configuration Commands"

show stats dns

Description

Displays the DNS statistics.

Syntax

show stats dns {1min | 5min | hour | day | week | month}

Parameters

1min | 5min | hour | day | week | month	Specify the time period.

Example

```
amnesiac > show stats dns hour
Total Requests:             0
Cache Hit Rate:             0%
Average Cache Entries:      0
Average Cache Usage:        0 Bytes
```

Product

Steelhead appliance

Related Topics

"DNS Cache Commands"

show stats ecc-ram

Description

Displays the ECC error counts.

Syntax

show stats ecc-ram

Parameters

None

Example

```
amnesiac > show stats ecc-ram
No ECC memory errors have been detected
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"show stats memory"

show stats fan

Description

Displays the fan statistics.

Syntax

show stats fan

Parameters

None

Example

```
amnesiac > show stats fan
FanId    RPM      Min RPM Status
1        3825     750     ok
2        3750     750     ok
```

Product

CMC, Interceptor appliance, Steelhead appliance

Related Topics

"show hardware error-log"

show stats http

Description

Displays HTTP statistics.

Syntax

show stats http

Parameters

None

Example

```
amnesiac > show stats http
---HTTP Prefetch Stats---
   Objects Requested:           0

   Parse-and-Prefetch Hits:     0
   Metadata Hits:               0
   URL Learning Hits:           0

   Total Hits:                  0
   Total Misses:                0

   Parse-and-Prefetch Hit %:    0.000000
   Metadata Hit %:              0.000000
   URL Learning Hit %:          0.000000

   Total Hit %:                 0.000000
```

Product

Steelhead appliance

Related Topics

"HTTP Support Commands"

show stats memory

Description

Displays memory statistics.

Syntax

show stats memory

Parameters

None

Example

```
amnesiac > show stats memory
Total Swapped Over Last Hour:          0 pages
Average Swapped Over Last Hour:        0 pages
Peak Swapped Over Last Hour:           0 pages
Peak Swapped Time:                     2008/10/17 17:37:41
```

Product

Steelhead appliance

Related Topics

"show stats ecc-ram"

show stats neighbor-fwd

Description

Displays connection forwarding statistics. For detailed information about alarms, see the *Steelhead Appliance Management Console User's Guide*.

Syntax

show stats neighbor-fwd {[<port> | all] [packet | byte] [1min | 5min | hour | day | week | month]}

Parameters

<port> | all	Specify all ports or a specified port.
packet | byte	Specify the data type.
1min | 5min | hour | day | week | month	Specify the time period.

Example

```
amnesiac > show stats neighbor-fwd packet hour

Total Sent:          0 packets
Data Sent Peak:      0 packets
Data Sent Peak Time: 2008/10/17 17:42:20
```

Product

Steelhead appliance

Related Topics

"Connection Forwarding"

show stats nfs

Description

Displays connection forwarding statistics. For detailed information about alarms, see the *Steelhead Appliance Management Console User's Guide*.

Syntax

show stats nfs {[<port> | all] [1min | 5min | hour | day | week | month]}

Parameters

<port> | all	Specify all ports or a specified port.
1min | 5min | hour | day | week | month	Specify the time period.

Example

```
amnesiac > show stats nfs all week
Locally Served:                 0 calls
Remotely Served:                0 calls
Delay Response:                 0 calls
Data Reduction:                 0%
Data Reduction Peak:            0%
Data Reduction Peak Time:       2009/09/09 14:34:23
Capacity Increase:              1X
```

Product

Steelhead appliance

Related Topics

"NFS Support Commands"

show stats pfs

Description

Displays PFS statistics.

Syntax

show stats pfs {[<port> | all] [1min | 5min | hour | day | week | month]}

Parameters

<port> | all	Specify all ports or a specified port.
1min | 5min | hour | day | week | month	Specify the time period.

Example

```
amnesiac > show stats pfs all hour
Byte Sent:                      0 Bytes
Data Sent Peak:                 0 Bytes
Data Sent Peak Time:
Byte Recv:                      0 Bytes
Data Recv Peak:                 0 Bytes
Data Recv Peak Time:
```

Product

Steelhead appliance

Related Topics

"PFS Support Commands"

show stats protocol srdf

Description

Displays SRDF protocol statistics for a specified time period.

Syntax

show stats protocol srdf [symm id <symm-id>] [rdf-group <rdf-group>] [total] {interval <interval-time> | start-time <"YYYY/MM/DD HH:MM:SS"> end-time <"YYYY/MM/DD HH:MM:SS">}

Parameters

symm id <symm-id>	Specify a Symmetrix ID. The Symmetrix ID is an alpha-numeric string (for example, a standard Symmetrix serial number : 000104900363).
rdf-group <rdf-group>	Specify a Symmetrix RDF group. The RDF number can begin with either a 0 or 1. The default value is 1. The maximum number of RDF groups is 254.
total	Displays the total bytes transferred instead of throughput.
interval <time-interval>	Specify the time interval. Choices are the most recent: • 1min • 5min • hour • day • week • month Statistics are refreshed, periodically, as specified by the time interval.
start-time <YYYY/MM/DD HH:MM:SS>	Specify the start time to collect SRDF statistics. Use the format "YYYY/MM/DD HH:MM:SS" (enclosed in double quotes).
end-time <YYYY/MM/DD HH:MM:SS>	Specify the end time to stop collecting SRDF statistics. Use the format "YYYY/MM/DD HH:MM:SS" (enclosed in double quotes).

Usage

EMC Symmetrix Remote Data Facility/Asynchronous (SRDF/A) is a SAN replication product. It carries out data replication over GigE instead of Fibre Channel, using gateways that implement the SRDF protocol.

RiOS v6.1 and later SRDF storage optimization provides support for environments using storage technology that originates traffic through Symmetrix GigE ports.

To increase the data reduction LAN-to-WAN ratio with either equal or greater data throughput in environments with SRDF traffic, RiOS separates the SRDF headers from the application data workload written to storage. The SRDF headers contain changing protocol state information, such as sequence numbers. These headers interrupt the network stream and reduce the ability of SDR to match large, contiguous data patterns. After isolating the header data, the Steelhead appliance performs SDR network deduplication on the larger, uninterrupted storage data workload and LZ compression on the headers. RiOS then optimizes, reassembles, and delivers the data to the TCP consumer without compromising data integrity.

The **show stats protocol srdf** command displays SRDF statistics such as average throughput, the total amount of LAN and WAN traffic, the amount of data reduction after optimization, and the peak LAN and WAN data transfer.

Example

The following example shows throughput statistics for all Symmetrix IDs:

```
amnesiac > show stats protocol srdf interval week
Array                LAN Tput (Kbps)    WAN Tput (Kbps)    Rdxn   Cap Incr
-------------------- ------------------ ------------------ ------ ---------
myfooserver          79.7               0.7                99.18% 121.00X
                     Peak LAN Tput: 377,410.6 Kbps at 11:00:00 on 2011/09/30
                     Peak WAN Tput: 3,073.7 Kbps at 11:00:00 on 2011/09/30
```

The following example shows output for the total bytes transferred:

```
amnesiac > show stats protocol srdf total interval week
Array                Total LAN KB Total WAN KB Rdxn         Cap Incr
-------------------- ------------ ------------ ------------ ------------
myfooserver          6,027,666    49,418       99.18%       121.00X
                     Peak LAN transfer: 707,644 KB at 11:00:00 on 2011/09/30
                     Peak WAN transfer: 5,763 KB at 11:00:00 on 2011/09/30
```

The following example shows the output for the start-time/end-time format:

```
amnesiac > show stats protocol srdf symm id 6000000060 start-time "2011/11/04 16:17:00" end-time
"2011/11/11 15:17:00"

Array                RDF Group  LAN Tput (Kbps)    WAN Tput (Kbps)    Rdxn
-------------------- ---------- ------------------ ------------------ ------
6000000060           1          2,142.3            2,177.7            -1.65%
                     Peak LAN Tput: 57,005.0 Kbps at 09:00:00 on 2011/11/10
                     Peak WAN Tput: 57,901.5 Kbps at 09:00:00 on 2011/11/10

6000000060           2          2,142.3            412.4              80.75%
                     Peak LAN Tput: 56,982.9 Kbps at 09:00:00 on 2011/11/10
                     Peak WAN Tput: 10,970.0 Kbps at 09:00:00 on 2011/11/10

6000000060           3          2,142.3            20.1               99.06%
                     Peak LAN Tput: 56,993.5 Kbps at 09:00:00 on 2011/11/10
                     Peak WAN Tput: 2,736.1 Kbps at 16:00:00 on 2011/11/07

6000000060           Total      21,423.0           2,751.8            87.16%
                     Peak LAN Tput: 569,949.3 Kbps at 09:00:00 on 2011/11/10
                     Peak WAN Tput: 72,609.9 Kbps at 09:00:00 on 2011/11/10
```

Product

Steelhead appliance

Related Topics

"SRDF Support Commands"

show stats qos-inbound

Description

Displays QoS inbound statistics.

Syntax

show stats qos-inbound {all | unknown | <default-class-name>} {packet | byte} <time-period>

Parameters

all	Displays all ports.
unknown	Displays statistics for a class or classes that are no longer configured on the system. For example, if you deleted a class, the statistics for that class are still displayed.
<default-class-name>	Displays statistics for the default class. Traffic classification options are: • **Default-Site$$Business-Critical** • **Default-Site$$Interactive** • **Default-Site$$Low-Priority** • **Default-Site$$Normal** • **Default-Site$$Realtime** • **Default-Site$$Best-effort** • **Default-Site$$parent_class**
packet	Displays the packet count.
byte	Displays the byte count.
<time-period>	Displays statistics for the specified time period: • **1min** - Displays statistics for the last 1 minute. • **5min** - Displays statistics for the last 5 minutes. • **hour** - Displays statistics for the last 1 hour. • **day** - Displays statistics for the last day. • **week** - Displays statistics for the last week. • **month** - Displays statistics for the last month.

Example

```
amnesiac > show stats qos-inbound all packet 5min
Class Name                                  Total Sent          Total Dropped

Default                                     0 packets            0 packets

All Classes (cumulative)                    0 packets            0 packets
```

Product

Steelhead appliance

Related Topics

"Inbound QoS Commands"

show stats qos-outbound

Description

Displays outbound QoS statistics for the specified time period.

Syntax

show stats qos-outbound {all | unknown |<default-class-name>} {packet | byte} <time-period>

Parameters

all	Displays all ports.
unknown	Displays statistics for a class or classes that are no longer configured on the system. For example, if you deleted a class, the statistics for that class are still displayed.
<default-class-name>	Displays statistics for the default class. Traffic classification options are: • **Default-Site$$Business-Critical** • **Default-Site$$Interactive** • **Default-Site$$Low-Priority** • **Default-Site$$Normal** • **Default-Site$$Realtime** • **Default-Site$$Best-effort** • **Default-Site$$parent_class**
packet	Displays the packet count.
byte	Displays the byte count.
<time-period>	Displays statistics for the specified time period: • **1min** - Displays statistics for the last 1 minute. • **5min** - Displays statistics for the last 5 minutes. • **hour** - Displays statistics for the last 1 hour. • **day** - Displays statistics for the last day. • **week** - Displays statistics for the last week. • **month** - Displays statistics for the last month.

Example

```
amnesiac > show stats qos-outbound all packet 5min
Class Name                               Total Sent          Total Dropped

Default-Site$$Best-Effort                0 packets            0 packets
Default-Site$$Business-Critical          0 packets            0 packets
Default-Site$$Interactive                0 packets            0 packets
Default-Site$$Low-Priority               0 packets            0 packets
Default-Site$$Normal                     0 packets            0 packets
Default-Site$$Realtime                   0 packets            0 packets
Default-Site$$parent_class               0 packets            0 packets
All Classes (cumulative)                 0 packets            0 packets
```

Product

Steelhead appliance

Related Topics

"Advanced Outbound QoS Commands"

show stats rsp

Description

Displays RSP statistics.

Syntax

show stats rsp {[all-opt-vnis | opt-vni <vin-name>] [side lan | wan | package] [period 1min | 5min | hour | day | week | month]}

Parameters

all-opt-vnis	Displays RSP statistics for all virtual network interfaces (VNIs).
opt-vni <vni>	Displays RSP VNI statistics for the specified VNI, for example RiOS.
side lan | wan | package	Displays the statistics for the specified interface. For example, the WAN side.
period 1min | 5min | hour | day | week | month	Specify the time period.

Example

```
amnesiac > show stats rsp all-opt-vnis period hour
VNI: RiOS 0_0 Interface: lan
Bytes in:                 0    Packets in:               0
Bytes out:                0   Packets out:              0

VNI: RiOS 0_0 Interface: wan
Bytes in:                 0   Packets in:               0
Bytes out:                0   Packets out:              0

VNI: RiOS 0_0 Interface: package
Bytes in:                 0   Packets in:               0
Bytes out:                0   Packets out:              0
```

Product

Steelhead appliance

Related Topics

"RSP Commands"

show stats settings app-vis

Description

Displays whether or not the application visibility feature is enabled.

Syntax

show stats settings app-vis

Parameters

None

Usage

Use the **stats settings app-vis enable** command to enable the application visibility feature. See the *Steelhead Appliance Management Console User's Guide* for information about viewing Application Statistics reports.

Example

```
amnesiac > show stats settings app-vis
Application Visibility Enabled: yes
```

Product

Steelhead appliance

Related Topics

"stats settings app-vis enable"

show stats settings bandwidth

Description

Displays settings used to generate statistics.

Syntax

show stats settings bandwidth ports | top-talkers

Parameters

ports	Displays monitored ports.
top-talkers	Displays Top Talker settings.

Example

```
amnesiac > show stats settings bandwidth ports
Monitoring the following ports:
  21    FTP
  80    HTTP
  139   CIFS:NetBIOS
  443   SSL
  445   CIFS:TCP
  1352  Lotus Notes
  1433  SQL:TDS
  7830  MAPI
  8777  RCU
  10566 SnapMirror
```

Product

Steelhead appliance

Related Topics

"Top Talkers Commands," "Statistics Manipulation Commands"

show stats ssl

Description

Displays SSL statistics.

Syntax

show stats ssl {1min | 5min | hour | day | week | month}

Parameters

1min | 5min | hour | day | week | month	Specify a time period.

Example

```
amnesiac > show stats ssl hour
Total Connection Requests:          0 connections
Successful Requests:                0 connections
Failed Requests:                    0 connections
Average Connections/Second:         0 connections per second
Peak Connections/Second:            0 connections per second
Number of Current Connections:      0
tcfe52 >
```

Product

Steelhead appliance

Related Topics

"SSL Support Commands," "Statistics Manipulation Commands"

show stats throughput

Description

Displays throughput statistics.

Syntax

show stats throughput {[<port> | all] [bidirectional | lan-to-wan | wan-to-lan] [1min | 5min | hour | day | week | month]}

Parameters

<port> | all	Specify the all ports or a specified port.
bidirectional | lan-to-wan | wan-to-lan	Specify the traffic type.
1min | 5min | hour | day | week | month	Specify a time period.

Example

```
amnesiac > show stats throughput all lan-to-wan hour
LAN Link Throughput
Average Throughput:          0 bps
95th Percentile Throughput: 0 bps
Peak Throughput:             0 bps
Peak Throughput Time:        2008/10/18 10:56:30


WAN Link Throughput
Average Throughput:          0 bps
95th Percentile Throughput: 0 bps
Peak Throughput:             0 bps
Peak Throughput Time:        2008/10/18 10:56:30
```

Product

Steelhead appliance

Related Topics

"Statistics Manipulation Commands"

show stats top-talkers

Description

Displays top talkers statistics.

Syntax

show stats top-talkers <cr> | [end-time <YYYY/MM/DD HH:MM:SS>] | [start-time <YYYY/MM/DD HH:MM:SS>]

Parameters

end-time <YYYY/MM/DD HH:MM:SS>	Specify the end time period for top talkers. Use the following format: YYYY/MM/DD HH:MM:SS
start-time <YYYY/MM/DD HH:MM:SS>	Specify the start and end time period for top talkers. Use the following format: YYYY/MM/DD HH:MM:SS

Example

```
amnesiac > show stats top-talkers end-time 2008/09/10 05:00:00
```

Product

Steelhead appliance

Related Topics

"Top Talkers Commands"

show stats top-talkers protocol

Description

Displays top talkers protocol statistics.

Syntax

show stats top-talkers protocol {[tcp | udp | both] <cr>] | [start-time <starttime> end-time <endtime>] <cr> | [report [conversation | src_host_only | ignore_ports | dest_host_only | app_port_only]}

Parameters

protocol tcp | udp | both] <cr>]	Displays top talkers for the specified protocol: TCP, UDP, or both.
[start-time <starttime>] | [end-time <endtime>]	Optionally, specify the start and end time. Use the following format: YYYY/MM/DD HH:MM:SS
report [conversation | src_host_only | ignore_ports | dest_host_only | app_port_only]	Display report statistics for the specified protocol. Optionally, specify the start and end time. Use the following format: YYYY/MM/DD HH:MM:SS For detailed information about report types, see "show stats top-talkers report" on page 144.

Example

```
amnesiac > show stats top-talkers protocol tcp start-time 2008/09/09 00:00:00 end-time 2008/09/29
00:00:00
```

Product

Steelhead appliance

Related Topics

"Top Talkers Commands"

show stats top-talkers report

Description

Displays top talkers report statistics.

Syntax

show stats top-talkers {[report conversation <cr>] | dest_host_only <cr> | src_host_only <cr> | ignore_ports <cr> | dest_host_only | app_port_only] <cr> | [start-time <start-time> end-time <end-time>]}

Parameters

report conversation <cr> [start-time <start-time> end-time <end-time>]	Displays top talkers with IP address and ports. Optionally, specify the start and end time. Use the following format: YYYY/MM/DD HH:MM:SS.
dest_host_only <cr> [start-time <start-time> end-time <end-time>]	Display top destinations receiving traffic. Optionally, specify the start and end time. Use the following format: YYYY/MM/DD HH:MM:SS.
src_host_only <cr> [start-time <start-time> end-time <end-time>]	Display top sources generating traffic. Optionally, specify the start and end time. Use the following format: YYYY/MM/DD HH:MM:SS.
ignore_ports <cr> [start-time <start-time> end-time <end-time>]	Displays the top talkers while ignoring ports. Optionally, specify the start and end time. Use the following format: YYYY/MM/DD HH:MM:SS.
dest_host_only <cr> [start-time <start-time> end-time <end-time>]	Displays top destinations receiving traffic. Optionally, specify the start and end time. Use the following format: YYYY/MM/DD HH:MM:SS.
app_port_only <cr> [start-time <start-time> end-time <end-time>]	Display the top applications carrying traffic Optionally, specify the start and end time. Use the following format: YYYY/MM/DD HH:MM:SS.

Example

```
amnesiac > show stats top-talkers report conversation
```

Product

Steelhead appliance

Related Topics

"Top Talkers Commands"

show stats top-talkers top-n

Description

Displays the statistics for the specified number of top talkers.

Syntax

show stats top-talkers top-n <top-number> <cr> | [protocol *] [traffic *] [report *] [start-time *] [end-time *]

Parameters

[start-time <start time> end-time <end time>]	Specify the start time period for top talkers. Use the format: YYYY/MM/DD HH:MM:SS.
[protocol [tcp | udp | both] <cr>] | [report [conversation | src_host_only | ignore_ports | dest_host_only | app_port_only] end-time <endtime> starttime <starttime>]] | [start-time <starttime>] | [end-time <endtime>]]	Specify the protocol type and optionally the report and the start and end time. Use the format for the start and end time: YYYY/MM/DD HH:MM:SS. For details about protocol types, see "show stats top-talkers traffic" on page 146.
[traffic [optimized | pass-through | both] <cr>] | [report [conversation | src_host_only | ignore_ports | dest_host_only | app_port_only] end-time <endtime> starttime <starttime>] | [start-time <starttime> end-time <endtime>]]	Specify the traffic type and optionally the report and the start and end time. Use the format for the start and end time: YYYY/MM/DD HH:MM:SS. For details about traffic types, see "show stats top-talkers traffic" on page 146.
[report [conversation | src_host_only | ignore_ports | dest_host_only | app_port_only] end-time <endtime> starttime <starttime>]]	Specify the report type and optionally the start and end time period for top talkers. Use the format for the start and end time: YYYY/MM/DD HH:MM:SS. For details about report types, see "show stats top-talkers report" on page 144.

Example

```
amnesiac > show stats top-talkers top-n 5 report conversation start-time 2008/09/09 00:00:00 end-
time 2008/09/29 00:00:00
```

Product

Steelhead appliance

Related Topics

"Top Talkers Commands"

show stats top-talkers traffic

Description

Displays top talkers traffic statistics.

Syntax

show stats top-talkers traffic [optimized | pass-through | both] <cr>] | [report {conversation | src_host_only | ignore_ports | dest_host_only | app_port_only} | end-time <endtime> starttime <starttime>]] | start-time <starttime> end-time <endtime>]

Parameters

[optimized | pass-through | both]	Displays top talkers with the specified traffic type: optimized, pass-through, or both. Optionally, specify the start and end time. Use the format: YYYY/MM/DD HH:MM:SS
[report [conversation | src_host_only | ignore_ports | dest_host_only | app_port_only] end-time <endtime> starttime <starttime>]	Display report statistics for the specified protocol. Optionally, specify the start and end time. Use the format: YYYY/MM/DD HH:MM:SS For detailed information about report types, see "show stats top-talkers report" on page 144.
[start-time <starttime> end-time <endtime>]	Displays the top talkers while ignoring ports. Optionally, specify the start and end time. Use the format: YYYY/MM/DD HH:MM:SS

Example

```
amnesiac > show stats top-talkers traffic optimized report conversation start-time 2008/09/09
00:00:00 end-time 2008/09/29 00:00:00
```

Product

Steelhead appliance

Related Topics

"Top Talkers Commands"

show stats traffic optimized

Description

Displays the optimized traffic statistics.

Syntax

show stats traffic optimized {[bi-directional | lan-to-wan | wan-to-lan] [1min | 5min | hour | day | week | month]}

Parameters

bi-directional | lan-to-wan | wan-to-lan	Specify the traffic type.
1min | 5min | hour | day | week | month	Specify the time period.

Example

```
amnesiac > show stats traffic optimized lan-to-wan week
Port                             Rdx%  LAN Data   WAN Data   Trf%
------------------------------- ------ ---------- ---------- ------
Total Traffic                               3 MB     3.7 MB
Lotus Notes (1352)               0.00%      3 MB     3.7 MB 100.00%
```

Product

Steelhead appliance

Related Topics

"Statistics Manipulation Commands"

show stats traffic passthrough

Description

Displays the pass-through traffic statistics.

Syntax

show stats traffic passthrough {1min | 5min | hour | day | week | month}

Parameters

1min | 5min | hour | day | week | month	Specify the time period.

Example

```
amnesiac > show stats traffic passthrough week
Port                             Rdx%  LAN Data   WAN Data   Trf%
------------------------------- ------ ---------- ---------- ------
Total Traffic                            290.7 MB   290.7 MB
Lotus Notes (1352)               0.00%   290.7 MB   290.7 MB 100.00%
```

Product

Steelhead appliance

Related Topics

"Statistics Manipulation Commands"

show subnet side rules

Description

Displays subnet-side rule settings.

Syntax

show subnet side rules

Parameters

None

Example

```
amnesiac > show subnet side rules
Rule Network Prefix     Type
---- ------------------ ----
   1 all                 WAN
```

Product

Steelhead appliance

Related Topics

"Subnet-Side Rule Commands"

show tcp cong-ctrl

Description

Displays TCP congestion control settings.

Syntax

show tcp cong-ctrl

Parameters

None

Example

```
amnesiac > show tcp cong-ctrl
TCP Congestion Control Algorithm:   Standard TCP
```

Product

Steelhead appliance

Related Topics

"tcp cong-ctrl mode"

show tcp highspeed

Description

Displays HS-TCP settings.

Syntax

show tcp highspeed

Parameters

None

Example

```
amnesiac > show tcp highspeed
High Speed TCP enabled: no
```

Product

Steelhead appliance

Related Topics

"High-Speed TCP and Satellite Optimization Commands"

show tcp max-time-out

Description

Displays time-out settings for TCP connections.

Syntax

show tcp max-time-out

Parameters

None

Example

```
amnesiac > show tcp max-time-out
TCP max-time-out mode enabled: no
Maximum time out value for TCP connections: 1800 secs
```

Product

Steelhead appliance

Related Topics

"tcp connection send keep-alive"

show tcp rate-pacing status

Description

Displays whether the TCP rate pacing mechanism is enabled or disabled.

Syntax

show tcp rate-pacing status

Parameters

None

Example

```
amnesiac > show tcp rate-pacing status
Enabled: yes
```

Product

Steelhead appliance

Related Topics

"tcp rate-pacing enable"

show tcp reordering

Description

Displays TCP reordering information.

Syntax

show tcp reordering

Parameters

None

Example

```
amnesiac > show tcp reordering
TCP reordering enabled:   no
TCP reordering threshold: 3
```

Product

Steelhead appliance

Related Topics

"tcp connection send reset"

show tcp sack

Description

Displays the TCP selective acknowledgement setting.

Syntax

show tcp sack

Parameters

None

Example

```
amnesiac > show tcp sack
TCP Selective Acknowledgment Enabled: yes
```

Product

Steelhead appliance

Related Topics

"tcp connection send reset"

show tcp sat-opt scps legacy-comp

Description

Displays SkipWare legacy compression settings.

Syntax

show tcp sat-opt scps legacy-comp {process-batch | queuing-delay}

Parameters

process-batch	Displays the maximum number of packets to process before yielding to the processor.
queuing-delay	Displays the maximum number of packets that are in the queue for module processing.

Example

```
amnesiac > show tcp sat-opt scps legacy-comp process-batch
Max number of packets to process: 25
```

```
amnesiac > show tcp sat-opt scps legacy-comp queuing-delay
Max queuing delay of packets: 1500
```

Product

Steelhead appliance

Related Topics

"tcp sat-opt scps legacy-comp process-batch," "tcp sat-opt scps legacy-comp queuing-delay"

show tcp sat-opt scps rules

Description

Displays the SCPS rules.

Syntax

show tcp sat-opt scps rules

Parameters

None

Example

```
amnesiac > show tcp sat-opt scps rules

 Rule Source Addr             Dest Addr               Port           VLAN S P R C
----- ----------------------- ----------------------- -------------- ---- - - - -
    1 all-ipv4                all-ipv4                all            all  Y N N C
    2 all-ip                  all-ip                  Interactive    all  N Y N C
    3 all-ip                  all-ip                  RBT-Proto      all  N Y N C
    4 all-ip                  all-ip                  all            all  Y Y N E
  def all-ip                  all-ip                  all            all  Y Y N C
```

```
----- ----------------------- ----------------------- -------------- ---- - - - -

4 user-defined rule(s)

(S) SCPS setting:            Y=Allow SCPS  N=SCPS Bypass
(P) Allow only SCPS peering: Y=Enabled  N=Disabled
(R) Rate-Pacing:             Y=Enabled  N=Disabled
(C) Congestion Control:      B=BW-EST C=PER-CONN-TCP E=ERR-TOL-TCP
                             H=HSTCP  D=STANDARD (RFC-COMPLIANT)
```

Product

Steelhead appliance

Related Topics

"High-Speed TCP and Satellite Optimization Commands"

show tcp sat-opt settings

Description

Displays the satellite optimization TCP SCPS configuration.

Syntax

show tcp sat-opt settings

Parameters

None

Example

```
amnesiac > show tcp sat-opt settings
Bandwidth Estimation Mode: refl-peer
SCPS Table Enabled: no
```

Product

Steelhead appliance

Related Topics

"High-Speed TCP and Satellite Optimization Commands"

show tcpdump stop-trigger

Description

Displays the configuration settings that trigger the stop of a TCP dump.

Syntax

show tcpdump stop-trigger

Parameters

None

Example

```
amnesiac > show tcpdump stop-trigger
Tcpdump trigger enabled: no
Regex: ntp
Delay: 10
Last triggered on: 2013/01/12 17:33:52
Last triggered by: ntp
```

Product

Steelhead appliance, CMC Appliance

Related Topics

"tcpdump stop-trigger delay," "tcpdump stop-trigger enable," "tcpdump stop-trigger regex," "tcpdump stop-trigger restart,"

show tcpdump-x

Description

Displays currently running tcpdumps.

Syntax

show tcpdump-x

Parameters

None

Example

```
amnesiac > show tcpdump-x
No running capture
```

Product

Steelhead appliance, CMC Appliance, Steelhead Mobile Controller, Interceptor appliance

Related Topics

"RiOS TCP Dump Commands"

show terminal

Description

Displays terminal settings.

Syntax

show terminal

Parameters

None

Example

```
amnesiac > show terminal
CLI current session settings
  Terminal width:     80 columns
  Terminal length:    24 rows
  Terminal type:      xterm
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"CLI Terminal Configuration Commands"

show uploads

Description

Displays system dump files uploaded to Riverbed Technical Support.

Syntax

show uploads

Parameters

None

Usage

The **show uploads** command shows the system dump files that have been uploaded to Riverbed Technical Support or are in progress. The display shows up to 100 upload statistics, includes whether the upload is completed or in progress, and shows whether or not an error occurred during the upload process. You can clear the upload statistics using the **file upload clear-stats** command.

Example

```
amnesiac > show uploads

Upload 0:
file: /var/opt/tms/tcpdumps/bravo-sh236_aux_new.cap0
url: ftp://ftp.riverbed.com/incoming/case_194170_F82JY00002BE4_bravo-sh236_aux_new.cap0
status: finished
percent complete: 100%
start time: 2013/03/25 12:16:40 -0700
finish time: 2013/03/25 12:16:41 -0700
```

Product

Steelhead appliance

Related Topics

"file upload clear-stats," "RiOS TCP Dump Commands"

show version

Description

Displays the installed software version, including build number.

Syntax

show version [all | concise | history]

Parameters

all	Displays version information for the current system image. This option displays the product release and the RiOS version.
concise	Displays the installed software version without build information.
history	Displays upgrade version history.

Example

```
amnesiac >  show version
Product name:      rbt_sh
Product release:   7.0.2
Build ID:          #0
Build date:        2012-02-15 16:36:45
Build arch:        x86_64
```

```
Built by:          root@moscow.nbttech.com
Uptime:            15d 19h 40m 38s
Product model:
System memory:     208 MB used / 3681 MB free / 3890 MB total
Number of CPUs:    4
CPU load averages: 0.02 / 0.03 / 0.00

amnesiac >  show version all
Product release:   1.0.1
RiOS release:      rbt_sh 7.0.2 #202_101 2012-02-15 10:16:14 x86_64 root@basel:s
vn://svn/mgmt/branches/release_branch
Build ID:          #202_101
Build date:        2012-02-15 14:22:27
Build arch:        x86_64
Built by:          root@basel

Uptime:            14h 13m 5s

Product model:     EX760
System memory:     5329 MB used / 10681 MB free / 16010 MB total
Number of CPUs:    4
CPU load averages: 0.36 / 0.40 / 0.32
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"image fetch," "image install"

show wccp

Description

Displays WCCP settings.

Syntax

show wccp

Parameters

None

Example

```
amnesiac > show wccp
WCCP Support Enabled: no
WCCP Multicast TTL: 1
Service Groups(s):
91:
Protocol: tcp
Priority: 200
Password:
Encapsulation Scheme: either
Assignment Scheme: hash
Weight: 1
Flags: dst-ip-hash, src-ip-hash
Router(s):
1.1.1.1
amnesiac > show wccp
WCCP Support Enabled: no
WCCP Multicast TTL: 1
Service Groups(s):
91:
Protocol: tcp
```

```
Priority: 200
Password:
Encapsulation Scheme: either
Assignment Scheme: mask
Source IP Mask: 0x1741
Destination IP Mask: 0x0
Source Port Mask: 0x0
Destination Port Mask: 0x0
Router(s):
1.1.1.1
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

"WCCP Support Commands"

show wccp interface service-group

Description

Displays WCCP settings for the specified interface and service group.

Syntax

show wccp interface <interface> service-group <service-id> [detail]

Parameters

<interface>	Specify the interface (i.e., **inpath0_0**).
<service-id>	Specify the WCCP group number.
detail	Optionally, displays detailed information about the service group.

Usage

With multi-inpath WCCP, any interface can participate in WCCP and different interfaces can be in different service groups. Therefore, the interface must be specified.

This command is the most useful troubleshooting command for WCCP status and supports multi-inpath WCCP. It provides the following information:

- what redirection, return, and assignment methods have been negotiated between the Steelhead appliance and the WCCP routers.
- whether the **wccp override-return route-no-gre command** is in use (displayed as WCCP Return via Gateway Override).
- if the Steelhead appliance is receiving WCCP control messages from the router (*I-see-you* messages).
- details the load distribution for either mask or hash assignment.

Example

```
amnesiac > show wccp interface inpath0_0 service-group 91
WCCP Support Enabled:       no
WCCP Multicast TTL:         1
WCCP Return Path Override:  no
   Service Group 91 on inpath0_0:
      Protocol:                        tcp
      Priority:                        200
      Password:                        <no password>
      Encapsulation Requested:         l2
      Assignment Requested:            either
      Source IP Mask:                  0x1741
      Destination IP Mask:             0x0
      Source Port Mask:                0x0
      Destination Port Mask:          0x0
      Weight:                         120
      Hash Flags:                     dst-ip-hash, src-ip-hash
      Router IP Address:              1.1.1.1
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

"WCCP Support Commands"

show web

Description

Displays current Web settings.

Syntax

show web

Parameters

None

Example

```
amnesiac > show web
web-based management console enabled:
   HTTP enabled: yes
   HTTP port: 80
   HTTPS enabled: yes
   HTTPS port: 443
   Inactivity timeout: 15 minutes
   Session timeout: 60 minutes
   Session renewal threshold: 30 minutes
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Web Configuration Commands"

show web prefs

Description

Displays the current Web preferences.

Syntax

show web prefs

Parameters

None

Example

```
amnesiac > show web prefs
Log:
Lines Per Page: 100
```

Product

Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"Web Configuration Commands"

show workgroup account

Description

Displays the current workgroup account settings.

Syntax

show workgroup account

Parameters

None

Example

```
amnesiac > show workgroup account
```

Product

Steelhead appliance

Related Topics

"Job Commands"

show workgroup configuration

Description

Displays the current workgroup configuration settings.

Syntax

show workgroup configuration

Parameters

None

Example

```
amnesiac > show workgroup configuration
```

Product

Steelhead appliance

Related Topics

"Job Commands"

show workgroup status

Description

Displays the current workgroup status settings.

Syntax

show workgroup status

Parameters

None

Example

```
amnesiac > show workgroup status
```

Product

Steelhead appliance

Related Topics

"Job Commands"

CHAPTER 3

Enable-Mode Commands

This chapter is a reference for enable-mode commands. It includes the following sections:

- "System Administration Commands" on page 161
- "Displaying System Data" on page 176

You can perform basic system administration tasks in enable mode. Only administrator users can perform enable-mode commands. All commands available in user mode are also available in enable mode.

Chapter 4, "Configuration-Mode Commands" describes some enable commands because they are more easily understood in relationship to the feature set of which they are a part. For example, the "in-path asym-route-tab flush" and the "in-path asym-route-tab remove" commands are described with the in-path asymmetric routing commands. The usage section for these enable-mode commands remind you that you can also access these commands while in enable mode.

To enter enable mode

1. Connect to the CLI and enter the following command:

```
login as: admin
Riverbed Steelhead
Last login: Wed Jan 20 13:02:09 2012 from 10.0.1.1
gen1-sh139 > enable
gen1-sh139 #
```

To exit enable mode, enter **exit**. For information about the **exit** command, see "exit" on page 10.

System Administration Commands

This section describes the system administration commands that are available in enable mode.

For debugging commands, see "Debugging Commands" on page 726.

clear arp-cache

Description

Clears dynamic entries from the ARP cache. This command does not clear static entries.

Syntax

clear arp-cache

Parameters

None

Example

```
amnesiac # clear arp-cache
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

“show arp”

clear hardware error-log

Description

Clears IPMI System Event Log (SEL).

Syntax

clear hardware error-log

Parameters

None

Usage

The amber LED light stops blinking on the system.

Example

```
amnesiac # clear hardware error-log
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

“show hardware error-log”

clear interface

Description

Sets the interface counters for the specified interface to **0**.

Syntax

clear interface {<interface name>}

Parameters

<interface name>	Specify the interface name: **aux**, **primary**, **lo**, **wan1_1**, **lan1_1**, **wan1_0**, **lan1_0**, **inpath1_0**, **inpath1_1**, **all**

Example

```
amnesiac # clear interface aux
```

Product

Steelhead appliance, Steelhead EX appliance, Interceptor appliance

Related Topics

“show interfaces”

clock set

Description

Sets the system date and time.

Syntax

clock set {<yyyy/mm/dd>/<hh:mm:ss>}

Parameters

<yyyy/mm/dd>/<hh:mm:ss>	Specify the date and time (year, month, day, hour, minutes, and seconds).

Example

```
amnesiac # clock set 2003/12/31 23:59:59'
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show clock"

configure terminal

Description

Enables configuration from the terminal by entering the configuration subsystem. You must execute the "enable" command first to enter configuration mode.

Syntax

[no] configure terminal

Parameters

None

Usage

To exit the configuration subsystem, type **exit**.

The **no** command option disables the terminal configuration.

Example

```
amnesiac # configure terminal
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show terminal," "show connection"

disable

Description

Exits enable mode.

Syntax

disable

Parameters

None

Example

```
amnesiac # disable
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"exit"

file sa delete

Description

Delete a system activity report (SAR) log file.

Syntax

file sa delete <filename>

Parameters

<filename>	Specify the filename for the SAR file.

Example

```
amnesiac # file sa delete 2007.12.18.23.54.sar
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"show files sa," "show files stats"

file sa generate

Description

Generates a system activity report (SAR) log file.

Syntax

file sa generate

Parameters

None

Example

```
amnesiac # file sa generate
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"show files sa," "show files stats"

file sa upload

Description

Uploads a system activity report (SAR) log file to a remote host.

Syntax

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

Parameters

<filename>	Specify the name of the file to upload.
<URL or scp://username:password@hostname/path/filename>	Specify the destination of the file in URL or scp format.

Example

```
amnesiac # file sa upload 2007.12.18.23.54.sar http://www.riverbed.com/support
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"show files sa," "show files stats"

file stats delete

Description

Deletes the statistics file.

Syntax

file stats delete <filename>

Parameters

<filename>	Specify the name of the file to delete.

Example

```
amnesiac # file stats delete throughput
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show files stats"

file stats move

Description

Renames the statistics file.

Syntax

file stats move <source filename> <destination filename>

Parameters

<source filename>	Specify the source file to rename.
<destination filename>	Specify the new filename.

Example

```
amnesiac # file stats move throughput throughput2
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Steelhead Mobile Controller

Related Topics

"show files stats"

file stats upload

Description

Uploads the statistics report file to a remote host.

Syntax

file stats upload <filename>
{<URL, **scp://**, or **ftp://username:password@hostname/path/filename> | <case-number>}**

Parameters

<filename>	Specify the source filename to upload.
<URL, **scp://**, or **ftp://username:password@hostname/path/filename>**	Specify the upload protocol, the location, and authentication credentials for the remote file.
<case-number>	Specify the customer case number. This upload method provides a convenient and intuitive way to upload a statistics report file to Riverbed Technical Support without using a URL. The case number is a numeric string.

Example

```
amnesiac # file stats upload throughput http://www.test.com/stats
amnesiac # file stats upload throughput 194170
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show files stats"

file tcpdump delete

Description

Deletes a TCP dump output file.

Syntax

file tcpdump delete <filename>

Parameters

<filename>	Specify the **tcpdump** file to delete.

Example

```
amnesiac # file tcpdump delete dumpfile
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"debug generate dump," "file tcpdump upload"

file tcpdump upload

Description

Uploads a TCP dump output file.

Syntax

file tcpdump upload <filename>
{ <URL or scp://username:password@hostname/path/filename> |<case-number>}

Parameters

upload <filename> <URL or **scp://username:password@hostname/path/filename>**	Uploads a **tcpdump** output file to a remote host. Specify the upload protocol, the location, and authentication credentials for the remote configuration file.
<case-number>	Specify the customer case number. This upload method provides a convenient and intuitive way to upload a **tcpdump** file to Riverbed Technical Support. Riverbed Technical Support recommends using a case number rather than a URL. The case number is a numeric string.

Example

```
amnesiac # file tcpdump upload dumpfile http://www.test.com/stats
amnesiac # file tcpdump upload dumpfile 194170
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"debug generate dump," "file tcpdump delete"

file upload clear-stats

Description

Clears the file upload statistics.

Syntax

file upload clear-stats

Parameters

None

Usage

The **file upload clear-stats** command clears the statistics displayed by the **show uploads** command.

Example

```
amnesiac > file upload clear-stats
```

Product

CMC, Steelhead appliance, Steelhead EX appliance

Related Topics

"show uploads"

image delete

Description

Deletes the specified software image.

Syntax

image delete <image-filename>

Parameters

<image-filename>	Specify the name of the software image to delete.

Example

```
amnesiac # image delete snkv1.0
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show images," "show bootvar," "show info," "show version"

image delete-all

Description

Deletes all software image files on the disk.

Syntax

image delete-all

Parameters

None

Example

```
amnesiac # image delete-all
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show images," "show bootvar," "show info," "show version"

image fetch

Description

Downloads a software image from a remote host.

Syntax

image fetch <URL, scp://, or ftp://username:password@hostname/path/filename> <image-filename>

Parameters

<URL, **scp://**, or **ftp://username:password@hostname/path/filename>**	Specify the upload protocol, the location, and authentication credentials for the remote image file. Press the Enter key to download the image. The image retains the same name it had on the server.
<image-filename>	Specify a local filename for the image.

Example

```
amnesiac # image fetch http://www.domain.com/v.1.0 version1.0
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"image fetch version," "show bootvar," "show images," "show info," "show version"

image install

Description

Installs the software image onto a system partition.

Syntax

image install <image-filename> <partition>

Parameters

<image-filename>	Specify the software image filename to install.
<partition>	Specify the partition number: **1**, **2**.

Example

```
amnesiac # image install version1.0 2
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show images," "show bootvar," "show info," "show version"

image move

Description

Moves or renames an inactive system image on the hard disk.

Syntax

image move <source-image-name> <new-image-name>

Parameters

<source-image-name>	Specify the name of the software image to move or rename.
<new-image-name>	Specify the new name of the software image.

Example

```
amnesiac # image move www.domain.com/v.1.0 version1.0
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show bootvar," "show images," "show info," "show version"

image upgrade

Description

Installs a system image on the backup boot partition.

Syntax

image upgrade <image-name>

Parameters

<image-name>	Specify the software image filename to install.

Usage

The **image upgrade** command only installs the image on the backup boot partition.

Example

```
amnesiac # image upgrade image187.img
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show bootvar," "show images," "show info," "show version"

ntpdate

Description

Conducts a one-time synchronization with a specified NTP server.

Syntax

ntpdate <ip-addr>

Parameters

<ip-addr>	Specify the NTP server with which to synchronize.

Example

```
amnesiac # ntpdate 10.10.10.1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show ntp"

reload

Description

Reboots the system.

Syntax

reload [clean [halt] | halt | force]

Parameters

clean	Clears the datastore, then reboots or shuts down the system.
clean halt	Clears the datastore, then shuts down the system.
halt	Shuts down the system.
force	Forces an immediate reboot of the system even if it is busy.

Example

```
amnesiac # reload
The session will close. It takes about 2-3 minutes to reboot the appliance.
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show connection,""show datastore"

restart

Description

Restarts the optimization service.

Syntax

restart [clean]

Parameters

clean	Restarts the optimization service and clears the data store.

Example

```
amnesiac # restart
Terminating the process....
Relaunching the process
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"show connection,""show datastore"

service enable

Description

Starts the Riverbed service.

Syntax

[no] service enable

Parameters

None

Usage

The **no service enable** command is not persistent across reboots of appliances even if you save the running configuration using the **write memory** command. The service restarts at the next reboot of the appliance.

The **no** command option temporarily disables the optimization service (that is, it disables all the configured in-path IP addresses and ports and the appliance loses its connection to the Management Console) until a **service enable** or **restart** command is issued or a reboot of the appliance occurs.

If you need the service disabled across reboots, use the **no in-path enable** or **no in-path oop enable** commands.

Example

```
amnesiac # service enable
```

Product

Interceptor appliance, Steelhead appliance, Steelhead EX appliance

Related Topics

"show connection," "show datastore"

service error reset

Description

Resets the Steelhead service after a service error.

Syntax

service error reset

Parameters

None

Example

```
amnesiac # service error reset
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"show connection," "show service"

service restart

Description

Restarts the Riverbed service.

Syntax

service restart [clean]

Parameters

clean	Restarts the optimization service and clears the data store.

Example

```
amnesiac # service restart
```

Product

Interceptor appliance, Steelhead appliance, Steelhead EX appliance

Related Topics

“show connection,” “show service”

stats clear-all

Description

Clears data for all samples, computed history data points (CHDs), and status for all alarms.

Syntax

stats clear-all

Parameters

None

Example

```
amnesiac # stats clear-all
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

“show alarm,” “show alarms”

stats convert

Description

Converts statistical data from one storage format to another.

Syntax

stats convert <format>

Parameters

<format>	Specify the storage format: • **1** - Storage 1 version • **2** - Storage 2 version

Example

```
amnesiac # stats convert 2
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show alarm," "show alarms"

tcpdump

Description

Executes the tcpdump utility. You can quickly diagnose problems and take traces for Riverbed Support. The **tcpdump** command takes the standard Linux options. For detailed information, see the Linux man page.

Syntax

tcpdump [<options>] [<filter string>]

Parameters

<options>	The tcpdump command takes the standard Linux options: **-a** Attempt to convert network and broadcast addresses to names. **-c** Exit after receiving count packets. **-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). **-e** Print the link-level header on each dump line. **-E** Use secret algorithm for decrypting IPsec ESP packets. **-f** Print foreign internet 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. **-n** Do not convert addresses, such as host addresses and port numbers to names. **-N** Do not print domain name qualification of hostnames. For example, if you specify this flag, then tcpdump will print nic instead of nic.ddn.mil. **-m** Load SMI MIB module definitions from file module. This option can be used several times to load several MIB modules into tcpdump. **-q** Quiet output. Print less protocol information so output lines are shorter. **-r** Read packets from created with the -w option. **-S** Print absolute, not relative, TCP sequence numbers. **-v** (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. **-w** Write the raw packets to a file rather than parsing and printing them out. They can later be printed with the -r option. Standard output is used if file is **-**. **-x** Print each packet without its link level header in hexi-decimal format. The smaller of the entire packet or bytes will be printed. **-X** When printing hex, print ascii too. Thus if -x is also set, the packet is printed in hex/ascii. This option enables you to analyze new protocols. For detailed information, see the Linux man page.

Usage

Make sure you take separate tcpdumps for the LAN and WAN to submit to Riverbed Support. Make sure you take the tcpdump on the in-path interface.

The most common options are:

-n Do not resolve addresses via DNS

-i <interface> capture on <interface>

To take traces on lanX_Y and wanX_Y, not inpathX_Y:

-e display layer 2 headers, MAC addresses, and VLAN tags

-s <bytes> capture up to <bytes> bytes per packet

The default is 96 bytes; not enough for deep packet inspection for Riverbed Support, instead use:

-s 0 to capture full frames

-w <file> store the trace in <file> (needed when taking traces for offline analysis)

Common Packet Filters

- src host <ip> - source IP address is <ip>
- dst host <ip> - destination IP address is <ip>
- host <ip> - either source or destination is <ip>
- Same for src port, dst port, and port
- Can connect multiple filters together with logical operators: and, or, and not. Use parentheses to override operator precedence. For example:

```
tcpdump -i lan0_0 not port 22
tcpdump -i lan0_0 host 1.1.1.1 and port 2222
tcpdump -i wan0_0 host 3.3.3.3 and (port 4444 or port 5555)
```

Suppose two Steelhead appliances are having a problem optimizing a connection:

```
Client IP = 10.10.10.10
Client SH IP = 10.10.10.20
Server IP = 11.11.11.11
Server SH IP  = 11.11.11.21
```

Take traces on all LAN/WAN interfaces on both Steelhead appliances to diagnose:

```
C-SH# tcpdump -n -i lan0 host 10.10.10.10 and host 11.11.11.11
C-SH# tcpdump -n -i wan0_0 (host 10.10.10.10 and host 11.11.11.11) or (host 10.10.10.20 and
host 11.11.11.21)
S-SH# tcpdump -n -i lan0 host 10.10.10.10 and host 11.11.11.11
S-SH# tcpdump -n -i wan0_0 (host 10.10.10.10 and host 11.11.11.11) or (host 10.10.10.20 and
host 11.11.11.21)
```

Keep the tcpdump running and establish a connection.

If the problem is not obvious, use -w to capture to files, and examine in a tool like Wireshark. Sometimes you can capture very large traces of data and traffic you are interested in is a small subset of the entire trace. To work around this problem, run tcpdump through its own trace to cut down on the number of packets. Use the -r <file> option, to read from a file instead of capture on an interface

```
tcpdump -n -r my_trace.cap -w my_filtered_trace.cap host 5.5.5.5 and port 2323
```

The following example captures both VLAN tagged and untagged traffic on destination port 7850 and ARP packets:

```
tcp -i lan0_0 ((port 7850 or arp) or (vlan and (port 7850 or arp)))
```

Example

```
amnesiac # tcpdump
tcpdump: listening on primary
18:59:13.682568 amnesiac.domain.com.ssh > dhcp-22.domain.com.3277: P 3290808290:3290808342(52) ack
3412262693 win 5840 (DF) [dscp 0x10]
18:59:13.692513 amnesiac.domain.com.ssh > dhcp-22.domain.com.3277: P 0:52(52) ack 1 win 5840 (DF)
[dscp 0x10]
18:59:13.702482 amnesiac.domain.com.ssh > dhcp-22.domain.com.3277: P 0:52(52) ack 1 win 5840 (DF)
[dscp 0x10]
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"RiOS TCP Dump Commands"

tproxytrace

Description

Describes the proxy path in real time.

Syntax

tproxytrace [options] <target_ip:target_port>

Parameters

<target_ip:target_port>	Specify the target IP address and port
[options]	Specify **tproxytrace** options and the target IP address and port: • **-h** - Print this help text • **-i** - Use this interface to send probes on • **-d** - Probe to this depth of proxies • **-s** - Use this source IP address for probes • **-t** - Milliseconds per depth to listen for probe responses • **-o** - TCP option to use for probes

Example

```
amnesiac # tproxytrace 10.0.0.1:124
Probe from 10.11.34.17 (primary) to 10.0.0.1:124
depth 1 timed out
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"show connections"

Displaying System Data

This section describes the **show** commands that require you to be in enable mode. These commands are not available in user mode because the output can include sensitive system administration data such as passwords. This type of data is not available to monitor users; it is only available to administrator users.

Note: All the **show** commands that are available in user mode are available in enable mode.

show aaa

Description

Displays the authentication methods used for log in.

Syntax

show aaa

Parameters

None

Example

```
amnesiac # show aaa
AAA authorization:
    Default User: admin
    Map Order: remote-first
Authentication fallback mode: always fallback
Authentication method(s): for console login
   local
Authentication method(s): for remote login
   local
Per-command authorization method(s):
   local
Per-command accounting method(s):
   local
```

Product

CMC Appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"AAA, Role-Based Management, Radius, and TACACS+ Commands"

show arp

Description

Displays the contents of the ARP cache. The ARP cache includes all statically configured ARP entries, as well as any that the system has acquired dynamically.

Syntax

show arp [static]

Parameters

static	Displays static ARP addresses.

Example

```
amnesiac # show arp
ARP cache contents
IP 10.0.0.1 maps to MAC 00:07:E9:70:20:15
IP 10.0.0.2 maps to MAC 00:05:5D:36:CB:29
IP 10.0.100.22 maps to MAC 00:07:E9:55:10:09
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"clear arp-cache"

show autolicense status

Description

Displays the status of the autolicense client operation.

Syntax

show autolicense status

Parameters

None

Example

```
amnesiac # show autolicense status
Server:       api.licensing.riverbed.com
```

```
Last attempt: 2011/08/18 09:15:46
Successful:   no
Status:       License server unreachable
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"license autolicense enable"

show banner

Description

Displays the banner settings.

Syntax

show banner

Parameters

None

Example

```
amnesiac # show banner
Banners:
    MOTD:
    Issue: Riverbed Interceptor
    Net Issue: Riverbed Interceptor
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"CLI Terminal Configuration Commands"

show cmc

Description

Displays CMC Appliance settings.

Syntax

show cmc

Example

```
amnesiac # show cmc
CMC auto-registration enabled:       yes
CMC auto-registration hostname:      riverbedcmc.nbttech.com
Managed by CMC:                      yes
CMC hostname:                        tsfe7 (10.0.2.2)
Auto configuration status:           Inactive
Last message sent to cmc:            Auto-registration
Time that message was sent:          Thu Nov 13 12:02:25 2008
```

Product

Interceptor appliance, Steelhead appliance, Steelhead EX appliance

Related Topics

"Central Management Console Feature Commands"

show configuration

Description

Displays the current and saved configuration settings that differ from the default settings.

Syntax

show configuration [full]

Parameters

full	Displays all CLI commands and does not exclude commands that set default values.

Example

```
amnesiac # show configuration
##
## Network interface configuration
##
no interface aux dhcp
interface aux duplex "auto"
no interface aux shutdown
interface aux speed "auto"
interface primary ip address 10.0.0.3 /16
##
## Routing configuration
##
ip default-gateway "10.0.0.1"
##
## Other IP configuration
##
hostname "amnesiac"
ip domain-list domain.com
ip domain-list domain.com
ip name-server 10.0.0.2
##
## Logging configuration
##
logging local "info"
##
## Process Manager configuration
##
pm process mgmtd launch timeout "4000"
pm process sport shutdown order "0"
pm process statsd shutdown order "0"
##
## Network management configuration
##
## Miscellaneous other settings (this is a partial list of settings)
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"Configuration File Commands"

show configuration files

Description

Displays the list of active and backup configuration files or the contents of a specified file.

Syntax

show configuration [<filename>]

Parameters

<filename>	Specify a configuration file. The default filesnames are: • **initial** • **initial.bak** • **cold** • **working (active)** • **working.bak**

Example

```
amnesiac # show configuration files initial
##
## Network interface configuration
##
no interface aux dhcp
   interface aux duplex "auto"
   interface aux ip address 10.0.62.75 /16
   interface aux mtu "1500"
no interface aux shutdown
   interface aux speed "auto"
   interface aux txqueuelen "100"
no interface primary dhcp

##
## Routing configuration
##
   ip default-gateway "10.0.0.1"

##
## Logging configuration
##
   logging 10.1.10.200
   logging 10.1.10.200 trap "info"
<<this is a partial display>>
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"Configuration File Commands"

show configuration flash

Description

Displays the flash-enabled RiOS images stored on flash memory.

Syntax

show configuration flash [text]

Parameters

text	Displays the contents of the flash disk text configuration file.

Example

```
amnesiac # show configuration flash
% No backup configuration found on flash disk

amnesiac # show configuration flash text
% No text configuration stored on flash disk
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"Configuration File Commands"

show configuration running

Description

Displays running configuration settings that are different from the defaults.

Syntax

show configuration running [full]

Parameters

running	Displays system CLI commands to recreate current running configuration.
full	Displays all system CLI commands and does not exclude commands that set default values.

Example

```
amnesiac # show configuration running
##
## Network interface configuration
##
no interface aux dhcp
   interface aux duplex "auto"
   interface aux ip address 10.0.62.75 /16
   interface aux mtu "1500"
no interface aux shutdown
   interface aux speed "auto"
   interface aux txqueuelen "100"
no interface inpath0_0 dhcp
   interface inpath0_0 duplex "auto"
   interface inpath0_0 ip address 10.11.62.75 /16
   interface inpath0_0 mtu "1500"
no interface inpath0_0 shutdown
   interface inpath0_0 speed "auto"
   interface inpath0_0 txqueuelen "100"
no interface lan0_0 dhcp
   interface lan0_0 duplex "auto"
   interface lan0_0 mtu "0"
no interface lan0_0 shutdown
   interface lan0_0 speed "auto"
   interface lan0_0 txqueuelen "100"
lines 1-23

##(displays running configuration; this is a partial list of settings.)
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"Configuration File Commands"

show files debug-dump

Description

Displays a list of debug dump files.

Syntax

show files debug-dump [<filename>]

Parameters

<filename>	Displays the content of the specified filename.

Example

```
amnesiac # show files debug-dump
sysinfo-sysdump-amnesiac-20050725-183016.txt
sysdump-amnesiac-20050606-140826.tgz
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"Debugging Commands"

show files process-dump

Description

Displays a list of crash dump files.

Syntax

show files process-dump

Parameters

None

Example

```
amnesiac # show files process-dump
```

Product

CMC Appliance, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"Debugging Commands"

show files sa

Description

Displays Steelhead appliance log files.

Syntax

show files sa [<filename>]

Parameters

<filename>	To display the contents of the log file, specify the filename and press `Enter`.

Example

```
amnesiac # show files sa
2006.05.16.23.53.sar
2006.05.17.23.53.sar
2006.05.18.23.53.sar
2006.05.19.23.53.sar
2006.05.20.23.53.sar
2006.05.21.23.53.sar
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"file sa generate"

show files stats

Description

Displays performance statistics files.

Syntax

show files stats

Parameters

None

Usage

You export performance statistics to files using the **stats export** command.

Example

```
amnesiac # show files stats
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"show stats bandwidth," "stats export"

show files tcpdump

Description

Displays files saved by the tcpdump utility.

Syntax

show files tcpdump

Parameters

None

Example

```
amnesiac # show files tcpdump
unopt.cap
big-noopt.cap
big-opt.cap
big.tgz
big-opt2.cap
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"tcpdump"

show hardware all

Description

Displays hardware information such as the current slot configuration.

Syntax

show hardware all

Parameters

None

Example

```
amnesiac # show hardware all
Hardware Revision: B
Mainboard:  Series 3000/5000 motherboard, ................. CMP-00072
Slot 0:     4 Port Copper GigE Network Bypass Card, ....... CMP-00074
Slot 1:     (Empty)
Slot 2:     (Empty)
Slot 3:     (Empty)
Slot 4:     6 Port SATA RAID I/O Card, .................... CMP-00014
Slot 5:     (Empty)
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"hardware spec activate"

show hardware licensing info

Description

Displays hardware licensing information.

Syntax

show hardware licensing info

Parameters

None

Example

```
amnesiac # show hardware licensing info
Hardware Revision: B
Mainboard:  Series 3000/5000 motherboard, ................. CMP-00072
```

```
Slot 0:     4 Port Copper GigE Network Bypass Card, ....... CMP-00074
Slot 1:     (Empty)
Slot 2:     (Empty)
Slot 3:     (Empty)
Slot 4:     6 Port SATA RAID I/O Card, .................... CMP-00014
Slot 5:     (Empty)
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"hardware spec activate"

show interfaces

Description

Displays the running state settings and statistics.

Syntax

show interfaces [<intname>] | [brief | configured]

Parameters

<intname>	Specify the interface name. For example, **aux**, **lan0_0**, **wan0_0**, **primary**, **in-path0_0, lo**.
brief	Displays the running state settings without statistics.
configured	Displays configured settings for the interface.

Usage

The settings and statistics displayed varies when using DHCP.

Example

```
amnesiac # show interfaces configured
Interface aux configuration
   Enabled:            yes
   DHCP:               no
   Speed:              auto
   Duplex:             auto
   IP address:         10.0.190.139
   Netmask:            255.255.0.0
   MTU:                1500

Interface inpath0_0 configuration
   Enabled:            yes
   DHCP:               no
   IP address:         10.11.192.139
   Netmask:            255.255.0.0
   MTU:                1500
   Failure mode:       Bypass <<fail-to-block or fail-to-bypass>>
<<this is a partial example>>
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"interface"

show in-path mgmt-interface

Description

Displays the configured management in-path (MIP) interface.

Syntax

show in-path mgmt-interface

Parameters

None

Example

```
amnesiac # show in-path mgmt-interface
   In-path interface: inpath0_0
   Enabled: true
   IP address: 90.90.90.1
   Mask Length: 24
   VLAN: 0
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"Management In-Path Interface Commands"

show ip default-gateway

Description

Displays the IP default gateway.

Syntax

show ip default gateway [static]

Parameters

static	Displays the static default gateway.

Example

```
amnesiac # show ip default-gateway static
Configured default gateway: 10.0.0.1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"ip in-path-gateway"

show ipv6

Description

Displays current IPv6 status and IPv6 status to be applied after next boot.

Syntax

show ipv6

Parameters

None

Usage

The **show ipv6** command displays status for both the currently enabled configuration and the configuration that will be applied after the next boot.

- **IPv6 Currently Enabled** - Is IPv6 enabled and has the Steelhead appliance rebooted after enabling IPv6?
- **IPv6 Enabled Next Boot** - Will IPv6 support be effective after the Steelhead appliance is rebooted?

Example

```
amnesiac #  show ipv6
IPv6 Currently Enabled: no
IPv6 Enabled Next Boot: no
```

Product

CMC, Steelhead appliance Steelhead EX appliance

Related Topics

"ipv6 in-path-gateway"

show ipv6 default-gateway

Description

Displays the IPv6 default gateway.

Syntax

show ipv6 default gateway [static]

Parameters

static	Displays the static default gateway.

Example

```
amnesiac # show ipv6 default-gateway static
Configured default gateway: 2001:38dc:52::e9a4:c5:6282/64
```

Product

CMC, Steelhead appliance, Steelhead EX appliance

Related Topics

"ipv6 default-gateway"

show ipv6 in-path-gateway

Description

Displays the in-path IPv6 default gateway.

Syntax

show ipv6 in-path-gateway <interface> [static]

Parameters

<interface>	Specify the interface for display.
static	Displays the static default gateway.

Example

```
amnesiac # show ipv6 in-path-gateway inpath0_0
Destination Network                          Gateway
default                                      2001:38dc:52::e9a4:c5:6282
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"ipv6 in-path-gateway"

show ipv6 in-path route

Description

Displays active in-path IPv6 route settings, both dynamic and static.

Syntax

show ipv6 in-path route <interface> [static]

Parameters

<interface>	Specify the interface for display.
static	Displays the static default gateway.

Example

```
amnesiac # show ipv6 in-path route inpath0_0
Destination Network                          Gateway
2001:38dc:52::/64                            ::
2001:7632::/64                               2001:38dc:52::e9a4:c5:6289
2001:7639::/64                               2001:38dc:52::e9a4:c5:6279
default                                      2001:38dc:52::e9a4:c5:6282

amnesiac # show ipv6 in-path route inpath0_0 static
Destination Network                          Gateway
2001:7632::/64                               2001:38dc:52::e9a4:c5:6289
2001:7639::/64                               2001:38dc:52::e9a4:c5:6279
default                                      2001:38dc:52::e9a4:c5:6282
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"ipv6 in-path route"

show ipv6 route

Description

Displays active IPv6 routes, both dynamic and static.

Syntax

show ipv6 route [static]

Parameters

static	Displays the static default gateway.

Example

```
amnesiac # show ipv6 route
Destination Network              Gateway                      Interface
::1/128                          ::                           lo
2000::/64                        ::                           primary
2001::20e:b6ff:fe01:58f1/128     ::                           lo
2001::/60                        ::                           aux
2001::/60                        ::                           primary
fe80::200:ff:fe00:0/128          ::                           lo
fe80::200:ff:fe00:0/128          ::                           lo
[partial example]
```

Product

CMC, Steelhead appliance, Steelhead EX appliance

Related Topics

"ipv6 route"

show ip route

Description

Displays active routes both dynamic and static.

Syntax

show ip route [static]

Parameters

static	Displays configured static routes.

Example

```
amnesiac # show ip route static
Destination       Mask             Gateway
default           0.0.0.0          10.0.0.4
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"ip route"

show job

Description

Displays the status of a scheduled job.

Syntax

show job <job-id>

Parameters

<job-id>	Specify the job identification number.

Example

```
amnesiac # show job 10
job {job_id}: 10
Status: pending
Name: myjob
Comment: this is a text
Absolute range:
Commands:
show info.
show connections.
show version.
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"Job Commands"

show jobs

Description

Displays a list of all jobs.

Syntax

show jobs

Parameters

None

Example

```
amnesiac # show jobs
% No jobs configured.
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"Job Commands"

show licenses

Description

Displays installed (active) licenses.

Syntax

show licenses

Parameters

None

Example

```
amnesiac # show licenses
XXX-XXXXXX-XXXX-XXXX-X-XXXX-XXXX-XXXX
```

```
Feature:     SH10BASE
Valid:       yes
Active:      yes
Start date:
End date:
XXX-XXXXXX-XXXX-XXXX-X-XXXX-XXXX-XXXX
Feature:     SH10CIFS
Valid:       yes
Active:      yes
Start date:
End date:
XXX-XXXXXX-XXXX-XXXX-X-XXXX-XXXX-XXXX
Feature:     SH10EXCH
Valid:       yes
Active:      yes
Start date:
End date:
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"License and Hardware Upgrade Commands"

show log

Description

Displays the system logs.

Syntax

show log [continuous | files <log number> | reverse | matching]

Parameters

continuous	Displays the log continuously, similar to the Linux **tail -f** command.
files <log number>	Displays a list of log files or a specific log file.
reverse	Displays the log information, in reverse order, with the latest entry at the top.
matching	Displays a list of matching log files.

Example

```
amnesiac # show log
May 22 20:00:00 localhost /usr/sbin/crond[784]: (root) CMD (/usr/sbin/logrotate /etc/
logrotate.conf)
May 22 20:00:00 localhost cli[555]: [cli.INFO]: user admin: CLI got signal 2 (SIGINT)
May 22 20:02:31 localhost cli[555]: [cli.INFO]: user admin: Executing command: show ip route
May 22 20:02:38 localhost cli[555]: [cli.INFO]: user admin: CLI got signal 2 (SIGINT)
Dec 22 20:03:16 localhost cli[555]: [cli.INFO]: user admin: CLI got signal 2 (SIGINT)
May 22 20:04:00 localhost cli[555]: [cli.INFO]: user admin: Executing command: show ip route static
May 22 20:05:02 localhost cli[555]: [cli.INFO]: user admin: Executing command: show licenses
Dec 22 20:05:09 localhost cli[555]: [cli.INFO]: user admin: CLI got signal 2 (SIGINT)
May 22 20:06:44 localhost cli[555]: [cli.INFO]: user admin: Executing command: show limit bandwidth
May 22 20:06:49 localhost cli[555]: [cli.INFO]: user admin: CLI got signal 2 (SIGINT)
May 22 20:07:12 localhost cli[555]: [cli.INFO]: user admin: Executing command: show log
Virtual IP addresses:
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"Logging Commands"

show papi rest access_codes

Description

Displays the REST API settings.

Syntax

show papi rest access_codes

Parameters

None

Usage

Use this command to display the access code settings used to gain access to REST APIs.

Example

```
amnesiac # show papi rest access_codes
ID: b6c1efd5-a20b-4784-b2f2-44bedc9bc107
   Desc: example
   Creator: admin
   Code:eyJhdWQiOiAiaHR0cHM6Ly9wZXJmNC1zaDQubGFiLm5idHRlY2guY29tL2FwaS9jb21tb24vMS4wL3Rva2VuIiwgI
mlzcyI6ICJodHRwczovL3BlcmY0LXNoNC5sYWIubmJ0dGVjaC5jb20iLCAicHJuIjogImFkbWluIiwgImp0aSI6ICJiNmMxZW
ZkNS1hMjBiLTQ3ODQtYjJmMi00NGJlZGM5YmMxMDciLCAiZXhwIjogIjAiLCAiaWF0IjogIjEzNjM5Nzk4OTIifQ==
```

Product

CMC, Steelhead appliance, Steelhead EX appliance

Related Topics

"papi rest access_code generate," "papi rest access_code import," "web rest-server enable"

show port-label

Description

Displays a list of port label configurations or a list of ports that belong to the label.

Syntax

show port-label [<port label>]

Parameters

<port label>	Specify one of the following default port label names or a port label name: • **Secure -** Displays the list of ports that belong to the system label for secure ports. The Steelhead appliance automatically passes through traffic on commonly secure ports (for example, ssh, https, and smtps). For a list of secure ports, see Appendix A, “Riverbed Ports.” If you do not want to pass through secure ports, you must delete the default secure in-path rule. For detailed information, see “in-path rule fixed-target” on page 343. • **Granite -** Displays the list of ports that belong to the system label for Riverbed Granite ports 7950 - 7954, and 7960. • **Interactive -** Displays ports that belong to the system label for interactive ports. The Steelhead appliance automatically passes through traffic on interactive ports (for example, Telnet, TCP ECHO, remote logging, and shell). • **RBT-Proto** - Displays the list of ports that belong to the label for system processes: 7744 (data store synchronization), 7800-7801 (in-path), 7810 (out-of-path), 7820 (failover), 7850 (connection forwarding), 7860 (Interceptor appliance), 7870 (Steelhead Mobile Controller).

Example

```
amnesiac # show port-label
Port Label:        Interactive
Port Label:        Secure

amnesiac # show port-label Interactive
Port Label: Interactive
7, 23, 37, 107, 179, 513-514, 1494, 1718-1720, 2000-2003, 2427, 2598, 2727, 3389
, 5060, 5631, 5900-5903, 6000
```

Product

Interceptor appliance, Steelhead appliance, Steelhead EX appliance

Related Topics

“Port Label Commands”

show protocol domain-auth auto-conf delegation

Description

Displays delegation autoconfiguration results.

Syntax

show protocol domain-auth auto-conf delegation {add-server | del-server | setup-user} [verbose]

Parameters

add-server	Displays servers added to the msDS-Allowed-ToDelegateTo Active Directory attribute.
del-server	Displays servers deleted from the msDS-Allowed-ToDelegateTo Active Directory attribute.
setup-user	Displays delegation autoconfiguration results.
verbose	Displays delegation autoconfiguration results with verbose logs.

Example

```
amnesiac # show protocol domain-auth auto-conf delegation add-server

Action                            STATUS                      LAST RUN
--------------------------------------------------------------------------------

Auto-Conf Delegation Add-Server   NOT STARTED             ---------------
--------------------------------------------------------------------------------
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"protocol domain-auth auto-conf delegation adminuser," "protocol domain-auth auto-conf delegation domain"

show protocol domain-auth auto-conf easy-auth

Description

Displays easy domain authentication autoconfiguration results.

Syntax

show protocol domain-auth auto-conf easy-auth [verbose]

Parameters

verbose	Displays easy domain authentication autoconfiguration results with verbose logs.

Example

```
amnesiac # show protocol domain-auth auto-conf easy-auth

Action STATUS LAST RUN
--------------------------------------------------------------------------------
Auto-Conf Easy-Auth SUCCESS Wed Dec 31 16:00:00 2012
--------------------------------------------------------------------------------
RESULT : Auto-Conf Easy Auth result:
DNS Test Passed
Successfully joined domain:TESTDOM.COM
Successfully enabled nodes for smb2signing,emapi auto-conf
Auto-Conf of Replication user in AD succeeded
Please make sure Encrypted MAPI is enabled on the peers
Please make sure Encrypted MAPI NTLM is enabled on the peers
Please make sure Encrypted MAPI Native Kerberos is enabled on the peers
You must restart the optimization service for your changes to take effect.
emapi Auto-conf Successfully completed
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"protocol domain-auth auto-conf easy-auth"

show protocol domain-auth auto-conf replication

Description

Displays replication autoconfiguration results.

Syntax

show protocol domain-auth auto-conf replication [verbose]

Parameters

verbose	Displays replication autoconfiguration results with verbose logs.

Example

```
amnesiac # show protocol domain-auth auto-conf replication
```

```
Action                            STATUS                      LAST RUN
--------------------------------------------------------------------------------

Auto-Conf Replication             NOT STARTED             ---------------
--------------------------------------------------------------------------------
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"protocol domain-auth auto-conf replication"

show protocol domain-auth test authentication

Description

Displays authentication test results.

Syntax

show protocol domain-auth test authentication

Parameters

verbose	Displays the authentication test result with verbose logs.

Example

```
amnesiac # show protocol domain-auth test authentication
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"protocol domain-auth test authentication"

show protocol domain-auth test delegation server-privs

Description

Displays delegation server privilege test results.

Syntax

show protocol domain-auth test delegation server-privs [verbose]

Parameters

verbose	Displays the delegation server privilege test result with verbose logs.

Example

```
amnesiac # show protocol domain-auth test delegation server-privs

Action                            STATUS                      LAST RUN
--------------------------------------------------------------------------------

Test Delegation Server-Privs      NOT STARTED             ---------------
--------------------------------------------------------------------------------
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"protocol domain-auth test delegation server-privs"

show protocol domain-auth test delegation setup

Description

Displays delegation setup test results.

Syntax

show protocol domain-auth test delegation setup [verbose]

Parameters

verbose	Displays the delegation setup test result with verbose logs.

Example

```
amnesiac # show protocol domain-auth test delegation setup

Action                             STATUS                         LAST RUN
--------------------------------------------------------------------------------

Test Delegation Setup              NOT STARTED              ---------------
--------------------------------------------------------------------------------
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"protocol domain-auth test delegation setup"

show protocol domain-auth test dns

Description

Displays DNS test results for domain authentication.

Syntax

show protocol domain-auth test dns [verbose]

Parameters

verbose	Displays DNS test results with verbose logs.

Example

```
amnesiac # show protocol domain-auth test dns
Action                             STATUS                         LAST RUN
--------------------------------------------------------------------------------

Test DNS                           NOT STARTED              ---------------
--------------------------------------------------------------------------------
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"protocol domain-auth test dns"

show protocol domain-auth test join

Description

Displays domain join test results.

Syntax

show protocol domain-auth test join [verbose]

Parameters

verbose	Displays domain join test results with verbose logs.

Example

```
amnesiac # show protocol domain-auth test join
Action                            STATUS                       LAST RUN
--------------------------------------------------------------------------------

Test Join                         NOT STARTED              ---------------
--------------------------------------------------------------------------------
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"protocol domain-auth test join"

show protocol domain-auth test replication prp

Description

Displays password replication policy (PRP) setup results.

Syntax

show protocol domain-auth test replication prp [verbose]

Parameters

verbose	Displays the test PRP setup result with verbose logs.

Example

```
amnesiac > show protocol domain-auth test replication prp

Action                            STATUS                       LAST RUN
--------------------------------------------------------------------------------

Test Replication PRP              NOT STARTED              ---------------
--------------------------------------------------------------------------------
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"protocol domain-auth test replication prp"

show protocol domain-auth test replication try-repl

Description

Displays ability to replicate server account results.

Syntax

show protocol domain-auth test replication try-repl [verbose]

Parameters

verbose	Displays ability to replicate server account result with verbose logs.

Example

```
amnesiac > show protocol domain-auth test replication try-repl

Action                            STATUS                      LAST RUN
--------------------------------------------------------------------------------

Test Replication try-repl         NOT STARTED             ---------------
--------------------------------------------------------------------------------
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"protocol domain-auth test replication try-repl"

show protocol notes encrypt

Description

Displays Lotus Notes settings.

Syntax

show protocol notes encrypt [blacklist | server-ids]

Parameters

blacklist	Displays the IP addresses that are currently in the blacklist.
server-ids	Displays a list of server names for which ID files have been imported.

Example

```
amnesiac # show protocol notes encrypt
Notes Encryption Optimization:     no
Notes Unencrypted Server Port Number: 1352
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"protocol notes encrypt server-port," "protocol notes encrypt import server-id"

show radius

Description

Displays RADIUS configuration settings.

Syntax

show radius

Parameters

None

Example

```
amnesiac # show radius
No radius settings
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"AAA, Role-Based Management, Radius, and TACACS+ Commands"

show remote ip

Description

Displays the current IP network settings for the remote management port.

Syntax

show remote ip

Parameters

None

Example

```
amnesiac # show remote ip
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"Remote Management Port Commands"

show running-config

Description

Displays the running configuration settings that differ from the defaults.

Syntax

show running-config [full]

Parameters

full	Displays all settings, including those set to the default value.

Example

```
amnesiac # show running-config
(displays running configuration)
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"Configuration File Commands"

show tacacs

Description

Displays TACACS+ settings.

Syntax

show tacacs

Parameters

None

Example

```
amnesiac # show tacacs
No tacacs settings
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"AAA, Role-Based Management, Radius, and TACACS+ Commands"

show telnet-server

Description

Displays Telnet server settings.

Syntax

show telnet-server

Parameters

None

Example

```
amnesiac # show telnet-server
TCP reordering enabled:   no
TCP reordering threshold: 3
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"telnet-server enable"

show userlog

Description

Displays current user log file in a scrollable pager.

Syntax

show userlog [continuous | files <file number>]

Parameters

continuous	Displays new user log messages as they occur.
files <file number>	Displays archived user log files.

Example

```
amnesiac # show userlog
Oct 17 15:38:54 amnesiac-sh75 cli[26992]: [cli.NOTICE]: user admin: CLI launched
Oct 17 15:39:00 amnesiac-sh75 cli[26992]: [cli.INFO]: user admin: Executing command:
enable
Oct 17 17:18:03 amnesiac-sh75 cli[26992]: [cli.INFO]: user admin: Executing command:
show raid diagram
Oct 17 17:18:13 amnesiac-sh75 cli[26992]: [cli.INFO]: user admin: Executing command:
show version
Oct 17 18:00:00 amnesiac-sh75 cli[26992]: [cli.INFO]: user admin: Executing command matching: show
rsp slots
Oct 17 18:00:36 amnesiac-sh75 cli[26992]: [cli.INFO]: user admin: Executing command matching: show
rsp dataflow RiO
Oct 17 18:00:46 amnesiac-sh75 cli[26992]: [cli.INFO]: user admin: Executing command matching: show
rsp dataflow RiOS
Oct 17 18:00:57 amnesiac-sh75 cli[26992]: [cli.INFO]: user admin: Executing command matching: show
rsp dataflow inpath0_0
Oct 17 18:01:10 amnesiac-sh75 cli[26992]: [cli.INFO]: user admin: Executing command matching: show
rsp images
Oct 17 18:08:22 amnesiac-sh75 cli[26992]: [cli.INFO]: user admin: Executing command:
show service
Oct 17 18:11:18 amnesiac-sh75 cli[26992]: [cli.INFO]: user admin: Executing command: show smb
signing delegation domains
<<this is partial display>>
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"Logging Commands"

show usernames

Description

Displays a list of user accounts..

Syntax

show usernames

Parameters

None

Example

```
amnesiac # show usernames
User                          Status      Active    Capability
---------------------------------------------------------------
admin@                        enabled       y         admin
monitor                       enabled       n         monitor
---------------------------------------------------------------
@ = current user
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"AAA, Role-Based Management, Radius, and TACACS+ Commands"

CHAPTER 4 Configuration-Mode Commands

This chapter is a reference for configuration-mode commands. It includes the following sections:

You can perform configuration tasks while in configuration mode. Only administrator users can perform configuration mode and enable mode commands. All commands available in user mode and enable mode are also available in configuration mode. Monitor users cannot perform configuration tasks.

To enter configuration mode

1. Connect to the CLI and enter the following commands:

```
login as: admin
Riverbed Steelhead
Last login: Wed Jan 20 13:02:09 2010 from 10.0.1.1
amnesiac > enable
amnesiac # configure terminal
amnesiac (config) #
```

You are now in configuration mode.

To exit configuration mode, enter **exit**. For information about the **exit** command, see "exit" on page 10.

Although most of the Steelhead appliance configuration commands are also available in the Interceptor appliance, CMC appliance, Steelhead Mobile Controller, and Cloud Steelhead, Riverbed strongly recommends that you do not use the CLI to perform configuration tasks on these products. Riverbed recommends that you use these products respective Management Consoles to perform configuration, system administration, and system reporting and monitoring tasks.

For an alphabetical list of commands, see the Index at the end of this book.

System Administration Commands

This section describes commands you use to perform system administration tasks. Many system administration commands are common to the CMC appliance, the Interceptor appliance, and the Steelhead appliance. System Administrator Commands includes the following sections:

- "Alarm Commands" on page 204
- "Displaying Role-Based Management Configuration Settings" on page 215
- "Host Setup Commands" on page 215
- "AAA, Role-Based Management, Radius, and TACACS+ Commands" on page 229
- "Account Control Management Commands" on page 243
- "Secure Shell Access Commands" on page 253
- "CLI Terminal Configuration Commands" on page 257
- "Web Configuration Commands" on page 260
- "Configuration File Commands" on page 269
- "Statistics Manipulation Commands" on page 280
- "Notification Commands" on page 282
- "SNMP Commands" on page 287
- "Logging Commands" on page 299
- "License and Hardware Upgrade Commands" on page 305
- "System Administration and Service Commands" on page 314

Alarm Commands

This section describes the commands to configure alarm settings.

alarm clear

Description

Clears the specified alarm type.

Syntax

alarm <type> clear

Parameters

<type>	See the "alarm enable" command for a complete listing and description of alarm types.

Usage

Use this command to clear the status of the specified alarm type. If you clear an alarm and the error condition still exists, the alarm might be triggered again immediately. If you need to clear an alarm permanently, use the **no alarm enable** command.

Example

```
amnesiac (config) # alarm secure_vault_unlocked clear
```

Product

CMC, Steelhead appliance

Related Topics

"alarm enable," "alarm clear-threshold," "show alarm,""show alarms"

alarm clear-threshold

Description

Sets the threshold to clear the specified alarm type.

Syntax

[no] alarm <type> clear-threshold <threshold level>

Parameters

<type>	See the "alarm enable" command for a complete listing and description of alarm types.
<threshold level>	Specify the threshold level. The threshold level depends on the alarm type, as do the possible values.

Usage

Use this command to set the threshold at which the alarm is cleared.

Example

```
amnesiac (config) # alarm cpu_util_indiv clear-threshold 70
```

Product

CMC, Steelhead appliance

Related Topics

"alarm enable," "alarm clear," "show alarm,""show alarms"

alarm enable

Description

Enables the specified alarm.

Syntax

[no] alarm <type> enable

Parameters

<type>

- **admission_conn** - This alarm should not be disabled. It indicates that the system connection limit has been reached. Additional connections are passed through unoptimized. The alarm clears when the Steelhead appliance moves out of this condition.
- **admission_control** - This alarm should not be disabled. It indicates that the system admission control pressure limit has been reached. Additional connections are passed through unoptimized. This alarm clears when the Steelhead appliance moves out of this condition.
- **admission_cpu** - This alarm should not be disabled. This alarm is triggered by high CPU usage. Additional connections are passed through unoptimized. The alarm clears when the Steelhead appliance moves out of this condition.
- **admission_mapi** - This alarm should not be disabled. It indicates that the total number of MAPI optimized connections has exceeded the maximum admission control threshold.
- **admission_mem** - This alarm should not be disabled. It indicates that the system connection memory limit has been reached. Additional connections are passed through unoptimized. The alarm clears when the Steelhead appliance moves out of this condition.
- **admission_tcp** - This alarm should not be disabled. This alarm is triggered by high TCP memory usage. Additional connections are passed through unoptimized. The alarm clears when the Steelhead appliance moves out of this condition.
- **appliance_unlicensed** - This alarm triggers if the Steelhead appliance has no BASE or MSPEC license installed for its currently configured model. This alarm also triggers for hardware earlier than xx60 with no BASE licensing installed.
- **arcount** - This alarm should not be disabled. It indicates whether the system is experiencing asymmetric traffic. If the system experiences asymmetric traffic, the system detects this condition and reports the failure. The traffic is passed through, and the route appears in the Asymmetric Routing table.
- **autolicense_error** - This alarm triggers on a Virtual Steelhead appliance when the Riverbed Licensing Portal cannot respond to a license request with valid licenses.
- **autolicense_info** - This alarm triggers if the Riverbed Licensing Portal has information regarding licenses for a Virtual Steelhead appliance.
- **block_store** - This alarm indicates that access to the Granite block store is lost.
- **bypass** - This alarm should not be disabled. It indicates that the system is in bypass mode. If the Steelhead appliance is in bypass mode, restart the Steelhead service.
- **certs_expiring** - This alarm indicates that the system has expiring SSL certificates.
- **cf_ack_timeout_aggr** - This alarm indicates that the connection has been lost because requests have not been acknowledged by a connection-forwarding neighbor within the set threshold.
- **cf_conn_failure_aggr -** This alarm indicates that the connection cannot be established with a connection-forwarding neighbor.
- **cf_conn_lost_eos_aggr -** This alarm indicates that the connection has been closed by the connection-forwarding neighbor.
- **cf_conn_lost_err_aggr -** This alarm indicates that the connection has been lost with the connection-forwarding neighbor due to an error.
- **cf_ipv6_incompatible_cluster -** This alarm sends an email notification if a connection-forwarding neighbor is running a RiOS version that is incompatible with IPv6, or if the IP address configuration between neighbors does not match. Neighbors must be running RiOS v8.5. The Steelhead appliance neighbors pass through IPv6 connections when this alarm triggers.
- **cf_keepalive_timeout_aggr -** This alarm indicates that the connection forwarding neighbor has not sent a keep-alive message within the time-out period to the neighbor Steelhead appliance(s) indicating that the connection has been lost.
- **cf_latency_exceeded_aggr -** This alarm indicates that the amount of latency between connection-forwarding neighbors has exceeded the specified threshold.
- **cf_read_info_timeout_aggr -** This alarm indicates that the Steelhead appliance has timed out while waiting for an initialization message from the connection-forwarding neighbor.

<type>	• **connection_forwarding** - This alarm is the connection forwarding parent alarm. • **cpu_util_indiv** - This alarm indicates whether the system has reached the CPU threshold for any of the CPUs in the system. If the system has reached the CPU threshold, check your settings. If your alarm thresholds are correct, reboot the Steelhead appliance • **critical_temp** - This alarm indicates that the CPU temperature has exceeded the critical threshold. The default value for the rising threshold temperature is 80º C; the default reset threshold temperature is 70º C. • **datastore** - This alarm indicates the overall data store health. • **datastore clean needed** - This alarm indicates that you need to clear the RiOS data store. • **datastore_error** - This alarm indicates that the data store is corrupt or has become incompatible with the current configuration. Clear the data store to clear the alarm. If the alarm was caused by an unintended change to the configuration, you can change the configuration to match the previous RiOS data store settings. Then restart the optimization service without clearing the RiOS data store to reset the alarm. Typical configuration changes that require a restart with a clear RiOS data store are enabling the Extended Peer Table or changing the data store encryption. • **datastore_sync_error** - This alarm indicates that the system has detected a problem with the synchronized data. • **disconnected_sh_alert** - This alarm indicates that the connection to a Steelhead appliance in a connection forwarding cluster is lost. • **disk** - This alarm indicates that the system has detected a problem with the specified disk or a solid-state drive. • **domain_join_error** - This alarm indicates that the system has encountered an error when attempting to join a domain. • **duplex** - This alarm indicates that the system has encountered a large number of packet errors in your network. Make sure that the speed and duplex settings on your system match the settings on your switch and router. By default, this alarm is enabled. • **edge** - This alarm indicates that Granite Core has lost connection with one of its configured Granite Edge appliances.

<type>

- **esxi_communication_failed** - This alarm indicates that the RiOS software cannot communicate with ESXi because of a password problem or another connection problem. The polling interval is 10 seconds. This alarm is enabled by default on the Steelhead EX appliance.
- **esxi_disk_creation_failed** - This alarm indicates that the ESXi disk creation failed during the VSP setup. The polling interval is 10 seconds. This alarm is enabled by default on the Steelhead EX appliance.
- **esxi_initial_config_failed** - This alarm indicates that the ESXi initial configuration failed. Contact Riverbed Support. This is a Steelhead EX appliance alarm.
- **esxi_license** - This alarm is the parent ESXi licensing alarm on the Steelhead EX appliance. It sends an email notification if the ESXi license is removed, about to expire, has expired, or is a trial version. This is a Steelhead EX appliance alarm.
- **esxi_license_expired** - This alarm indicates that the ESXi license has expired on the Steelhead EX appliance. This is a Steelhead EX appliance alarm.
- **esxi_license_expiring** - This alarm indicates that the ESXi license is going to expire within two weeks on the Steelhead EX appliance.
- **esxi_license_is_trial** - This alarm indicates that ESXi is using a trial license. This is a Steelhead EX appliance alarm.
- **esxi_memory_overcommitted** - This alarm indicates that the total memory assigned to powered-on VMs is more than the total memory available to ESXi for the VMs. To view this number in the vSphere client, choose Allocation > Memory > Total Capacity. The amount of memory overcommitted=Total memory assigned to powered-on VMs - ESXi memory total capacity. This alarm has configurable thresholds. The polling interval is 30 minutes. This alarm is enabled by default on the Steelhead EX appliance.
- **esxi_not_set_up** - This alarm indicates that a freshly installed appliance and ESXi have not yet been set up. Complete the initial installation wizard to enable VSP for the first time. The alarm clears after ESXi installation begins. The polling interval is 10 seconds. This alarm is enabled by default on the Steelhead EX appliance.
- **esxi_version_unsupported** - This alarm indicates that the running ESXi version is unsupported. The polling interval is 10 seconds. This alarm in enabled by default Steelhead EX appliance.
- **esxi_vswitch_mtu_unsupported** - This alarm is triggered when a vSwitch with an uplink or vmknic interface is configured with an MTU greater than 1500. Jumbo frames greater than 1500 MTU are not supported. The polling interval is 10 seconds. This alarm in enabled by default Steelhead EX appliance.
- **fan_error** - This alarm indicates that the system has detected a fan error.
- **flash_error** - This alarm indicates that the system has detected an error with the flash drive hardware. At times, the USB flash drive that holds the system images might become unresponsive; the Steelhead appliance continues to function normally. When this error triggers you cannot perform a software upgrade, as the Steelhead appliance is unable to write a new upgrade image to the flash drive without first power cycling the system. To reboot the appliance, enter the **reload** command to automatically power cycle the Steelhead appliance and restore the flash drive to its proper function. On desktop Steelhead appliance *x*50 and *x*55 models, you must physically power cycle the appliance (push the power button or pull the power cord).
- **flash_protection_failed** - This alarm indicates that the USB flash drive has not been backed up because there is not enough available space in the /var filesystem directory.
- **fs_mnt** - This alarm indicates that one of the mounted partitions is full or almost full. The alarm is triggered when only 7% of free space is remaining.
- **granite-core** - This alarm indicates that the connection to the Granite Core is lost.
- **granite -** This alarm indicates that a large amount of data in the block store needs to be committed to Granite Core.

<type>

- **halt_error** - This alarm cannot be disabled. It indicates that the system has detected an unexpected halt to the optimization service.
- **hardware** - This alarm indicates the overall health of the hardware.
- **high_availability** - This alarm indicates that at least one of the appliances in a high availability (HA) Steelhead EX appliance pair is actively serving storage data (the active node).
- **ipmi** - This alarm indicates that the system has detected an Intelligent Platform Management (IPMI) event. This alarm is not supported on all appliance models.
- **iscsi** - This alarm indicates that the iSCSI initiator is not accessible.
- **licensing -** This alarm is the parent licensing alarm and triggers if any of the license_expired, license_expiring, or appliance_unlicensed alarms are active.
- **license_expired** - This alarm triggers if any feature has at least one license installed, but all of them are expired.
- **license_expiring** - This alarm triggers if one or more features is going to expire within two weeks.

Note: The license expiring and license expired alarms are triggered per feature; for example, if you install two license keys for a feature, LK1-FOOxxx (expired) and LK1-FOO-yyy (not expired), the alarms do not trigger, because the feature has one valid license.

- **link_duplex -** This alarm is triggered when an interface was not configured for half-duplex negotiation but has negotiated half-duplex mode. Half-duplex significantly limits the optimization service results. This alarm is enabled by default.
- **link_io_errors -** This alarm is triggered when the link error rate exceeds 0.1% while either sending or receiving packets. This threshold is based on the observation that even a small link error rate reduces TCP throughput significantly. A properly configured LAN connection should experience very few errors. The alarm clears when the rate drops below 0.05%. This alarm is enabled by default.
- **linkstate -** This alarm indicates that the system has detected a link that is down. The system notifies you through SNMP traps, email, and alarm status. By default, this alarm is not enabled. The **no alarm linkstate enable** command disables the link state alarm.
- **lun -** This alarm indicates that the Granite LUN is unavailable.
- **memory_error** - This alarm indicates that the system has detected a memory error.
- **mismatch_peer_aggr** - This alarm indicates that the appliance has encountered another appliance that is running an incompatible version of system software. Refer to the CLI, Management Console, or the SNMP peer table to determine which appliance is causing the conflict. Connections with that peer will not be optimized, connections with other peers running compatible RiOS versions are unaffected. To resolve the problem, upgrade your system software. No other action is required as the alarm clears automatically.
- **model_unlicensed** - This alarm indicates that the model license has been removed or is expired.
- **nfs_v2_v4** - This alarm indicates that the system has triggered a v2 or v4 NFS alarm.
- **non_443_ssl_servers_detected_on_upgrade** - This alarm indicates that during a RiOS upgrade (for example, from v5.5 to v6.0), the system has detected a pre-existing SSL server certificate configuration on a port other than the default SSL port 443. SSL traffic might not be optimized. To restore SSL optimization, you can either add a peering rule to the server-side Steelhead appliance to intercept the connection and optimize the SSL traffic on the non-default SSL server port or you can add an in-path rule to the client-side Steelhead appliance to intercept the connection and optimize the SSL traffic on the non-default SSL server port. After adding a peering or in-path rule, you must clear this alarm manually by issuing the following CLI command:

```
alarm non_443_ssl_servers_detected_on_upgrade clear
```

<type>	• **optimization_general** - This alarm indicates that the optimization service is not operating normally. The service might not be running, it might be disabled, or it might have stopped optimizing. • **optimization_service** - This alarm indicates that the system has encountered an optimization service condition. • **other_hardware_error** - This alarm indicates that the system has detected a problem with the Steelhead appliance hardware. The alarm clears when you add the necessary hardware, remove the nonqualified hardware, or resolve other hardware issues. The following issues trigger the hardware error alarm: – the Steelhead appliance does not have enough disk, memory, CPU cores, or NIC cards to support the current configuration. – the Steelhead appliance is using a dual in-line memory module (DIMM), a hard disk, or a NIC that is not qualified by Riverbed. – DIMMs are plugged into the Steelhead appliance but RiOS cannot recognize them because the DIMM modules are in the wrong slot. You must plug DIMM modules into the black slots first and then use the blue slots when all of the black slots are in use. – a DIMM module is broken and you must replace it. – other hardware issues. • **paging** - This alarm indicates whether the system has reached the memory paging threshold. If 100 pages are swapped approximately every two hours the Steelhead appliance is functioning properly. If thousands of pages are swapped every few minutes, then reboot the system. If rebooting does not solve the problem, contact Riverbed Support. • **path_selection_path_down** - This alarm indicates that one of the paths selected using the path selection feature for a connection is unavailable because it has exceeded either the timeout value for path latency or the threshold for observed packet loss. • **pfs** - This alarm is the parent PFS alarm and triggers if the pfs_config or pfs_operation alarms are active. • **pfs_config** - This alarm indicates that there has been a PFS or prepopulation operation error. If the system detects an operation error, restart the Steelhead service and PFS. • **pfs_operation** - This alarm indicates that a synchronization operation has failed. If the system detects an operation failure, attempt the operation again. • **power_supply** - This alarm indicates that an inserted power supply cord does not have power, as opposed to a power supply slot with no power supply cord inserted. • **profile_switch_failed** - This alarm indicates that an error has occurred while repartitioning the disk drives during a storage profile switch. A profile switch changes the disk space allocation on the drives, clears the Granite and VSP data stores, and repartitions the data stores to the appropriate sizes. You switch a storage profile by using the **disk-config layout** command on an EX or EX+G Steelhead appliance. By default, this alarm is enabled. • **raid_disk_indiv** - This alarm indicates that the system has encountered RAID errors (for example, missing drives, pulled drives, drive failures, and drive rebuilds). For drive rebuilds, if a drive is removed and then reinserted, the alarm continues to be triggered until the rebuild is complete. Rebuilding a disk drive can take 4-6 hours.

<type>	• **rsp** - This alarm is the parent RSP alarm and triggers if any of the rsp_general_alarm, rsp_license_expired, or rsp_license_expiring alarms are active. • **rsp_general_alarm** - The RSP alarm automatically triggers when the system has detected a problem with RSP. Issues that might trigger the RSP alarm include lack of memory, incompatible RSP images, or watchdog activation. This alarm can indicate that an RSP package or a virtual machine has failed and is blocking or bypassing traffic or that virtual machines are enabled but are not currently powered on. • **rsp_license_expired** - This alarm indicates whether an RSP license has expired. • **rsp_license_expiring** - This alarm indicates whether an RSP license is about to expire. • **rsp_service** - This alarm enables an alarm when RSP is not running. • **secure_vault** - This alarm indicates a general secure vault error. • **secure_vault_rekey_needed** - This alarm indicates whether the system has detected that the secure vault needs to be rekeyed. • **secure_vault_uninitialized** - This alarm indicates that the system has detected that the secure vault is uninitialized. • **secure_vault_unlocked** - This alarm indicates whether the secure vault is unlocked. When the vault is unlocked, SSL traffic is not optimized and you cannot encrypt a data store. • **serial_cascade_misconfig** - This alarm indicates that the system has encountered an error in reaching a neighbor appliance configured for connection forwarding. • **service_error** - This alarm cannot be disabled. It indicates that the system has detected a software error in the Steelhead service. The Steelhead service continues to function, but an error message that you should investigate appears in the logs. • **single_cf** - This alarm indicates that the connection to a Steelhead appliance connection forwarding neighbor is lost. • **smb_alert** - This alarm indicates that the system has detected an SMB signing error.

<type>

- **snapshot -** This alarm indicates that a snapshot has failed to commit to the SAN, or a snapshot has failed to complete.
- **ssd_wear -** This is the parent alarm for ssd_wear_warning. This alarm triggers if one of the ssd_wear_warning:<x> alarms becomes active.
- **ssd_wear_warning** - This alarm indicates that the specified disk is approaching its write cycle limit. (Appears only on Steelhead appliance models 7050L or 7050M.)

  RiOS tracks the number of writes to each block. To view the overall status, enter the following command:

  ```
  show alarm ssd_wear
  ```

  To view the status of an individual alarm, enter the following command:

  ```
  show alarm ssd_wear:<x>
  ```

  where <x> is the SSD disk port number.
- **ssl** - This alarm indicates whether the system has detected an SSL error.
- **ssl_peer_scep_auto_reenrol**l - This alarm indicates that the system has detected an SCEP error. The Steelhead appliance uses SCEP to dynamically reenroll a peering certificate to be signed by a certificate authority. The alarm clears automatically when the next automatic reenrollment succeeds. To clear the alarm, execute the **protocol ssl peering auto- reenroll last-result clear-alarm** command.
- **sticky_staging_dir** - This alarm indicates that the system has detected an error while trying to create a process dump.
- **store_corruption** - This alarm cannot be disabled. It indicates whether the data store is corrupt. To clear the data store of data, restart the Steelhead service and clear the data store on the next restart.
- **sw_version_aggr** - This alarm indicates that there is a software version mismatch between peer appliances. The client-side and server-side Steelheads are running incompatible versions of software.
- **system_detail_report** - This alarm indicates that a system component has encountered a problem. This alarm is enabled by default.
- **temperature** - This alarm is the parent temperature alarm and triggers if any of the warning_temp or critical_temp alarms are active.
- **upgrade -** This alarm indicates the status of an upgrade.
- **virt_cpu_util_indiv** - This alarm indicates the status of the VSP virtual CPU utilization and is triggered if the virtualization CPU usage exceeds an acceptable threshold over a period of time on a single core. CPU utilization is sampled only for the physical CPU core or cores available for virtualization, not for the CPU cores used by RiOS software. The polling interval is 15 seconds. This alarm is disabled by default.
- **vsp** - This alarm is the parent VSP alarm; it is triggered if any of the VSP alarms are active. This alarm is enabled by default.
- **vsp_service_not_running** - This alarm is triggered when any of the services critical for virtualization are not running. This alarm is enabled by default.
- **vsp_unsupported_vm_count** - This alarm is triggered when the number of VMs powered on exceeds five. The polling interval is 30 minutes. This alarm is enabled by default.
- **warning_temp -** This alarm indicates whether the CPU temperature has exceeded the warning threshold. The default value for the rising threshold temperature is 80º C; the default reset threshold temperature is 70º C.

Usage

Enabling alarms is optional.

Critical temperature settings cannot be changed. Warning temperature settings can be changed.

The **no** command option disables all statistical alarms. The **no alarm <type> enable** command disables specific statistical alarms.

Example

```
amnesiac # alarm connection_forwarding enable
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"alarm clear," "alarm clear-threshold," "alarm error-threshold," "show alarm,""show alarms"

alarm error-threshold

Description

Sets a threshold to trigger an alarm.

Syntax

[no] alarm <type> error-threshold <threshold level>

Parameters

<type>	See the "alarm enable"command for a complete listing and description of alarm types.
<threshold level>	Specify the threshold level. The threshold level and possible values depend on the alarm type.

Usage

The **no** version of the command resets the threshold to the default level.

Example

```
amnesiac (config) # alarm cpu_util_indiv error-threshold 80
```

Product

CMC, Steelhead appliance

Related Topics

"alarm clear," "alarm clear-threshold," "alarm enable," "show alarm,""show alarms"

alarm rate-limit

Description

Sets the alarm rate-limit values.

Syntax

alarm <type> rate-limit [email | snmp] term {long | medium | short} {count <value> | window <duration-seconds>}

Parameters

<type>	See the "alarm enable" command for a complete listing and description of alarm types.
email	Sets rules for email.
snmp	Sets rules for SNMP.
term {long | medium | short}	Sets the alarm event rate-limit term value. Valid choices are: • **long** • **medium** • **short**
count <value>	Sets the count value. The default values are 50 (long), 20 (medium), and 5 (short).
window <duration-seconds>	Sets the duration of time, in seconds, that the window remains open. The default values are 604,800 (long), 86,400 (medium), and 3600 (short).

Usage

There are three term values—long, medium, and short. Each has a window, which is a number of seconds, and a maximum count. If, for any term value, the number of alarm events exceeds the maximum count during the window, the corresponding email/SNMP notifications are not sent.

Example

```
amnesiac (config) # alarm crl_error rate-limit email term short window 30
```

Product

Steelhead appliance

Related Topics

"alarm clear," "alarm clear-threshold," "alarm enable," "alarm error-threshold," "show alarm,""show alarms"

alarms reset-all

Description

Globally sets all alarms to their default settings.

Syntax

[no] alarms reset-all

Parameters

None

Usage

Use this command to reset all the alarms to their default settings.

Example

```
amnesiac (config) # alarms reset-all
```

Product

Steelhead appliance

Related Topics

"alarm clear," "alarm clear-threshold," "alarm enable," "show alarm,""show alarms"

Displaying Role-Based Management Configuration Settings

This section describes the commands to display role-based management settings.

The following commands are available in configuration mode and enable mode. You must have administrator permissions to display these system settings.

show rbm user

Description

Displays user configuration.

Syntax

show rbm user <username>

Parameters

<username>	Specify the user name.

Example

```
amnesiac (config) # show rbm user helpdesk
```

Product

Steelhead appliance, CMC

Related Topics

"AAA, Role-Based Management, Radius, and TACACS+ Commands"

show rbm users

Description

Displays user configuration for all users.

Syntax

show rbm users

Parameters

None

Example

```
amnesiac (config) # show rbm users
```

Product

Steelhead appliance, CMC

Related Topics

"AAA, Role-Based Management, Radius, and TACACS+ Commands"

Host Setup Commands

This section describes the host setup commands.

arp

Description

Creates static ARP entries in the ARP table.

Syntax

[no] arp <ip-addr> <MAC-addr>

Parameters

<ip-addr>	Specify the IP address of the appliance.
<MAC-addr>	Specify the MAC address.

Usage

The **no** command option disables ARP static entries.

Example

```
amnesiac (config) # arp 10.0.0.1 00:07:E9:55:10:09
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show admission"

arp filter response

Description

Enables ARP filtering.

Syntax

arp <ip-addr> filter response

Parameters

<ip-addr>	Specify the IP address of the appliance.

Example

```
amnesiac (config) # arp 10.0.0.1 filter response
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"show arp"

clock timezone

Description

Sets the current time zone.

Syntax

clock timezone <zone>

Parameters

<zone>	Specify the time zone name: **Africa**, **America**, **Antarctica**, **Arctic**, **Asia**, **Atlantic_Ocean**, **Australia**, **Europe**, **GMT-offset**, **Indian_Ocean**, **Pacific_Ocean**, **UTC**.

Usage

The default value is GMT-offset.

Example

```
amnesiac (config) # clock timezone Africa
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show clock"

hostname

Description

Sets the hostname for this system.

Syntax

[no] hostname <hostname>

Parameters

<hostname>	Specify the hostname. Do not include the domain name.

Usage

The **no** command option removes the hostname for this appliance.

Example

```
amnesiac (config) # hostname park
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show hosts"

interface

Description

Configures system interfaces.

Syntax

[no] interface <interfacename> <options>

Parameters

<interfacename>	Specify the interface name: **lo**, **aux**, **lan0_0**, **wan0_0**, **primary**, **in-path0_0**. The interface name varies according to the Riverbed product your are configuring. For example, for the Steelhead Mobile Controller the interface options are: **primary**, **aux**, **lo**. For details, see the CLI online help.
<options>	Each interface has the following configuration options: • **arp** - Adds static entries to the ARP cache. • **description** - Configure the description string of this interface. • **dhcp renew** - Enables DHCP on the interface or renews DHCP. Setting DHCP on the auxiliary interface only provides an IP lease, and does not update the gateway, routes, and DNS settings. • **dhcp dynamic-dns** - Enables DHCP hostname registration with dynamic DNS. This option is not available on the Steelhead Mobile Controller. • **duplex <speed>** - Specify the duplex speed: **auto**, **full**, **half**. The default value is **auto**. • **ip address <ip-addr> <netmask>** - Specify the IP address and netmask for the interface. • **ipv6 address <ipv6-addr> <prefix length>** - Specify the IPv6 address and prefix length for the interface. Your Steelhead appliance can have both an IPv4 address and an IPv6 address. You can only configure one IPv6 address per in-path interface. **To set an IPv6 address** `amnesiac (config) # interface primary ipv6 address 2001:38dc:52::e9a4:c5:6282 64` • **mtu <speed>** - Specify the MTU. The MTU is set once on the in-path interface; it propagates automatically to the LAN and the WAN. The **no** command option disables the MTU setting. The default value is 1500. • **shutdown** - Shuts down the interface. • **speed <speed>** - Specify the speed for the interface: **auto**, **10**, **100**, **1000**. The default value is 100.

<options>	• **fail-to-bypass enable** - Disables fail-to-block (disconnect) mode. The **no interface <interface> fail-to-bypass enable** command enables fail-to-block mode. This option is not available on the Steelhead Mobile Controller.
	In fail-to-block mode, if the Steelhead appliance has an internal software failure or power loss, the Steelhead appliance LAN and WAN interfaces power down and stop bridging traffic. This feature is only useful if the network has a routing or switching infrastructure that can automatically divert traffic off of the link once the failed Steelhead appliance blocks it. For details about which NICs support fail-to-block, see the *Network Interface Card Installation Guide*.
	To enable fail-to-block mode
	`enable`
	`configure terminal`
	`no interface inpath0_0 fail-to-bypass enable`
	`write memory`
	To change from fail-to-block mode back to fail-to-wire mode
	`enable`
	`configure terminal`
	`interface inpath0_0 fail-to-bypass enable`
	`write memory`
	Fail-to-wire (or bypass) mode allows the Steelhead appliance WAN and LAN ports to serve as an Ethernet crossover cable. In fail-to-wire mode, Steelhead appliances cannot view or optimize traffic. Instead, all traffic is passed through the Steelhead appliance unoptimized. All Steelhead appliance in-path interfaces support fail-to-wire mode. Fail-to-wire mode is the default setting for Steelhead appliances.
	For details about enabling and disabling fail-to-block, see the *Steelhead Appliance Deployment Guide*.

Usage

The **no** command option disables the interface settings.

Example

```
amnesiac (config) # no interface inpath0_0 fail-to-bypass enable
```

Product

CMC, Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show interfaces", "ipv6 in-path-gateway", "show ipv6"

ip default-gateway

Description

Sets the default gateway for the appliance.

Syntax

[no] ip default-gateway <ip-addr>

Parameters

<ip-addr>	Specify the IP address of the management interface.

Usage

This command is used to set the default gateway for the entire appliance. It is primarily used for the primary or auxiliary (**aux**) interfaces for management, but can also be used for out-of-path optimization configurations as well as PFS.

The **no** command option disables the default gateway IP address.

Example

```
amnesiac (config) # ip default-gateway 10.0.0.12
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show ip", "ipv6 default-gateway"

ip domain-list

Description

Adds a domain name to the domain list for resolving hostnames.

Syntax

[no] ip domain list <domain>

Parameters

<domain>	Specify the domain name.

Usage

The **no** command option removes a domain from the domain list.

Example

```
amnesiac (config) # ip domain-list example.com
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show hosts"

ip host

Description

Adds an entry to the static host table.

Syntax

[no] ip host <hostname> <ip-addr>

Parameters

<hostname>	Specify the hostname.
<ip-addr>	Specify the IP address.

Usage

The **no** command option removes an entry from the static host table.

Example

```
amnesiac (config) # ip host park 10.10.10.1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show hosts"

ipv6 default-gateway

Description

Configures a default IPv6 route.

Syntax

[no] ipv6 default-gateway <ipv6-address>

Parameters

<ipv6-address>	Specify the IPv6 address.

Usage

Support for IPv6 is enabled by default. The **no** command option removes the default gateway for IPv6 routing.

Example

```
amnesiac (config) # ipv6 default-gateway 2001:38dc:52::e9a4:c5:6282
```

Product

Steelhead appliance

Related Topics

"show domain", "ipv6 route"

ipv6 in-path-gateway

Description

Configures an in-path IPv6 default gateway.

Syntax

[no] ipv6 in-path-gateway <interface> <ipv6-address>

Parameters

<interface>	Specify the interface.
<ipv6-address>	Specify the IPv6 address of the in-path gateway.

Usage

Support for IPv6 is enabled by default. The **no** command option deletes the in-path default gateway for IPv6 routing.

Example

```
amnesiac (config) # ipv6 in-path-gateway inpath0_0 2001:38dc:52::e9a4:c5:6282
```

Product

Steelhead appliance

Related Topics

"ipv6 in-path route," "show ipv6 default-gateway"

ipv6 in-path route

Description

Adds IPv6 in-path routes in addition to the default gateway, if needed.

Syntax

[no] ipv6 in-path route <interface> <ipv6-network prefix> <ipv6-address>

Parameters

<interface>	Specify the interface: • **inpath0_0** • **inpath0_1**
<ipv6-network prefix>	Specify the IPv6 network prefix. Use the format X:X:X::X/<0-128>.
<ipv6-address>	Specify the next-hop IPv6 address in this route.

Usage

Support for IPv6 is enabled by default. The **no** command option deletes the in-path IPv6 routes.

Example

```
amnesiac (config) #  ipv6 in-path route inpath0_0 2001:7632::/64 2001:38dc:52::e9a4:c5:6289
```

Product

Steelhead appliance

Related Topics

"ipv6 in-path-gateway," "show ipv6 in-path route"

ipv6 route

Description

Adds IPv6 routes in addition to the default gateway, if needed.

Syntax

[no] ipv6 route <IPv6 destination> <prefix length> <gateway>

Parameters

<IPv6 destination>	Specify the IPv6 address.
<prefix length>	Specify the IPv6 prefix length.
<gateway>	Specify the IPv6 address of the gateway.

Usage

Support for IPv6 is enabled by default. The **no** command option removes the specified IPv6 route.

Example

```
amnesiac (config) # ipv6 route 2001:38dc:52::e9a4:c5:6282 64 2001:38dc:52::1
```

Product

Steelhead appliance

Related Topics

"show domain", "ipv6 default-gateway"

ip name-server

Description

Adds a DNS name server.

Syntax

[no] ip name-server <ip-addr>

Parameters

<ip-addr>	Specify the name server IP address.

Usage

The **no** command option removes a DNS name server.

Example

```
amnesiac (config) # ip name-server 10.10.10.1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show hosts"

ip route

Description

Adds a static route.

Syntax

[no] ip route <network prefix> <netmask> <netmask length> <next-hop-ip-addr>

Parameters

<network prefix>	Specify the network prefix.
<netmask>	Specify the netmask. For example: **255.255.255.0**
<netmask length>	Specify the netmask length. For example: **/24**
<next-hop-ip-addr>	Specify the next hop IP address.

Usage

The **no** command option disables the static route. If **no ip route** is run with only a network prefix and mask, it deletes all routes for that prefix.

Example

```
amnesiac (config) # ip route 192 193.166.0/24 10.10.10.1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show ip"

limit connection

Description

Sets the connection limit for the source IP address.

Syntax

[no] limit connection <limit>

Parameters

<limit>	Specify the connection limit.

Usage

The **no** command option disables the connection limit.

Example

```
amnesiac (config) # limit connection 200
```

Product

Steelhead appliance, CSH

Related Topics

"show limit connection"

ntp authentication

Description

Configures the Network Time Protocol (NTP) authentication settings to authenticate NTP servers and peers.

Syntax

[no] ntp authentication key <key id> secret {<plaintext> | 0 <plaintext> |7 <encrypted-string>}

Parameters

key <key id>	Specify the key identifier. The key ID values must be in the range 1 - 65534.
secret {<plaintext> | 0 <plaintext> |7 <encrypted-string>}	Specify the shared secret parameter. Choose one of the following: • <plaintext> - Specify a shared secret in plain text. This option is the same as the 0 <plaintext> option and is provided for backward compatibility. • **0** <plaintext> - Specify a shared secret in plain text. • **7** <encrypted-string> - Specify a shared secret with an encrypted string.

Usage

The **no** version of the command removes NTP authentication settings.

NTP authentication involves three steps that you can perform in any order:

- Configure a key ID using the **ntp authentication** command.
- Add the configured key ID to the trusted keys list using the **ntp authentication trusted-keys** command.
- Configure the NTP server or peer with the key ID using the **ntp server key** or **ntp peer key** command.

Example

```
amnesiac (config) # ntp authentication key 56732 secret zza419
```

Product

CMC, Steelhead appliance

Related Topics

"ntp authentication trustedkeys," "ntp peer key," "ntp server key," "show ntp," "show ntp authentication"

ntp authentication trustedkeys

Description

Adds a configured key ID to the trusted keys list.

Syntax

[no] ntp authentication trustedkeys <key id> [key id, ...]

Parameters

key <key id> [key id, ...]	Specify the key identifier. The key ID values must be in the range 1 - 65534. You can specify multiple key IDs in the same list, separated by commas. When specifying multiple key IDs separated by commas, you must enclose them in quotes.

Usage

Use this command to add the configured key ID to the trusted keys list.

The **no** command removes a key from the trusted key list.

NTP authentication involves three steps that you can perform in any order:

- Configure a key ID using the **ntp authentication** command.
- Add the configured key ID to the trusted keys list using the **ntp authentication trusted-keys** command.
- Configure the NTP server or peer with the key ID using the **ntp server key** or **ntp peer key** command.

Example

```
amnesiac (config) # ntp authenticatication trustedkeys 56732
```

Product

CMC, Steelhead appliance

Related Topics

"ntp authentication," "ntp peer key," "ntp server key," "show ntp authentication"

ntp disable

Description

Disables NTP support.

Syntax

[no] ntp disable

Parameters

None

Usage

The **no** command option enables NTP support.

Example

```
amnesiac (config) # ntp disable
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show ntp"

ntp enable

Description

Enables NTP support.

Syntax

[no] ntp enable

Parameters

None

Usage

The **no** command option disables NTP support.

Example

```
amnesiac (config) # ntp enable
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show ntp"

ntp peer

Description

Enables an NTP peer.

Syntax

[no] ntp peer <hostname | ip-addr> [version <number>]

Parameters

<hostname | ip-addr>	Specify the NTP peer hostname or IP address.
<version <number>	Specify the NTP version number. You do not need to specify the version number for the **no ntp peer** command.

Usage

The **no** command option disables an NTP peer.

Example

```
amnesiac (config) # ntp peer 10.10.10.1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show ntp," "show ntp active-peers"

ntp peer key

Description

Configures an NTP peer with an authentication key ID.

Syntax

[no] ntp peer <host-name | ip-addr> key <key id>

Parameters

<hostname | ip-addr>	Specify the NTP peer hostname or IP address.
key <key id> [key id, ...]	Specify the key identifier. The key ID values must be in the range 1 - 65534. You can specify multiple key IDs in the same list, separated by commas. When specifying multiple key IDs separated by commas, you must enclose them in quotes.

Usage

The **no** command option removes the authentication key from the NTP peer configuration.

NTP authentication involves three steps that you can perform in any order:

- Configure a key ID using the **ntp authentication** command.
- Add the configured key ID to the trusted keys list using the **ntp authentication trusted-keys** command.
- Configure the NTP server or peer with the key ID using the **ntp server key** or **ntp peer key** command.

Example

```
amnesiac (config) # ntp peer 10.10.10.1 key 56732
```

Product

CMC, Steelhead appliance

Related Topics

"show ntp," "show ntp active-peers"

ntp server

Description

Configures an NTP server with the default NTP version number or with a specified version number.

Syntax

[no] ntp server <hostname | ip-addr> <cr> | [version <number>]

Parameters

<hostname | ip-addr>	Specify the hostname or IP address of the NTP server to synchronize with.
<version <number>	Specify the NTP version number of this server. You do not need to specify the version number for the **no ntp server** command.

Usage

The **no** command option removes an NTP server.

Example

```
amnesiac (config) # ntp server 10.10.10.1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show ntp," "show ntp active-peers"

ntp server enable

Description

Enables an NTP server.

Syntax

[no] ntp server <hostname | ip-addr > enable

Parameters

<hostname | ip-addr>	Specify the hostname or IP address of the NTP server.

Usage

The **no** command option removes an NTP server.

Example

```
amnesiac (config) # ntp server companyserver enable
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show ntp"

ntp server key

Description

Configures an NTP server with an authentication key ID.

Syntax

[no] ntp server <hostname | ip-addr> key <key id>

Parameters

<hostname | ip-addr>	Specify the hostname or IP address of the NTP server to authenticate.
key <key id>	Specify the key identifier. The key ID values must be in the range 1 - 65534.

Usage

The **no** version of the command removes the authentication key from the NTP server.

NTP authentication involves three steps that you can perform in any order:

- Configure a key ID using the **ntp authentication** command.
- Add the configured key ID to the trusted keys list using the **ntp authentication trusted-keys** command.
- Configure the NTP server or peer with the key ID using the **ntp server key** or **ntp peer key** command.

Example

```
amnesiac (config) # ntp server companyserver key 56732
```

Product

CMC, Steelhead appliance

Related Topics

"ntp authentication," "ntp authentication trustedkeys," "ntp peer key," "show ntp authentication"

telnet-server enable

Description

Enables you to access the CLI using telnet. This feature is disabled by default.

Syntax

[no] telnet-server enable

Parameters

None

Usage

You can use telnet to troubleshoot your system. It enables you to access the CLI from another system.

Example

```
amnesiac (config) # telnet-server enable
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show telnet-server"

AAA, Role-Based Management, Radius, and TACACS+ Commands

This section describes the AAA, role-based management, Radius, and TACACS+ commands. The Steelhead appliance supports authentication and authorization.

aaa accounting per-command default

Description

Configures per-command account settings.

Syntax

[no] aaa accounting per-command default <method>

Parameters

<method>	Specify the authentication method: **tacacs+** or **local**. Use a space-separated list.

Usage

The Steelhead appliance performs accounting based on the order in which you specify the methods.

The **no** command option clears all accounting states and returns the per-command accounting to the local method (local logs).

Example

```
amnesiac (config) # aaa accounting per-command default tacacs+ local
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show radius," "show tacacs"

aaa authentication cond-fallback

Description

Configures fall-back only if the server is unavailable.

Syntax

[no] aaa authentication cond-fallback

Parameters

None

Usage

If enabled, the Steelhead appliance tries the next authentication method only if the servers for the current authentication method are unavailable.

The **no** command option disables fall-back mode.

Example

```
amnesiac (config) # aaa authentication cond-fallback
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show radius," "show tacacs"

aaa authentication console-login default

Description

Configures local, RADIUS, or TACACS+ console settings for log in.

Syntax

aaa authentication console-login default <method>

Parameters

<method>	Specify the authentication method: **radius**, **tacacs+,** or **local**. Use a space-separated list.

Usage

The Steelhead appliance performs authentication based on the order in which you specify the methods.

The **no** command option clears all authentication states and returns user authentication to the local user name database.

Example

```
amnesiac (config) # aaa authentication console-login default radius tacacs+ local
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show radius," "show tacacs"

aaa authentication login default

Description

Configures local, RADIUS, or TACACS+ login settings.

Syntax

[no] aaa authentication login default <method>

Parameters

<method>	Specify the authentication method: **radius**, **tacacs+,** or **local**. Use a space-separated list.

Usage

The Steelhead appliance performs authentication based on the order in which you specify the methods.

The **no** command option clears all authentication states and returns user authentication to the local user name database.

Example

```
amnesiac (config) # aaa authentication login default radius tacacs+
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show radius," "show tacacs"

aaa authorization map default-user

Description

Configures what local user the authenticated user will be logged in as when they are authenticated (through RADIUS or TACACS+) and when they do not have a local user mapping specified in the remote database.

Syntax

[no] aaa authorization map default-user <user_name>

Parameters

<user_name>	Specify the user name for RADIUS or TACACS+ authentication: **admin** or **monitor**.

Usage

For the local authentication method, this setting is ignored. This mapping depends on the setting of the **aaa authorization map order** command.

The **no** command option disables user default mapping.

Example

```
amnesiac (config) # aaa authorization map default-user admin
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show protocol domain-auth test delegation server-privs," "show tacacs"

aaa authorization map order

Description

Sets the order for remote-to-local user mappings for RADIUS or TACACS+ server authentication.

Syntax

[no] aaa authorization map order <policy>

Parameters

<policy>	Specify the order in which to apply the authentication policy: **remote-only**, **remote-first**, or **local-only**.

Usage

The order determines how the remote user mapping behaves. If the authenticated user name is valid locally, the Steelhead appliance does not perform any mapping. The setting has the following behaviors:

- **remote-first** - If a local-user mapping attribute is returned and it is a valid local user name, map the authenticated user to the local user specified in the attribute. If the attribute is not present or not valid locally, use the user name specified by the default-user command. (This is the default behavior.)
- **remote-only** - Map only to a remote authenticated user if the authentication server sends a local-user mapping attribute. If the attribute does not specify a valid local user, no further mapping is attempted.
- **local-only** - All remote users are mapped to the user specified by the **aaa authorization map default-user <user name>** command. Any vendor attributes received by an authentication server are ignored.

To set TACACS+ authorization levels (**admin** and **read-only**) to allow certain members of a group to log in, add the following attribute to **users** on the TACACS+ server:

```
        service = rbt-exec {
                local-user-name = "monitor"
        }
```

where you replace **monitor** with **admin** for write access.

To turn off general authentication in the Interceptor appliance, enter the following command at the system prompt:

```
aaa authorization map order remote-only
```

The **no** command option disables authentication.

Example

```
amnesiac (config) # aaa authorization map order remote-only
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show radius," "show tacacs"

aaa authorization per-command default

Description

Configures authorization mapping settings.

Syntax

[no] aaa authorization per-command default <method>

Parameters

<method>	Specify the authentication method: **tacacs+** or **local**. Use a space-separated list.

Usage

The order in which the methods are specified is the order in which the authorization is attempted.

The **no** command option clears all authorization states and returns the user authorization to the local user name database.

Example

```
amnesiac (config) # aaa authorization per-command default tacacs+ local
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show radius," "show tacacs"

radius-server host

Adds a RADIUS server to the set of servers used for authentication.

Syntax

[no] radius-server host {<ip-addr> [auth-port <port> [auth-type <type>]]} [auth-type <type>] [timeout <seconds>] [retransmit <retries>] [key <string>]

Parameters

<ip-addr>	Specify the RADIUS server IP address.
auth-port <port>	Specify the authentication port number to use with this RADIUS server. The default value is 1812.
auth-type <type>	Specify the authentication type to use with this RADIUS server. • **chap** - Specify the challenge handshake authentication protocol (CHAP), which provides better security than PAP. • **pap** - Specify the password authentication protocol (PAP).
timeout <seconds>	Specify the time-out period to use with this RADIUS server.
retransmit <retries>	Specify the number of times the client attempts to authenticate with any RADIUS server. The default value is 1. The range is 0-5. To disable retransmissions, set it to 0.
key <string>	Specify the shared secret text string used to communicate with this RADIUS server. • **0** - Specify a shared secret to use with this RADIUS server. • **7** - Specify a RADIUS key with an encrypted string.

Usage

RADIUS servers are tried in the order they are configured.

The same IP address can be used in more than one **radius-server host** command if the **auth-port** value is different for each. The **auth-port** value is a UDP port number. The **auth-port** value must be specified immediately after the **host <ip-addr>** option (if present).

PAP authentication validates users before allowing them access to the RADIUS server resources. PAP is the most flexible protocol but is less secure than CHAP.

CHAP authentication validates the identity of remote clients by periodically verifying the identity of the client using a three-way handshake. This happens at the time of establishing the initial link and might happen again at any time afterwards. CHAP bases verification on a user password and transmits an MD5 sum of the password from the client to the server.

Some parameters override the RADIUS server global defaults. For details, see the *Steelhead Appliance Deployment Guide*.

The **no** command option stops sending RADIUS authentication requests to the host.

If **no radius-server host <ip-addr>** is specified, all radius configurations for the host are deleted.

The **no radius-server host <ip-addr> auth-port <port>** command can be specified to refine which host is deleted, as the previous command deletes all RADIUS servers with the specified IP address.

Example

```
amnesiac (config) # radius-server host 10.0.0.1 timeout 10 key XXXX retransmit 3
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show radius"

radius-server key

Sets the shared secret text string used to communicate with a RADIUS server.

Syntax

[no] radius-server key <string>

Parameters

<string>	Sets the shared secret text string used to communicate with a RADIUS server.

Usage

This command can be overridden using the **radius-server host** command.

The **no** command option resets the key to the default value.

Example

```
amnesiac (config) # radius-server key XYZ
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show radius"

radius-server retransmit

Specify the number of times the client attempts to authenticate with a RADIUS server.

Syntax

[no] radius-server retransmit <retries>

Parameters

<retries>	Specify the number of times the client attempts to authenticate with a RADIUS server. The range is 0-5. The default value is 1.

Usage

This command can be overridden in a **radius-server host** command.

The **no** command option resets the value to the default value.

Example

```
amnesiac (config) # radius-server retransmit 5
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show radius"

radius-server timeout

Description

Sets the time-out period, in seconds, for retransmitting a request to a RADIUS server.

Syntax

[no] radius-server timeout <seconds>

Parameters

<seconds>	Sets the time-out for retransmitting a request to a RADIUS server. The range is 1-60. The default value is 3.

Usage

This command can be overridden in a **radius-server host** command.

The **no** command option resets the value to the default value.

Example

```
amnesiac (config) # radius-server timeout 30
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show radius"

rbm user

Description

Assigns a a role (that is, a feature set) to a user. A user can be associated with one or more roles.

Syntax

[no] rbm user <username> role <role> permissions <permissions>

Parameters

<username>	Specify the user name.
role <role>	Specify a role-based management type: • **acceleration_service** - Start and stop the optimization service. • **basic_diagnostics** - Customizes system diagnostic logs, but does not include TCP dumps. • **cifs_acceleration** - Enable CIFS optimization settings and Overlapping Open Optimization. • **citrix_acceleration** - Configure Citrix ICA optimization. • **general_settings** - Per source IP connection limit and the maximum connection pooling size. • **granite** - Configure Granite branch storage service. Branch storage services are only available on the Steelhead EX appliance. • **http_acceleration** - HTTP optimization settings including: cache settings, keep-alive, insert cookie, file extensions to prefetch, and ability to set up HTTP optimization for a specific server subnet. • **in-path_rules** - Configure which TCP traffic to optimize and how to optimize traffic by setting in-path rules. Includes WAN visibility to preserve TCP/IP address or port information. • **jinitiator_acceleration** - Optimize Oracle E-business application content and forms applications. • **mapi_acceleration** - Optimize MAPI, set Exchange and NSPI ports. • **network_settings** - Configure host and network interface settings, including DNS cache settings. • **nfs_acceleration** - Configure NFS optimization. • **notes_acceleration** - Configure Lotus Notes optimization. • **path_selection -** Configure path selection. • **proxy_file_service** - Enable the Proxy File Service. • **qos** - Enforce QoS policies. • **replication_acceleration** - Configure the SDRF/A and FCIP storage optimization modules. • **reports** - Set system report parameters. • **riverbed_services_platform** - Add various types of functionality into a virtualized environment on the client Steelhead appliance. The functionality can include a print server, a streaming video server and a package that provides core networking services (DNS, DHCP, TFTP and Radius mirroring). • **security_settings** - Configure security settings, including RADIUS and TACACS authentication settings and secure vault password. • **sql_acceleration** - Configure MS-SQL optimization. • **ssl_acceleration** - Configure SSL support. • **tcp_dump** - Configure TCP dump utility. • **virtual_services_platform** - Add various types of basic services (such as print, DNS, and DHCP services) in the branch to run in a virtualized environment on a Steelhead EX appliance. VSP uses ESXi 5.0 as the virtualization platform. • **windows_domain_auth** - Configure Windows domain authentication.
permissions <permissions>	You can also create users, assign passwords to the user, and assign varying configuration roles to the user. A user role determines whether the user has permission to: • **read-only** - With read privileges you can view current configuration settings but you cannot change them. • **read-write** - With write privileges you can view settings and make configuration changes for a feature. • **deny** - With deny privileges you cannot view settings or make configuration changes for a feature.

Usage

The **no** command option allows for the deletion of a role. Only users with administrative privileges can execute the **rbm user** command.

Example

```
amnesiac (config) # rbm user helpdesk role general_settings permissions read-only
```

Product

Steelhead appliance, CMC, CSH

Related Topics

"show rbm user"

tacacs-server first-hit

Description

Enables a first-hit option for TACACS+ servers.

Syntax

[no] tacacs-server first-hit <ip-addr>

Parameters

<ip-addr>	Specify the TACACS+ server IP address.

Usage

TACACS+ servers are tried in the order they are configured. If this option is enabled, only the first server in the list of TACACS+ servers is queried for authentication and authorization purposes.

The **no** command option disables TACACS+ first-hit option.

Example

```
amnesiac (config) # tacacs-server first-hit 10.0.0.1
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show tacacs"

tacacs-server host

Description

Adds a TACACS+ server to the set of servers used for authentication.

Syntax

[no] tacacs-server host {<ip-addr> <cr>| auth-port <port> | auth-type <type> | timeout <seconds> | retransmit <retries> | [key <string> | key 0 | key 7]}

Parameters

<ip-addr>	Specify the TACACS+ server IP address.
auth-port <port>	Specify the authorization port number. The default value is 49.\
auth-type <type>	Specify the authorization type to use with this TACACS+ server: ascii, pap.
timeout <seconds>	Sets the time-out for retransmitting a request to any TACACS+ server. The range is 1-60. The default value is 3.
retransmit <number>	Specify the number of times the client attempts to authenticate with any TACACS+ server. The default value is 1. The range is 0-5. To disable retransmissions set it to 0.
key <keynumber> | key 0 | key 7	Specify the shared secret text string used to communicate with this TACACS+ server. • **0** - Specify a shared secret to use with this RADIUS server. • **7** - Specify a TACACS+ key with an encrypted string.

Usage

TACACS+ servers are tried in the order they are configured.

The same IP address can be used in more than one **tacacs-server host** command if the **auth-port** value is different for each. The **auth-port** value is a UDP port number. The **auth-port** value must be specified immediately after the **hostname** option (if present).

Some of the parameters given can override the configured global defaults for all TACACS+ servers. For details, see the *Steelhead Appliance Deployment Guide*.

If **no tacacs-server host <ip-addr>** is specified, all TACACS+ configurations for this host are deleted. The **no tacacs-server host <ip-addr> auth-port <port>** command can be specified to refine which host is deleted, as the previous command deletes all TACACS+ servers with the specified IP address.

The **no** command option disables TACACS+ support.

Example

```
amnesiac (config) # tacacs-server host 10.0.0.1
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show tacacs"

tacacs-server key

Description

Sets the shared secret text string used to communicate with any TACACS+ server.

Syntax

[no] tacacs-server key <string>

Parameters

<string>	Sets the shared secret text string used to communicate with any TACACS+ server.

Usage

The **tacacs-server key** command can be overridden using the **tacacs-server host** command. The **no** command option resets the value to the default value.

Example

```
amnesiac (config) # tacacs-server key XYZ
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show tacacs"

tacacs-server retransmit

Description

Configures the number of times the client attempts to authenticate with any TACACS+ server.

Syntax

[no] tacacs-server retransmit <retries>

Parameters

<retries>	Specify the number of times the client attempts to authenticate with any TACACS+ server. The range is 0-5. The default value is 1. To disable retransmissions set it to 0.

Usage

The **tacacs-server retransmit** command can be overridden in a **tacacs-server host** command.

The **no** command option resets the value to the default value.

Example

```
amnesiac (config) # tacacs-server retransmit 5
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show tacacs"

tacacs-server timeout

Description

Sets the time-out period for retransmitting a request to any TACACS+ server.

Syntax

[no] tacacs-server timeout <seconds>

Parameters

<seconds>	Sets the time-out for retransmitting a request to any TACACS+ server. The range is 1-60. The default value is 3.

Usage

This command can be overridden with the **tacacs-server host** command.

The **no** command option resets the value to the default value.

Example

```
amnesiac (config) # tacacs-server timeout 30
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show aaa," "show tacacs"

username disable

Description

Disables the account so that no one can log in.

Syntax

[no] username <userid> disable

Parameters

<userid>	Specify the user login: **admin** or **monitor**.

Usage

The **no** command option re-enables the specified user account.

Example

```
amnesiac (config) # username monitor disable
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show usernames"

username nopassword

Description

Disables password protection for a user.

Syntax

username <userid> nopassword

Parameters

<userid>	Specify the user login: **admin** or **monitor**.

Example

```
amnesiac (config) # username monitor nopassword
```

Product

CMC, Interceptor appliance, Steelhead appliance

Related Topics

"show usernames"

username password

Description

Sets the password for the specified user.

Syntax

username <userid> password <cleartext> [old-password <cleartext>]

Parameters

<userid>	Specify the user login: **admin** or **monitor**.
<cleartext>	Specify the password. The password must be at least 6 characters.
old-password	Specify the old password.

Usage

The password is entered in cleartext format on the command line.

The **old-password** option allows you to check the minimum character difference between the old and new passwords under account control management.

Example

```
amnesiac (config) # username admin password xyzzzZ
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller

Related Topics

"show usernames," "Account Control Management Commands"

username password 0

Description

Sets the password for the specified user.

Syntax

username <userid> password 0 <cleartext password>

Parameters

<userid>	Specify the user login: **admin** or **monitor**.
<cleartext password>	Specify the password. The password must be at least 6 characters.

Usage

The password is entered in cleartext format on the command line.

Example

```
amnesiac (config) # username admin password 0 xyzzzZ
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller

Related Topics

"show usernames"

username password 7

Description

Sets the password for the specified user using the encrypted format of the password. Use this command if it becomes necessary to restore your appliance configuration, including the password.

Syntax

username <userid> password 7 <encrypted password>

Parameters

<userid>	Specify the user login: **admin** or **monitor**.
<encrypted password>	Specify the encrypted password. The password must be at least 6 characters.

Usage

Use this command to restore your password using an encrypted version of the password. You can display the encrypted version of the password using the **show running configuration** command.

For example, executing **username monitor password awesomepass** results in the following line being added to the running configuration file:

```
username monitor password 7 $1$f2Azp8N8$n0oy6Y1KhCfuMo93f24ku/
```

If you need to restore your password in the future, you would paste:

```
username monitor password 7 $1$f2Azp8N8$n0oy6Y1KhCfuMo93f24ku/
```

in the CLI, to restore your monitor password to **awesomepass**.

Example

```
amnesiac (config) # username admin password 7 $1$f2Azp8N8$n0oy6Y1KhCfuMo93f24ku/
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller

Related Topics

"show usernames"

Account Control Management Commands

This section describes the Account Control Management commands.

authentication policy enable

Description

Enables the authentication policy for account control.

Syntax

[no] authentication policy enable

Parameters

None

Usage

An authentication policy enables you to define a set of policies to enforce user login behavior and password strength. Passwords are mandatory when account control is enabled.

After you enable the authentication policy, the current passwords for all users expire. At the next login, each user is prompted to change their password, placing the new password under the account control authentication policy.

When account control is enabled and an administrator uses the **username password 7** command, the password automatically expires. Because the encrypted password cannot be checked against the configured password policy, the user is prompted to change their password at login.

Example

```
amnesiac (config) # authentication policy enable
```

Product

CMC, Steelhead appliance

Related Topics

"show alarm," "username password 7"

authentication policy login max-failures

Description

Sets the maximum number of unsuccessful login attempts before temporarily locking the user's access to the Steelhead appliance.

Syntax

authentication policy login max-failures <count> [unlock-time <seconds>]

no authentication policy login max-failures

Parameters

<count>	Specify the maximum number of unsuccessful login attempts before a temporary account lockout.
unlock-time <seconds>	Specify the number of seconds the system waits before the user can log in again after an account lockout. If this optional parameter is not specified, the unlock time defaults to 300 seconds.

Usage

The **no authentication policy login max-failures** command resets the maximum number of unsuccessful login attempts allowed to the default value, which is zero, indicating that the account lockout is disabled.

Example

```
amnesiac (config) # authentication policy login max-failures 3
```

Product

CMC, Steelhead appliance

Related Topics

"show alarm"

authentication policy password

Description

Configures the authentication policy password settings for account control.

Syntax

[no] authentication policy password {change-days <days> | dictionary enable | difference <count>| expire <days> [warn] | length <length> | lock <days> | lower-case <count> | numeric <count> | repeat <count> | reuse-interval <count> | special <count> | upper-case <count>}

Parameters

change-days <days>	Specify the minimum number of days before which passwords cannot be changed.
dictionary enable	Prevents the use of any word found in the dictionary as a password.
difference <count>	Specify the minimum number of characters that must change between an old and new password. The default for the strong security template is 4. If the **authentication policy password difference <count>** value is set to a value greater than zero, a non-administrator must specify the new and old passwords by entering the **username password [old-password]** command. Administrators are never required to enter an old password when changing an account password.
expire <days>	Specify the number of days the current password stays in effect. To set the password expiration to 24 hours, specify 0. To set the password expiration to 48 hours, specify 1. Specify a negative number to turn off password expiration.
warn <days>	Specify the number of days to warn a user of an expiring password before the password expires. The default for the strong security template is 7.
length <length>	Specify the minimum password length. The default setting for the strong security template is 14 alphanumeric characters.
lock <days>	Specify the number of days before an account with an expired password locks.
lower-case <count>	Specify the minimum number of lowercase letters required in the password. The default for the strong security template is 1.
numeric <count>	Specify the minimum number of numeric characters required in the password. The default for the strong security template is 1.
repeat <count>	Specify the maximum number of times a character can occur consecutively.
reuse-interval <count>	Specify the number of password changes allowed before a password can be reused. The default for the strong security template is 5.
special <count>	Specify the minimum number of special characters required in the password. The default for the strong security template is 1.
upper-case <count>	Specify the minimum number of uppercase letters required in the password. The default for the strong security template is 1.

Usage

Passwords are mandatory when account control is enabled. Passwords for all users expire as soon as account control is enabled. This behavior forces the user to create a new password that follows the password characteristics defined in the password policy.

When account control is enabled and an administrator uses the **username password 7** command, the password automatically expires. Because the encrypted password cannot be checked against the configured password policy, the user is prompted to change their password at log in.

Empty passwords are not allowed when account control is enabled.

Example

```
amnesiac (config) # authentication policy password expire 60 warn 3
```

Product

CMC, Steelhead appliance

Related Topics

“authentication policy template,” “username password,” “username password 7,” “show alarm”

authentication policy template

Description

Specify the authentication policy template for password policy configuration.

Syntax

authentication policy template {strong | basic}

Parameters

strong	Specifies the strong security policy template.
basic	Specifies the basic security policy template.

Usage

The **authentication policy template strong** command sets the password policy to more stringent enforcement settings. Selecting this template automatically prepopulates the password policy with stricter settings commonly required by higher security standards, such as for the Department of Defense.

To remove the strong security template and return to the basic password policy, use the **authentication policy template basic** command.

When account control is enabled for the first time, the password policy is set to the basic template.

Example

```
amnesiac (config) # authentication policy template strong

amnesiac #  show authentication policy
Authentication policy enabled:                        yes
Maximum unsuccessful logins before account lockout:   3
      Wait before account unlock:                     300 Seconds
Minimum password length:                              14
Minimum upper case characters in password:            1
Minimum lower case characters in password:            1
Minimum numerical characters in password:             1
Minimum special characters in password:               1
Minimum interval for password reuse:                  5
Minimum characters diff for password change:          4
Prevent dictionary words in password:                 yes
User passwords expire:                                60 days
Warn user of an expiring password:                    7 days before
User accounts with expired passwords lock:            305 days

amnesiac (config) # authentication policy template basic

amnesiac #  show authentication policy
Authentication policy enabled:                        yes
Maximum unsuccessful logins before account lockout:   none
      Wait before account unlock:                     300 Seconds
Minimum password length:                              6
Minimum upper case characters in password:            0
Minimum lower case characters in password:            0
Minimum numerical characters in password:             0
Minimum special characters in password:               0
Minimum interval for password reuse:                  0
Minimum characters diff for password change:          0
Prevent dictionary words in password:                 yes
User passwords expire:                                never
Warn user of an expiring password:                    7 days before
User accounts with expired passwords lock:            never
```

Product

CMC, Steelhead appliance

Related Topics

"show alarm"

authentication policy user lock never

Description

Configures the user account lock settings for account control management.

Syntax

[no] authentication policy user <username> lock never

Parameters

<username>	Specify the user login: **admin**, **monitor**, or **shark**.

Usage

The **authentication policy user lock never** command prevents the user's account from being locked after the password expires. This command is available only when account control is enabled.

The **no authentication policy user lock never** command allows the user account to be locked after the password expires.

Example

```
amnesiac (config) # authentication policy user admin lock never
```

Product

CMC, Steelhead appliance

Related Topics

"show alarm"

authentication policy user login-failures reset

Description

Resets a user account so the user can log in again.

Syntax

[no] authentication policy user <username> login-failures reset

Parameters

<username>	Specify the user login: **admin**, **monitor**, or **shark**.

Usage

If a user account is locked because of a failed login count exceeding the configured value, the **authentication policy user login-failures reset** command resets the account so the user can log in again. This command resets the login count to zero, which is the default value.

Example

```
amnesiac (config) # authentication policy user admin login-failures reset
```

Product

CMC, Steelhead appliance

Related Topics

"show alarm"

ACL Management Commands

This section describes the ACL management commands. For details, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

access enable

Description

Enables secure access to a Steelhead appliance using an internal management Access Control List (ACL).

Syntax

[no] access enable

Parameters

None

Usage

Steelhead appliances are subject to the network policies defined by corporate security policy, particularly in large networks. Using an internal management ACL you can:

- restrict access to certain interfaces or protocols of a Steelhead appliance.
- restrict inbound IP access to a Steelhead appliance, protecting it from access by hosts that do not have permission without using a separate device (such as a router or firewall).
- specify which hosts or groups of hosts can access and manage a Steelhead appliance by IP address, simplifying the integration of Steelhead appliances into your network. You can also restrict access to certain interfaces or protocols.

This feature provides the following safeguards to prevent accidental disconnection from the Steelhead appliance (or the CMC):

- It detects the IP address you are connecting from and displays a warning if you add a rule that denies connections to that address.
- It always allows the default Steelhead appliance ports 7800, 7801, 7810, 7820, and 7850.
- It always allows a previously-connected CMC to connect and tracks any changes to the IP address of the CMC to prevent disconnection.
- It converts well-known port and protocol combinations such as SSH, Telnet, HTTP, HTTPS, SNMP, and SOAP into their default management service and protects these services from disconnection. For example, if you specify protocol 6 (TCP) and port 22, the management ACL converts this port and protocol combination into SSH and protects it from denial.
- It tracks changes to default service ports and automatically updates any references to changed ports in the access rules.
- You can also change the standard port for HTTPS (443) to match your management standards using the "web https port" and "web http port" commands.

Usage Notes

- When you change the default port of services (SSH, HTTP, HTTPS, and so on) on either the client or server-side Steelhead appliance and then create a management ACL rule denying that service, the rule will not work as expected. The Steelhead appliance on the other end (either server or client) of an in-path deployment does not know that the default service port has changed, and therefore optimizes the packets to that service port. To avoid this problem, add a pass-through rule to the client-side Steelhead appliance for the management interfaces. The pass-through rule prevents the traffic from coming from the local host when optimized.
- A management ACL rule that denies access to port 20 on the server-side Steelhead appliance in an out-of-path deployment prevents data transfer using active FTP. In this deployment, the FTP server and client cannot establish a data connection because the FTP server initiates the SYN packet and the management rule on the server-side Steelhead appliance blocks the SYN packet. To work around this problem, use passive FTP instead. With passive

FTP, the FTP client initiates both connections to the server. For details about active and passive FTP, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

The **no** command option disables management ACL.

Example

```
amnesiac (config) # access enable
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show access inbound rules," "show access status"

access inbound rule add

Description

Adds a secure access inbound rule.

Syntax

[no] access inbound rule add [allow | deny] protocol <protocol number> service <service> dstport <port> srcaddr <ip-addr> interface <interface> description <description> rulenum <rulenum> | [log {on | off}] | [override]

Parameters

allow | deny	Specify the action on the rule: • **allow** - Allows a matching packet access to the Steelhead appliance. This is the default action. • **deny** - Denies access to any matching packets.
protocol <protocol number>	Specify **all**, **icmp**, **tcp**, **udp**, or protocol number (**1**, **6**, **17**) in IP packet header. The default setting is **all**.
service <service>	Optionally, specify the service name: **http**, **https**, **snmp**, **ssh, soap**, **telnet**
dstport <port>	Optionally, specify the destination port of the inbound packet. You can also specify port ranges: 1000-30000
srcaddr <ip-addr>	Optionally, specify the source subnet of the inbound packet; for example, 1.2.3.0/24
interface <interface>	Optionally, specify an interface name: **primary**, **aux**, **inpath0_0**.
rulenum <rulenum>	Optionally, specify a rule number from **1** to **N**, **start**, or **end**. The Steelhead appliances evaluate rules in numerical order starting with rule **1**. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule **1** do not match, rule **2** is consulted. If rule **2** matches the conditions, it is applied, and no further rules are consulted.
description <description>	Optionally, specify a description to facilitate communication about network administration.
log [on | off]	Optionally, specify to track denied packets in the log. By default, packet logging is enabled.
override	Specify to ignore the warning and force the rule modification. If you add, delete, edit, or move a rule that could disconnect you from the Steelhead appliance, a warning message appears. You can specify **override** to ignore the warning and force the rule modification. Use caution when you override a disconnect warning.

Usage

The management ACL contains rules that define a match condition for an inbound IP packet. You set a rule to allow or deny access to a matching inbound IP packet. When you add a rule on a Steelhead appliance, the destination specifies the Steelhead appliance itself, and the source specifies a remote host.

The ACL rules list contains default rules that allow you to use the management ACL with the RiOS features PFS, DNS caching, and RSP. These default rules allow access to certain ports required by these features. The list also includes a default rule that allows access to the CMC. If you delete the default ACL rules for one of these features and need to restore it.

To restore the default rule for PFS

```
access inbound rule add allow protocol tcp dstport 445 description "PFS Support" rulenum 1
access inbound rule add allow protocol tcp dstport 139 description "PFS Support" rulenum 1
access inbound rule add allow protocol udp dstport 137-138 description "PFS Support" rulenum 1
```

To restore the default rule for RSP

```
access inbound rule add allow protocol tcp dstport 8222 description "Allow RSP Console" rulenum 1
access inbound rule add allow protocol tcp dstport 8333 description "Allow RSP Console" rulenum 1
```

To restore the default rule for DNS cache

```
access inbound rule add allow protocol udp dstport 53 description "DNS Caching" rulenum 1
```

If you have a firewall rule set on server-side Steelhead appliance that prevents access to the server-side Steelhead appliance, you might not be able to transfer data using active FTP in out-of-path deployments. To solve this problem, Riverbed recommends you use passive FTP or if you have permission to change the configuration on the server-side Steelhead appliance you can add a rule to allow packets from source port 20. For example:

```
access inbound rule add allow protocol tcp srcport 20
```

To delete a rule, use the syntax:
no access inbound rule <rulenum>

Example

```
amnesiac (config) # access inbound rule add allow protocol tcp/udp
dstport 1234 srcaddr 10.0.0.1/16 interface primary rulenum 2
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show access inbound rules," "show access status"

access inbound rule edit rulenum

Description

Modifies a secure access inbound rule.

Syntax

[no] access inbound rule edit rulenum <rulenum> action [allow | deny] [protocol <protocol number> service <service> dstport <port>| srcaddr <ip-addr> | interface <interface> | description <description>] | log [on | off] | [override]

Parameters

rulenum <rulenum>	Optionally, specify a rule number from **1** to **N**, **start**, or **end**. Steelhead appliances evaluate rules in numerical order starting with rule **1**. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule **1** do not match, rule **2** is consulted. If rule **2** matches the conditions, it is applied, and no further rules are consulted.
action [allow | deny]	Specify the action on the rule: • **allow** - Allows a matching packet access to the Steelhead appliance. This is the default action. • **deny** - Denies access to and logs any matching packets.
protocol <protocol number>	Specify **all**, **icmp**, **tcp**, **udp**, or protocol number (**1**, **6**, **17**) in IP packet header. The default setting is **all**.
service <service>	Optionally, specify the service name: **http**, **https**, **snmp**, **ssh, telnet**
dstport <port>	Specify the destination port. You can also specify port ranges: 1000-30000
srcaddr <subnet>	Specify the source subnet. For the subnet address, use the format XXX.XXX.XXX.XXX/XX.
interface <interface>	Specify the interface: **primary**, **aux**, **inpath0_0**
description <description>	Optionally, specify a description to facilitate communication about network administration.
log [on | off]	Optionally, specify to enable or disable log in on this command.\
override	Specify to ignore the warning and force the rule modification. If you add, delete, edit, or move a rule that could disconnect you from the Steelhead appliance, a warning message appears. You can specify **override** to ignore the warning and force the rule modification. Use caution when overriding a disconnect warning.

Example

```
amnesiac (config) # access inbound rule edit action allow dstport 1234 srcaddr 10.0.0.1/16 service
http interface primary rulenum 2
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show access inbound rules," "show access status"

access inbound rule move

Description

Moves a secure access inbound rule.

Syntax

[no] access inbound rule move <rulenum>] to <rulenum> [override]

Parameters

rulenum <rulenum>	Specify a rule number from **1** to N, **start**, or **end**. Steelhead appliances evaluate rules in numerical order starting with rule 1. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.
override	Specify to ignore the warning and force the rule modification. If you add, delete, edit, or move a rule that could disconnect you from the Steelhead appliance, a warning message appears. You can specify **override** to ignore the warning and force the rule modification. Use caution when overriding a disconnect warning.

Example

```
amnesiac (config) # access inbound rule move 2 to 4
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show access inbound rules," "show access status"

Secure Shell Access Commands

This section describes the secure shell access commands.

ssh client generate identity user

Description

Generates SSH client identity keys for the specified user. SSH provides secure log in for Windows and UNIX clients and servers.

Syntax

ssh client generate identity user <user>

Parameters

<user>	Specify the client user login.

Usage

The **no ssh client identity user <user>** command disables SSH client identity keys for a specified user.

Example

```
amnesiac (config) # ssh client generate identity user test
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller

Related Topics

"show ssh client"

ssh client user authorized-key key sshv2

Description

Sets the RSA encryption method by RSA Security and authorized-key for the SSH user.

Syntax

[no] ssh client user <user> authorized-key key sshv2 <public key>

Parameters

<user>	Specify the user name. Must be an existing local user.
<public key>	Specify the public key for SSH version 2 for the specified SSH user.

Usage

The **no** command option disables the authorized-key encryption method.

Example

```
amnesiac (config) # ssh client user admin authorized-key key sshv2 MyPublicKey
```

Product

Steelhead appliance, CMC, Interceptor appliance, CSH

Related Topics

"show ssh client"

ssh server allowed-ciphers

Description

Sets the list of allowed ciphers for ssh server.

Syntax

[no] ssh server allowed-ciphers <ciphers>

Parameters

<ciphers>	Specify cipher or comma separated list of ciphers, in quotation marks. Default ciphers configured are aes128-ctr, aes192-ctr, and aes256-ctr. Supported ciphers are: • aes128-cbc • 3des-cbc • blowfish-cbc • cast128-cbc • arcfour • aes192-cbc • aes256-cbc • aes128-ctr • aes192-ctr • aes256-ctr

Usage

The **no** command option resets the SSH server allowed ciphers.

Example

```
amnesiac (config) # ssh server allowed-ciphers "aes128-ctr,aes192-ctr,aes256-ctr"
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller

Related Topics

"show ssh server"

---

ssh server enable

Description

Enables SSH access to the system.

Syntax

[no] ssh server enable

Parameters

None

Usage

The **no** command option disables SSH access.

Example

```
amnesiac (config) # ssh server enable
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show ssh server"

---

ssh server listen enable

Description

Enables SSH interface restriction access to the system (that is, it enables access control and blocks requests on all the interfaces).

Syntax

[no] ssh server listen enable

Parameters

None

Usage

If the list of interfaces is empty, none of the interfaces respond to the queries.

The **no** command option disables SSH interface restrictions which causes SSH to accept connections from all interfaces.

SSH interface restrictions are not available through the Management Console.

Example

```
amnesiac (config) # ssh server listen enable
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show ssh server"

ssh server listen interface

Description

Adds one or more interfaces to the SSH server access restriction list (thus, it unblocks requests on the specified interface).

Syntax

[no] ssh server listen interface <interface>

Parameters

<interface>	Specify the interface: **primary**, **aux**, **inpath0_0**, **inpath0_1**, **rios-lan0_0**, **rios_wan0_0**

Usage

If the list of interfaces is empty, none of the interfaces respond to the queries. If the list of interfaces has at least one entry, then the server listens on that subset of interfaces.

To add an interface to the list

```
ssh server listen interface primary
```

To remove an interface

```
no ssh server listen interface <interface>
```

The **no** command option removes the interface.

SSH interface restrictions are not available through the Management Console

Example

```
amnesiac (config) # ssh server listen interface primary
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show ssh server"

ssh server port

Description

Sets a port for SSH access.

Syntax

[no] ssh server port <port>

Parameters

<port>	Specify a port for SSH access.

Usage

The **no** command option resets the SSH port to its default.

Example

```
amnesiac (config) # ssh server port 8080
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller

Related Topics

"show ssh server"

ssh server v2-only enable

Description

Enables SSH server to accept only v2 connections, which are more secure.

Syntax

[no] ssh server v2-only enable

Parameters

None

Usage

This command restricts the server to accept only v2 protocol connections, which are more secure.

The **no** command option removes the restriction.

Example

```
amnesiac (config) # ssh server v2-only enable
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show ssh server"

CLI Terminal Configuration Commands

This section describes the CLI terminal configuration commands.

banner login

Description

Creates the system log in banner.

Syntax

[no] banner login <message string>

Parameters

<message string>	Specify the login banner message. Enclose the message in quotation marks.

Usage

The **no** command option disables the login banner.

Example

```
amnesiac (config) # banner login "reminder: meeting today"
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show bootvar"

banner motd

Description

Creates the system Message of the Day banner.

Syntax

[no] banner motd <message string>

Parameters

<message string>	Specify the login Message of the Day. Enclose the message in quotation marks.

Usage

The **no** command option disables the system Message of the Day banner.

Example

```
amnesiac (config) # banner motd "customer visit today"
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show bootvar"

cli clear-history

Description

Clears the command history for the current user.

Syntax

cli clear-history

Parameters

None

Example

```
amnesiac (config) # cli clear-history
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show cli"

cli default auto-logout

Description

Sets the keyboard inactivity time for automatic log out.

Syntax

[no] cli default auto-logout <minutes>

Parameters

<minutes>	Specify the number of minutes before log out occurs.

Usage

Suppose you are using telnet versus ssh to access your Steelhead appliances and thus have enabled a telnet server.

To disable timeout

```
   cli default auto-logout 0
```

The **no** command option disables the automatic logout feature.

Example

```
amnesiac (config) # cli default auto-logout 25
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show cli"

cli default paging enable

Description

Sets the ability to view text one screen at a time.

Syntax

[no] cli default paging enable

Parameters

None

Usage

The **no** command option disables paging.

Example

```
amnesiac (config) # cli default paging enable
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show cli"

cli session

Description

Sets CLI options for the current session only.

Syntax

[no] cli session {auto-logout <minutes> | paging enable | terminal length <lines> |terminal type <terminal_type> | terminal width <number of characters>}

Parameters

auto-logout <minutes>	Sets the number of minutes before the CLI automatically logs out the user. The default value is 15 minutes. The **no** command option disables the automatic logout feature.
paging enable	Sets paging. With paging enabled, if there is too much text to fit on the page, the CLI prompts you for the next page of text. The **no** command option disables paging.
terminal length <lines>	Sets the terminal length. The **no** command option disables the terminal length.
terminal type <terminal_type>	Sets the terminal type. The **no** command option disables the terminal type.
terminal width <number of characters>	Sets the terminal width. The **no** command option disables the terminal width.

Usage

The **no** command option disables CLI option settings.

Example

```
amnesiac (config) # cli session auto-logout 20
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show cli"

Web Configuration Commands

This section describes the Management Console configuration commands.

web auto-logout

Description

Sets the number of minutes before the Management Console automatically logs out the user.

Syntax

[no] web auto-logout <minutes>

Parameters

<minutes>	Specify the number of minutes before the system automatically logs out the user. The default value is 15 minutes.

Usage

The **no** command option disables the automatic log out feature.

Example

```
amnesiac (config) # web auto-logout 20
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web auto-refresh timeout

Description

Enables session timeouts on auto-refreshing report pages.

Syntax

[no] web auto-refresh timeout

Parameters

None

Usage

Disabling this feature keeps you logged in indefinitely on a report page that is auto-refreshing. This can be a security risk.

The **no** command option disables time-out.

Example

```
amnesiac (config) # web auto-refresh timeout
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web enable

Description

Enables the Management Console.

Syntax

[no] web enable

Parameters

None

Usage

The Management Console is enabled by default.

The **no** command option disables the Management Console.

Example

```
amnesiac (config) # web enable
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web http enable

Description

Enables HTTP access to the Management Console.

Syntax

[no] web http enable

Parameters

None

Usage

The Management Console is enabled by default.

The **no** command option disables the Management Console.

Example

```
amnesiac (config) # web http enable
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web http port

Description

Sets the Web port for HTTP access.

Syntax

[no] web http port <port>

Parameters

<port>	Specify the port number. The default value is 80.

Usage

The **no** command option resets the Web port to the default value.

Example

```
amnesiac (config) # web http port 8080
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web httpd listen enable

Description

Restricts Web interface access to this system (that is, it enables access control and blocks requests on all the interfaces).

Syntax

[no] web httpd listen enable

Parameters

None

Usage

The **no** command option disables Web interface restrictions.

Web interface restrictions are not available through the Management Console.

Example

```
amnesiac (config) # web httpd listen enable
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web httpd listen interface

Description

Adds an interface to the Web server access restriction list.

Syntax

[no] web httpd listen interface <interface>

Parameters

<interface>	Specify the interface: **primary**, **aux**, **inpath0_0**, **rios-lan0_0**, **rios_wan0_0**

Usage

If the list of interfaces is empty, none of the interfaces respond to the queries. If the list of interfaces has at least one entry, then the server listens on that subset of interfaces.

To add an interface to the list to listen on

```
web httpd listen interface primary
```

To remove an interface so that it is no longer listened to

```
no web httpd listen interface <interface>
```

Web interface restrictions are not available through the Management Console.

Example

```
amnesiac (config) # web httpd listen interface aux
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web https enable

Description

Enables HTTPS access to the Web-based management console.

Syntax

[no] web https enable

Parameters

None

Usage

The **no** command option disables access to the Web-based management console.

Example

```
amnesiac (config) # web https enable
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web https port

Description

Sets the HTTPS secure Web port.

Syntax

[no] web https port <port>

Parameters

<port>	Specify the port number. The default value is **80**.

Usage

The **no** command option disables support on a secure port.

Example

```
amnesiac (config) # web https port 8080
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web prefs graphs anti-aliasing

Description

Enables anti-aliasing for graphics in the Management Console.

Syntax

[no] web prefs graphs anti-aliasing

Parameters

None

Usage

The **no** command disables this feature.

Example

```
amnesiac (config) # web prefs graphs anti-aliasing
```

Product

Steelhead appliance, CSH

Related Topics

"show web prefs"

web prefs log lines

Description

Sets the number of lines for the system log page.

Syntax

[no] web prefs log lines <number>

Parameters

<number>	Specify the number of lines per log page.

Usage

The **no** command option disables the number of log lines.

Example

```
amnesiac (config) # web prefs logs lines 10
```

Product

Steelhead appliance, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web proxy host

Description

Sets the HTTP, HTTPS, and FTP proxy.

Syntax

[no] web proxy host <ip-addr> [port <port>] [user-cred username <username> password <password> [authtype <authentication type>]]

Parameters

<ip-addr>	Specify the IP address for the host.
port <port>	Specify the port for the host.
user-cred username <username> password <password>	Optionally, specify the user credentials for the autolicensing feature: • **username <username>** - Specify the user name. • **password <password>** - Specify the password, in cleartext format.
authtype <authentication type>	Optionally, specify the authentication type: • **basic** - Authenticates user credentials by requesting a valid user name and password. This is the default setting. • **digest** - Provides the same functionality as basic authentication; however, digest authentication improves security because the system sends the user credentials across the network as a Message Digest 5 (MD5) hash. • **ntlm** - Authenticates user credentials based on an authentication challenge and response.

Usage

Use this command to enable the Steelhead appliance to use a Web proxy to contact the Riverbed licensing portal and fetch licenses in a secure environment. You can optionally require user credentials to communicate with the Web proxy for use with the autolicensing feature. You can specify the method used to authenticate and negotiate these user credentials.

The **no** command option resets the Web proxy settings to the default behavior. Web proxy access is disabled by default.

RiOS supports the following proxies: Squid, Blue Coat Proxy SG, Microsoft WebSense, and McAfee Web Gateway.

Example

```
amnesiac (config) # web proxy host 10.1.2.1 port 1220
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web rest-server enable

Description

Enables the REST (REpresentational State Transfer) server.

Syntax

[no] web rest-server enable

Parameters

None

Usage

The **no** command disables the REST server.

Example

```
amnesiac (config) # web rest-server enable
```

Product

CMC, Steelhead appliance

Related Topics

"papi rest access_code generate," "papi rest access_code import,""show papi rest access_codes," "show web"

web session renewal

Description

Sets the session renewal time. This is the time before the Web session time-out. If a Web request comes in, it automatically renews the session.

Syntax

[no] web session renewal <minutes>

Parameters

<minutes>	Specify the number of minutes. The default value is **10** minutes.

Usage

The **no** command option resets the session renewal time to the default value.

Example

```
amnesiac (config) # web session renewal 5
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web session timeout

Description

Sets the session time-out value. This is the amount of time the cookie is active.

Syntax

[no] web session timeout <minutes>

Parameters

<minutes>	Specify the number of minutes. The default value is **60** minutes.

Usage

The **no** command option resets the session time-out to the default value.

Example

```
amnesiac (config) # web session timeout 120
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web snmp-trap conf-mode enable

Description

Enables SNMP traps in Web configure mode.

Syntax

[no] web snmp-trap conf-mode enable

Parameters

None

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # web snmp-trap conf-mode enable
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

web soap-server enable

Description

Enables the Simple Object Access Protocol (SOAP) server.

Syntax

[no] web soap-server enable

Parameters

None

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # web soap-server enable
```

Product

Steelhead appliance, CMC, Interceptor appliance Steelhead Mobile Controller, CSH

Related Topics

"show web"

web soap-server port

Description

Enables the Simple Object Access Protocol (SOAP) server port.

Syntax

[no] web soap-server port <port>

Parameters

<port>	Specify the port.

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # web soap-server port 1234
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web"

Configuration File Commands

This section describes the configuration file commands.

cmc enable

Description

Enables auto-registration for the CMC.

Syntax

[no] cmc enable

Parameters

None

Usage

The **no** command option disables CMC auto-registration.

Example

```
amnesiac (config) # cmc enable
```

Product

Steelhead appliance, CSH, Interceptor appliance

Related Topics

"show running-config"

cmc hostname

Description

Sets the CMC hostname used for auto-registration.

Syntax

[no] cmc hostname <hostname>

Parameters

<hostname>	Specify the hostname.

Usage

The **no** command option disables CMC auto-registration.

Example

```
amnesiac (config) # cmc hostname test
```

Product

Steelhead appliance, CSH, Interceptor appliance

Related Topics

"show running-config"

configuration copy

Description

Copies a configuration file.

Syntax

configuration copy <sourcename> <new-filename>

Parameters

<sourcename>	Specify the name of the source file.
<new-filename>	Specify the name of the destination file.

Example

```
amnesiac (config) # configuration copy westcoast eastcoast
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

configuration delete

Description

Deletes a configuration file.

Syntax

configuration delete <filename>

Parameters

<filename>	Specify the name of the configuration file to delete.

Example

```
amnesiac (config) # configuration delete westcoast
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

configuration factory

Description

Creates a new configuration file.

Syntax

configuration factory <filename>

Parameters

<filename>	Specify the name of the destination file.

Example

```
amnesiac (config) # configuration factory eastcoast
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

configuration fetch

Description

Downloads a configuration file over the network.

Syntax

configuration fetch
{<URL, scp://, or ftp://username:password@hostname/path/filename> | <filename>

Parameters

<URL, scp://, or ftp://username:password@hostname/path/filename>	Specify the location of the configuration file to download in URL, scp://, or ftp:// format.
<filename>	Create a new name for the configuration file.

Usage

To copy one configuration file to another appliance, run the following set of commands:

```
configuration fetch <url-to-remote-config> <new-config-name>
        ;; this fetches the configuration from the remote
configuration switch-to <new-config-name>
        ;; this activates the newly fetched configuration
```

Example

```
amnesiac (config) # configuration fetch http://domain.com/westcoast newconfig
amnesiac (config) # configuration switch-to newconfig
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

configuration jump-start

Description

Restarts the configuration wizard. The configuration wizard lets you set 20 configuration parameters with a single command. Press Enter to accept the value displayed or enter a new value.

Syntax

configuration jump-start

Parameters

None

Example

```
amnesiac (config) # configuration jump-start

Riverbed Steelhead configuration wizard.

Step 1: Hostname? [example]
Step 2: Use DHCP on primary interface? [no]
Step 3: Primary IP address? [10.11.6.6]
Step 4: Netmask? [255.255.0.0]
Step 5: Default gateway? [10.0.0.1]
Step 6: Primary DNS server? [10.0.0.2]
Step 7: Domain name? [example.com]
Step 8: Admin password?
Step 9: SMTP server? [exchange]
Step 10: Notification email address? [examplem@riverbed.com]
Step 11: Set the primary interface speed? [auto]
Step 12: Set the primary interface duplex? [auto]
Step 13: Would you like to activate the in-path configuration? [yes]
Step 14: In-Path IP address? [10.11.6.6]
Step 15: In-Path Netmask? [255.255.0.0]
Step 16: In-Path Default gateway?
Step 17: Set the in-path:LAN interface speed? [auto]
Step 18: Set the in-path:LAN interface duplex? [auto]
Step 19: Set the in-path:WAN interface speed? [auto]
Step 20: Set the in-path:WAN interface duplex? [auto]

You have entered the following information:

   1. Hostname: example
   2. Use DHCP on primary interface: no
   3. Primary IP address: 10.11.0.6
   4. Netmask: 255.255.0.0
   5. Default gateway: 10.0.0.1
   6. Primary DNS server: 10.0.0.2
   7. Domain name: example.com
   8. Admin password: (unchanged)
   9. SMTP server: exchange
   10. Notification email address: example@riverbed.com
   11. Set the primary interface speed: auto
   12. Set the primary interface duplex: auto
   13. Would you like to activate the in-path configuration: yes
   14. In-Path IP address: 10.11.6.6
   15. In-Path Netmask: 255.255.0.0
   16. In-Path Default gateway:
   17. Set the in-path:LAN interface speed: auto
   18. Set the in-path:LAN interface duplex: auto
   19. Set the in-path:WAN interface speed: auto
   20. Set the in-path:WAN interface duplex: auto

To change an answer, enter the step number to return to.
Otherwise hit <enter> to save changes and exit.

Choice:
amnesiac (config)>
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

configuration merge

Description

Merges common configuration settings from one system to another.

Syntax

configuration merge <filename> <new-config-name>

Parameters

<filename>	Name of file from which to merge settings.
<new-config-name>	Specify the new configuration name.

Usage

Use the configuration merge command to deploy a network of appliances. Set up a template for your appliance and merge the template with each appliance in the network.

The following configuration settings are not merged when you run the **configuration merge** command: failover settings, SNMP SysContact and SysLocation, alarm settings, CLI settings, and all network settings (for example, hostname, auxiliary interface, DNS settings, defined hosts, static routing, and in-path routing).

The following configuration settings are merged when you run the **configuration merge** command: in-path, out-of-path, log settings, protocols, statistics, email, NTP and time, Web, and SNMP.

To merge a configuration file, run the following set of commands:

```
configuration write to <new-config-name>
        ;; this saves the current config to the new name and activates
         ;; the new configuration
configuration fetch <url-to-remote-config> <temp-config-name>
        ;; this fetches the configuration from the remote
configuration merge <temp-config-name>
        ;; this merges the fetched config into the active configuration
         ;; which is the newly named/created one in step 1 above
configuration delete <temp-config-name>
        ;; this deletes the fetched configuration as it is no longer
         ;; needed since you merged it into the active configuration
```

Example

```
amnesiac (config) # configuration merge tempconfig
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

configuration move

Description

Moves and renames a configuration file.

Syntax

configuration move <sourcename> <destname>

Parameters

<sourcename>	Specify the name of the source configuration file.
<destname>	Specify the name of the new configuration file.

Example

```
amnesiac (config) # configuration move westcoast eastcoast
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

configuration new

Description

Creates a new, blank configuration file.

Syntax

configuration new <new-filename> <cr> | [keep licenses]

Parameters

<new-filename>	Specify the name of the new configuration file.
keep licenses	Creates a new configuration file with default settings and active licenses.

Usage

Riverbed recommends that you use the **keep licenses** command option. If you do not keep licenses, your new configuration will not have a valid license key.

Example

```
amnesiac (config) # configuration new westcoast keep licenses
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

configuration flash restore

Description

Restores a saved configuration from flash memory.

Syntax

configuration flash restore

Parameters

None

Example

```
amnesiac (config) # configuration flash restore
```

Product

Steelhead appliance

Related Topics

"show info"

configuration flash write

Description

Writes the active configuration to flash disk memory in binary and text form.

Syntax

configuration flash write

Parameters

None

Example

```
amnesiac (config) # configuration flash write
```

Product

Steelhead appliance

Related Topics

"show info"

configuration revert keep-local

Description

Reverts to the initial configuration but maintains some appliance-specific settings.

Syntax

configuration revert keep-local

Parameters

None

Example

```
amnesiac (config) # configuration revert keep-local
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

configuration revert saved

Description

Reverts the active configuration to the last saved configuration.

Syntax

configuration revert saved

Parameters

None

Example

```
amnesiac (config) # configuration revert saved
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller

Related Topics

"show info"

configuration switch-to

Description

Loads a new configuration file and makes it the active configuration.

Syntax

configuration switch-to <filename>

Parameters

<filename>	Specify the filename. The default filenames are: • **initial -** Specify the initial configuration. • **initial.bak -** Specify the initial backup configuration. • **cold -** Specify the configuration file before SDR has occurred. • **working -** Specify the current configuration.

Example

```
amnesiac (config) # configuration switch-to westcoast
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

configuration upload

Description

Uploads the configuration file.

Syntax

configuration upload <filename>
<http, ftp, or scp URL (e.g. scp://username:password@host/path)> <cr> | [active]

Parameters

<filename>	Specify the configuration filename.
<http, ftp, or scp URL (e.g. scp://username:password@host/path)>	Specify the HTTP, FTP, or scp URL.
active	Sets the uploaded file to the active configuration file.

Example

```
amnesiac (config) # configuration upload initial scp://test:MyPassword@example/tmp/
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

configuration write

Description

Writes the current, active configuration file to memory.

Syntax

configuration write <cr> [to <filename>]

Parameters

to <filename>	Save the running configuration to a file.

Example

```
amnesiac (config) # configuration write
```

Product

Steelhead appliance, CMC, Interceptor appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

write flash

Description

Saves the current configuration settings to flash memory.

Syntax

write flash

Parameters

None

Example

```
amnesiac (config) # write flash
```

Product

Steelhead appliance

Related Topics

"show info"

write memory

Description

Saves the current configuration settings to memory.

Syntax

write memory

Parameters

None

Example

```
amnesiac (config) # write memory
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

write terminal

Description

Displays commands to recreate current running configuration.

Syntax

write terminal

Parameters

None

Example

```
amnesiac (config) # write terminal
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show info"

tcp connection send keep-alive

Description

Configures TCP connection tools for debugging the system.

Syntax

tcp connection send keep-alive local-addr <local ip-addr> local-port <port> remote-addr <remote ip-addr> remote-port <port>

Parameters

local-addr <local ip-addr> local-port <port> remote-addr <remote ip-addr> remote-port <port>	Specify a local and remote Steelhead appliance for which you want to terminate a connection.

Usage

Enables a keep-alive timer between a local and remote Steelhead appliance so that you can determine if there is an active connection between the appliances. If the appliance is down, it terminates the connection. Use this command to debug connection problems in your network.

Example

```
amnesiac (config) # tcp connection send keep-alive local-addr 10.0.0.1 local-port 1240 remote-addr
10.0.0.2 remote-port 1300
```

Product

Steelhead appliance, CSH

Related Topics

"show tcpdump-x"

tcp connection send pass-reset

Description

Resets all pass-through connections that match the source and destination IP address and port.

Syntax

tcp connection send pass-reset source-addr <source ip-addr> source-port <source port> dest-addr <destination ip-addr> dest-port <destination port>

Parameters

source-addr <source ip-addr>	Specify the source IP address.
source-port <source port>	Specify the source port.
dest-addr <destination ip-addr>	Specify the destination IP address.
dest-port <destination port>	Specify the destination port.

Usage

Enables you to individually reset passed-through connections on the Steelhead appliance so that upon re-establishment they are optimized.

Example

```
amnesiac (config) # tcp connection send pass-reset source-addr 10.0.0.1 source-port 1234 dest-addr
10.0.0.2 dest-port 2345
```

Product

Steelhead appliance, CSH

Related Topics

"show stats traffic passthrough"

tcp connection send reset

Description

Configures TCP connection tools for debugging the system.

Syntax

tcp connection send reset
[both local-addr <local ip-addr> local-port <port> remote-addr <remote ip-addr> remote-port <port> |
local-only local-addr <local ip-addr> local-port <port> remote-addr <remote ip-addr> remote-port <port> |
remote-only remote-addr <remote ip-addr> remote-port <port> local-addr <local ip-addr> local-port <port>

Parameters

both local-addr <local ip-addr> local-port <port> remote-addr <remote ip-addr> remote-port <port>	Terminates the connection for the local and remote Steelhead appliances.
local-only local-addr <local ip-addr> local-port <port> remote-addr <remote ip-addr> remote-port <port>	Terminates the connection for the local Steelhead appliance.
remote-only remote-addr <remote ip-addr> remote-port <port> local-addr <local ip-addr> local-port <port>	Terminates the connection for the remote Steelhead appliance.

Usage

Terminates connections between Steelhead appliances so that you can debug connection problems in your network.

Example

```
amnesiac (config) # tcp connection send reset both local-only local-addr 10.0.0.1 local-port 1240
remote-addr 10.0.0.2 remote-port 1300
```

Product

Steelhead appliance, CSH

Related Topics

“show tcpdump-x”

Statistics Manipulation Commands

This section describes the statistics manipulation commands.

stats settings

Description

Configures settings to generate statistics.

Syntax

stats settings {bandwidth port <port number> desc <string>| top-talkers enable | top-talkers interval <hours>}

Parameters

bandwidth port <port number>	Specify a port to be monitored for statistics.
desc <string>	Specify a description for the port.
top-talkers enable	Enables top-talkers.
interval <hours>	Specify the top talkers collection interval: **24** or **48** hours.

Example

```
amnesiac (config) # stats settings top-talkers enable
```

Product

Steelhead appliance, CSH

Related Topics

"show stats bandwidth"

stats settings app-vis enable

Description

Enables the generation of statistics about application-based traffic flowing through the Steelhead appliance.

Syntax

[no] stats settings app-vis enable

Parameters

None

Usage

The Application Statistics report summarizes the traffic flowing through a Steelhead appliance classified by the application for the time period specified. This report provides application-level visibility into Layer-7 and shows the application dynamics for pass-through and optimized traffic.

RiOS collects application statistics for all data transmitted out of the WAN and primary interfaces and commits samples every 5 minutes. Let the system collect statistics for awhile to view the most meaningful data display.

Use the **no** version of the command to disable the application-visibility feature. Use the **show stats settings app-vis** command to display whether or not the application-visibility feature is enabled.

See the *Steelhead Appliance Management Console User's Guide* for details about viewing and interpreting Application Statistics reports.

Example

```
amnesiac (config) # stats settings app-vis enable
```

Product

Steelhead appliance

Related Topics

"stats settings bandwidth"

stats settings bandwidth

Description

Configures sampled statistics.

Syntax

[no] stats settings bandwidth <port> desc <description>

Parameters

<port>	Specify the port number.
desc <description>	Specify a description of the port.

Usage

The **no** command option disables bandwidth statistics.

Example

```
amnesiac (config) # stats settings bandwidth 2727
```

Product

Steelhead appliance, CSH

Related Topics

"show stats bandwidth"

stats settings totalwantxbps enable

Description

Enables the generation of statistics about WAN throughput.

Syntax

[no] stats settings totalwantxbps enable

Parameters

None

Usage

The WAN Throughput report summarizes the WAN throughput for the time period specified. The throughput is an aggregation of all data the system transmits out of all WAN interfaces. The report collects data that is transmitted out of all WAN interfaces in standard in-path or virtual in-path deployments. The report also collects data that is transmitted out of the primary interface in a server-side out-of-path deployment.

WAN throughput statistics are enabled by default. The **no** command option disables the WAN throughput reporting.

See the *Steelhead Appliance Management Console User's Guide* for details about viewing and interpreting the WAN throughput report.

Example

```
amnesiac (config) # stats settings totalwantxbps enable
```

Product

Steelhead appliance

Related Topics

"show stats bandwidth"

Notification Commands

This section describes the notification commands.

email autosupport enable

Description

Enables automatic email notification of significant alarms and events to Riverbed Support.

Syntax

[no] email autosupport enable

Parameters

None

Usage

The **no** command option disables automatic email notification.

Example

```
amnesiac (config) # email autosupport enable
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show email"

email domain

Description

Sets the domain for email notifications.

Syntax

[no] email domain <hostname or ip-addr>

Parameters

<hostname or ip-addr>	Specify the domain for email notifications (only if the email address does not contain it).

Usage

Use the email domain command only if the email address does not contain the domain.

The **no** command option disables the email domain.

Example

```
amnesiac (config) # email domain example.com
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show domain"

email from-address

Description

Sets the address from which email messages appear to come.

Syntax

[no] email from-address <email addr>

Parameters

<email addr>	Specify the full user name and domain to appear in the email "From:" address.

Usage

Use the email from-address command to override the default email address used in outgoing email messages, do-not-reply@[hostname].[domainname].

The **no** command option disables the email address configured and returns to the default email address.

Example

```
amnesiac (config) # email from-address bean@caffeitaly.com
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show domain", "show email"

email mailhub

Description

Sets the SMTP server for email notifications.

Syntax

[no] email mailhub <hostname or ip-addr>

Parameters

<hostname or ip-addr>	Specify the SMTP server for email notifications.

Usage

The **no** command option disables the SMTP server.

Example

```
amnesiac (config) # email mailhub mail-server.example.com
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show email"

email mailhub-port

Description

Sets the email port for email notifications.

Syntax

[no] email mailhub-port <port>

Parameters

<port>	Specify the email port for email notifications.

Usage

The **no** command option disables the email port.

Example

```
amnesiac (config) # email mailhub-port 135
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show email"

email notify events enable

Description

Enables email notification for events.

Syntax

[no] email notify events enable

Parameters

None

Usage

The **no** command option disables email notification.

Example

```
amnesiac (config) # email notify events enable
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show email"

email notify events recipient

Description

Sets the email address for notification of events.

Syntax

[no] email notify events recipient <email addr>

Parameters

<email addr>	Specify the email address of the user to receive notification of events.

Usage

The **no** command option disables email address for notification.

Example

```
amnesiac (config) # email notify events recipient johndoe@example.com
amnesiac (config) # email notify events recipient janedoe@example.com
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show email"

email notify failures enable

Description

Enables email notification of system failures, such as core dumps.

Syntax

[no] email notify failures enable

Parameters

None

Usage

The **no** command option disables email notification.

Example

```
amnesiac (config) # email notify failures enable
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show email"

email notify failures recipient

Description

Enables email notification of system failures, such as core dumps.

Syntax

[no] email notify failures recipient <email addr>

Parameters

recipient <email-addr>	Specify the email address of the user to receive notification of failures.

Usage

The **no** command option disables email notification.

You must enter separate commands for each email address. Each command line accepts only one email address.

Example

```
amnesiac (config) # email notify failures recipient johndoe@example.com

amnesiac (config) # email notify failures recipient janedoe@example.com
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show email"

email send-test

Description

Sends a test email to all configured event and failure recipients.

Syntax

email send-test

Parameters

None

Usage

You can also access this command from enable mode.

Example

```
amnesiac (config) # email send-test
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show email"

SNMP Commands

RiOS v5.0 provides support for the following:

- SNMP Version 1
- SNMP Version 2c

RiOS v6.0 and later provides support for the following:

- SNMP Version 3, which provides authentication through the User-based Security Model (USM).
- View-Based Access Control Mechanism (VACM), which provides richer access control.
- Enterprise Management Information Base (MIB).
- ACLs (Access Control Lists) for users (v1 and v2c only).

For detailed information about SNMP traps sent to configured servers, see the *Steelhead Appliance Management Console User's Guide*.

SNMP v3 provides additional authentication and access control for message security. For example, you can verify the identity of the SNMP entity (manager or agent) sending the message.

Using SNMPv3 is more secure than SNMP v1 or v2; however, it requires more configuration steps to provide the additional security features.

snmp-server acl

Description

Configures changes to the View-Based Access Control Model (VACM) ACL configuration.

Syntax

[no] snmp-server acl group <name> security-level <level> read-view <name>

Parameters

group <name>	Specify the name of the SNMP server community.
security-level <level>	Specify the security level for this ACL entry. • **noauth** - Does not authenticate packets and does not use privacy. This is the default setting. • **auth** - Authenticates packets but does not use privacy. • **authpriv** - Authenticates packets and uses privacy. **Note:** This setting determines whether a single atomic message exchange is authenticated**.** **Note:** A security level applies to a group, not to an individual user.
read-view <name>	Specify that read requests will be restricted to this view.

Usage

For details about SNMP traps sent to configured servers, the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

The **no** command option disables an SNMP server community.

Example

```
amnesiac (config) # snmp-server acl group ReadOnly security-level auth read-view ReadOnly
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server community

Description

Sets an SNMP read-only server community.

Syntax

[no] snmp-server community <name>

Parameters

<name>	Specify the name of the SNMP server community. The # and - characters are not allowed at the beginning of the <name> argument. If you use either of these characters at the beginning of the <name> argument, the CLI returns the following error message: `% Invalid SNMP community name`

Usage

For details about SNMP traps sent to configured servers, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

You can still access the entire MIB tree from any source host using this setting. If you do not want this type of access, you must delete this option and configure the security name for SNMP ACL support. For details, see "snmp-server group" on page 290.

This community string overrides any VACM settings.

The **no** command option disables an SNMP server community.

Example

```
amnesiac (config) # snmp-server community ReaDonLy
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server contact

Description

Sets the SNMP server contact.

Syntax

[no] snmp-server contact <name>

Parameters

<name>	Specify the user name of the SNMP server community contact.

Usage

The **no** command option disables the SNMP server contact.

Example

```
amnesiac (config) # snmp-server contact john doe
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server enable

Description

Enables an SNMP server.

Syntax

[no] snmp-server enable | [traps]

Parameters

traps	Enables sending of SNMP traps from this system.

Usage

The **no** command option disables the SNMP server or traps.

Example

```
amnesiac (config) # snmp-server enable traps
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server group

Description

Configures the View Access Control Model (VACM) group configuration.

Syntax

[no] snmp-server group <group> security name <name> security-model <model>

Parameters

group <group>	Specify a group name.
security-model <model>	Specify one of the following security models: • **v1** - Enables SNMPv1 security model. • **v2c** - Enables SNMPv2c security model. • **usm** - Enables User-based Security Model (USM).
security-name <name>	Specify a name to identify a requester (allowed to issue gets and sets) or a recipient (allowed to receive traps) of management data. The security name is also required to make changes to the VACM security name configuration.

Usage

The **no** command option disables the SNMP server group.

Example

```
amnesiac (config) # snmp-server group rvbdgrp security-name riverbed security-model v1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server host

Description

Configures hosts to which to send SNMP traps.

Syntax

[no] snmp-server host {<hostname> |<IPv4-addr> | <IPv6-addr>} traps <community string>

Parameters

<hostname> |<IPv4-addr> | <IPv6-addr>	Specify the hostname, IPv4 address, or IPv6 address for the SNMP server.
traps <community string>	Send traps to the specified host. Specify the password-like community string to control access. Use a combination of uppercase, lowercase, and numerical characters to reduce the chance of unauthorized access to the Steelhead appliance. The # and - characters are not allowed at the beginning of the <community string> argument. **Note:** If you specify a read-only community string, it takes precedence over this community name and allows users to access the entire MIB tree from any source host. If this is not desired, delete the read-only community string. **Note:** To create multiple SNMP community strings on a Steelhead, leave the default public community string and then create a second read-only community string with a different security name. Or, you can delete the default public string and create two new SNMP ACLs with unique names.

Usage

The **no** command option disables the SNMP server host.

Example

```
amnesiac (config) # snmp-server host 10.0.0.1 traps public
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server host version

Description

Configures the SNMP version of traps to send to the host.

Syntax

[no] snmp-server host {<hostname> |<IPv4-addr> | <IPv6-addr>} traps version {1 | 2 c | 3 remote-user <name>} password encrypted <key> auth-protocol {MD5 | SHA} security-level {noauth | auth | authpriv>} <cr> | plain-text <text > auth-protocol <MD5 | SHA>] [security-level <noauth | auth | authpriv> <cr>] | [priv-protocol {AES |DES} priv-key {encrypted <key> | plain-text <text>}] [port <port>]

Parameters

<hostname or ip-addr>	Specify the hostname, IPv4 address, or IPv6 address for the SNMP server.
traps	Send traps to the specified host.
version <number>	Specify the SNMP version of traps to send to this host: • **1** - Specifies SNMPv1. • **2c**. Specifies SNMPv2c. • **3** - Specifies SNMPv3.
remote-user <name>	For SNMPv3 specify the user name.
password [encrypted | plaintext]	Specify the password type: • **encrypted** - Enable encrypted password authentication. • **plaintext** - Enable plain-text password authentication.
encrypted <key>	For SNMPv3 specify the user password.
auth-protocol <MD5 | SHA>	Specify the authorization protocol: • **MD5** - Enable MD5 security protocol. • **SHA** - Enable SHA security protocol.
security-level <noauth | auth | authpriv>	Specify the security level: • **noauth** - Specify no authorization required. • **auth** - Specify authorization required. • **authpriv** - Specify authorization and privacy required.
priv-protocol {AES |DES}	Specify the privacy protocol: • **AES** - Specify CFB128-AES-128 as the privacy protocol. • **DES** - Specify CBC-DES as the privacy protocol.
priv-key {encrypted <key> | plain-text <text>}	Specify the privacy key: • **encrypted <key>** - Specify encrypted privacy key. • **plain-text <text>** - Specify plain-text privacy key. The plain-text privacy key must be at least 8 characters.
port <port>	Optionally, specify the destination port.

Usage

The **no** command option disables the SNMP server host.

Example

```
amnesiac (config) # snmp-server host 10.0.0.1 traps version 1 "public 99162?" port 1234
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp", "snmp-server community", "snmp-server security-name"

snmp-server ifindex

Description

Adds a custom index value for an interface.

Syntax

snmp-server ifindex <interface> <index>

Parameters

<interface>	Specify the interface: **wan0_0**, **lan0_0**, **wan0_1**, **lan0_1**, **primary**, **aux**, **inpath0_0**, **inpath0_1**
<index>	Specify the index.

Example

```
amnesiac (config) # snmp-server ifindex aux 1234
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server ifindex-persist

Description

Enables persistent SNMP interface indices.

Syntax

[no] snmp-server ifindex-persist

Parameters

None

Usage

The **no** command option disables the SNMP server group.

Example

```
amnesiac (config) # snmp-server ifindex-persist
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server ifindex-reset

Description

Resets the ifindex values of all interfaces to the factory default value.

Syntax

snmp-server ifindex-reset

Parameters

None

Example

```
amnesiac (config) # snmp-server ifindex-reset
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server listen enable

Description

Enables SNMP server interface restrictions (that is, it enables access control and blocks requests on all the interfaces).

Syntax

[no] snmp-server listen enable

Parameters

None

Usage

The **no** command option disables SNMP interface restrictions.
SNMP interface restrictions are not available through the Management Console.

Example

```
amnesiac (config) # snmp-server listen enable
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server listen interface

Description

Adds an interface to the SNMP server access restriction list.

Syntax

[no] snmp-server listen interface <interface>

Parameters

<interface>	Specify the interface: **primary**, **aux**, **inpath0_0**, **rios-lan0_0**, **rios_wan0_0**
<index>	Specify the index.

Usage

If the list of interfaces is empty, none of the interfaces respond to the queries. If the list of interfaces has at least one entry, then the server listens on that subset of interfaces.

To add an interface to the list to listen on

```
snmp-server listen interface primary
```

To remove an interface from the list

```
no snmp-server listen interface <interface>
```

SNMP interface restrictions are not available through the Management Console.

Example

```
amnesiac (config) # snmp-server listen interface aux
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server location

Description

Sets the value for the system location variable in the MIB.

Syntax

[no] snmp-server location <ip-addr>

Parameters

<ip-addr>	Specify the IP address of the system.

Usage

The **no** command option disables the SNMP server location.

Example

```
amnesiac (config) # snmp-server location 10.10.10.1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server security-name

Description

Configures the SNMP security name.

Syntax

[no] snmp-server security-name <name> community <community string> source <IPv4-addr | IPv6-addr> <netmask>

Parameters

<name>	Specify the security name.
community <community string>	Specify the password-like community string to control access. Use a combination of uppercase, lowercase, and numerical characters to reduce the chance of unauthorized access to the Steelhead appliance. Community strings allow printable 7-bit ASCII characters except for white spaces. Community strings can not begin with '#' or '-'. If you specify a read-only community string, it takes precedence over this community name and allows users to access the entire MIB tree from any source host. If this is not desired, delete the read-only community string. To create multiple SNMP community strings on a Steelhead, leave the default public community string and then create a second read-only community string with a different security name. Or, you can delete the default public string and create two new SNMP ACLs with unique names.
source <IPv4-addr | IPv6-addr> <netmask>	Specify the source IPv4 address or IPv6 address and netmask.

Usage

The **no** command option disables the trap interface.

Example

```
amnesiac (config) # snmp-server security-name riverbed community public source 10.1.2.3/24
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server trap-interface

Description

Configures the system to use the IP address of the specified interface in the SNMP trap header.

Syntax

[no] snmp-server trap-interface <interface>

Parameters

<interface>	Specify the interface.

Usage

The trap interface setting sets which interface IP address is used in the agent-address header field of SNMP v1 trap Protocol Data Units (PDUs). It does set the interface for the trap.

Traps are sent out the Primary interface. If the primary interface is physically disconnected, no traps are sent. Traps can be sent out the auxiliary interface if the trap receiver is reachable from the auxiliary interface.

The **no** command option disables the trap interface.

Example

```
amnesiac (config) # snmp-server trap-interface aux
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server trap-test

Description

Generates an SNMP trap test.

Syntax

snmp-server trap-test

Parameters

None

Usage

Use this command to send a sample trap test to ensure that the SNMP server is monitoring the Steelhead appliance.

Example

```
amnesiac (config) # snmp-server trap-test
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server user

Description

Configures changes to the User-Based Security (UBS) model.

Syntax

[no] snmp-server user <name> password {encrypted <key> | plain-text <text>} auth-protocol {MD5 | SHA} [priv-protocol {AES |DES} priv-key {encrypted <key> | plain-text <text>}]

Parameters

<name>	Specify the user name.
password {encrypted <key>| plain-text <text>}	Specify the password type: • **encrypted <key>** - Enable encrypted password authentication. • **plain-text <text>** - Enable plain-text password authentication. The plain-text password must be at least 8 characters.
auth-protocol {MD5 | SHA}	Specify the authorization protocol: • **MD5** - Enable MD5 security protocol. • **SHA** - Enable SHA security protocol.
priv-protocol {AES |DES}	Specify the privacy protocol: • **AES** - Specify CFB128-AES-128 as the privacy protocol. • **DES** - Specify CBC-DES as the privacy protocol.
priv-key {encrypted <key> | plain-text <text>}	Specify the privacy key: • **encrypted <key>** - Specify encrypted privacy key. • **plain-text <text>** - Specify plain-text privacy key. The plain-text privacy key must be at least 8 characters.

Usage

The **no** command option disables this option.

Example

```
amnesiac (config) # snmp-server user testuser password plain-text testpass auth-protocol SHA
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

snmp-server view

Description

Configures changes to the View-based Access Control Model (VACM) configuration.

Syntax

[no] snmp-server view <name> [excluded | included] <oid>

Parameters

<name>	Specify the user name.
excluded | included	Specify the following view options: • **excluded** - Excludes an oid sub-tree from this view. • **included** - Includes an OID subtree into this view.
<oid>	Specify the object ID. For example: **.1.3.6.1.2.1.1** or **.iso.org.dod.internet.mgmt.mib-2.system**

Usage

The **no** command option disables this option.

Example

```
amnesiac (config) # snmp-server view joedoe included .1.3.6.1.2.1.1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show snmp"

Logging Commands

This section describes the logging commands.

logging

Description

Adds a remote system log (syslog) server to the system.

Syntax

[no] logging <ip-addr> <cr> | [trap <log level>]

Parameters

<ip-addr>	Specify the IP address for the syslog server.
trap <log level>	Specify the trap log level of the syslog server: • **emerg** - Emergency, the system is unusable. • **alert** - Action must be taken immediately. • **critical** - Critical conditions. • **err** - Error conditions. • **warning** - Warning conditions. • **notice** - Normal but significant conditions, such as a configuration change. This is the default setting. • **info** - Informational messages. If you have set different log levels for each remote syslog server, this option changes all remote syslog servers to have a single log level.

Usage

The **no** command option removes a remote **syslog** server from the system.

Example

```
amnesiac (config) # logging 10.0.0.2
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show logging"

logging files delete

Description

Deletes the oldest log file or a specified number of the oldest log files.

Syntax

logging files delete oldest <number>

Parameters

oldest <number>	Specify the number of old log files to delete. The range is **1-10**.

Usage

You can also access this command from enable mode.

Example

```
amnesiac (config) # logging files delete oldest 10
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show logging"

logging files rotation criteria frequency

Description

Sets the frequency of log rotation.

Syntax

logging files rotation criteria frequency <rotation frequency>

Parameters

<rotation frequency>	Specify how often log rotation occurs: **monthly**, **weekly**, **daily** The size of the log file is checked every 10 minutes.

Usage

The size of the log file is checked every 10 minutes. If there is an unusually large amount of logging activity, it is possible for a log file to grow larger than the set limit in that period of time.

Example

```
amnesiac (config) # logging files rotation criteria frequency weekly
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show logging"

logging files rotation criteria size

Description

Sets the size, in MB, of the log file before rotation occurs.

Syntax

logging files rotation criteria size <size>

Parameters

<size>	Specify the size of the log file to save in MB. The default value is 0 (unlimited).

Usage

The size of the log file is checked every 10 minutes. If there is an unusually large amount of logging activity, it is possible for a log file to grow larger than the set limit in that period of time.

Example

```
amnesiac (config) # logging files rotation criteria size 100
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show logging"

logging files rotation force

Description

Rotates logs immediately.

Syntax

logging files rotation force

Parameters

None

Usage

The size of the log file is checked every 10 minutes. If there is an unusually large amount of logging activity, it is possible for a log file to grow larger than the set limit in that period of time.

Example

```
amnesiac (config) # logging files rotation force
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show logging"

logging files rotation max-num

Description

Sets the maximum number of log files to keep locally.

Syntax

logging files rotation max-num <number>

Parameters

<number>	Specify the number of log files to keep locally. The range is 1-100. The default value is 10.

Usage

The size of the log file is checked every 10 minutes. If there is an unusually large amount of logging activity, it is possible for a log file to grow larger than the set limit in that period of time.

Example

```
amnesiac (config) # logging files rotation max-num 10
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show logging"

logging filter

Description

Sets the minimal level of messages arriving from the specified process to the local subsystem.

Syntax

logging filter <process> <level>

Parameters

<process>	Specify the application process: • **cli** - Command-Line Interface. • **hald** - Hardware Abstraction Daemon. • **mgmtd** - Device Control and Management. • **pm** - Process Manager. • **rgp** - Central Management Client. • **rgpd** - Central Management Client Daemon. • **cmcf** - CMC automatic registration utility. • **sched** - Process Scheduler. • **statsd** - Statistics Collector. • **wdt** - Watchdog Timer. • **webasd** - Web Application Process. • **rspd** - RSP Watchdog. • **cifs** - CIFS Optimization. • **domain_auth** - Windows Domain Authentication. • **http** - HTTP Optimization. • **mapi** - MAPI Optimization. • **nfs** - NFS Optimization. • **notes** - Lotus Notes. • **virt_wrapperd** - Virtual machine.
<level>	Specify the trap log level: • **emerg** - Emergency, the system is unusable. • **alert** - Action must be taken immediately. • **critical** - Critical conditions. • **err** - Error conditions. • **warning** - Warning conditions. • **notice** - Normal but significant conditions, such as a configuration change. This is the default setting. • **info** - Informational messages. If you have set different log levels for each remote **syslog** server, this option changes all remote **syslog** servers to have a single log level.

Usage

Use this command to capture data when a Steelhead appliance is not able to sustain the flow of logging data that is being committed to disk.

This command overrides the **logging local** command. This command creates a global setting that controls all output, including remote hosts.

All CIFS protocol related messages are logged at level **debug**, and the remainder at the level **notice**.

All remote logging hosts (if defined) also log at **logging trap** setting and at the logging filter process.

The **no logging filter all** command deletes all filters.

Example

```
amnesiac (config) # logging filter cli alert
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show logging"

logging local

Description

Sets the minimum severity of log messages saved on the local syslog servers.

Syntax

[no] logging local <loglevel>

Parameters

<loglevel>	Specify the logging severity level. The follow severity levels are supported: • **emerg** - Emergency, the system is unusable. • **alert -** Action must be taken immediately. • **crit -**Critical conditions. • **err -** Error conditions. • **warning -** Warning conditions. • **notice -** Normal but significant conditions, such as a configuration change. This is the default setting. • **info -** Informational messages. The default value is **notice**.

Usage

The **no** command option sets the severity level for logging to none (no logs are sent).

Example

```
amnesiac (config) # logging local notice
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show logging"

logging trap

Description

Sets the minimum severity for messages sent to the remote syslog servers.

Syntax

[no] logging trap <loglevel>

Parameters

<loglevel>	Specify the logging severity level. The follow severity levels are supported: • **emerg** - Emergency, the system is unusable. • **alert -** Action must be taken immediately. • **crit -**Critical conditions. • **err -** Error conditions. • **warning -** Warning conditions. • **notice -** Normal but significant conditions, such as a configuration change. This is the default setting. • **info -** Informational messages. The default value is **notice**.

Usage

The **no** command option sets the severity level for logging to none.

Example

```
amnesiac (config) # logging trap notice
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show logging"

License and Hardware Upgrade Commands

This section describes the license and hardware upgrade commands.

boot bootloader password

Description

Sets the password for the bootloader.

Syntax

boot bootloader password {<password> | 0 <password> | 7 <password>}

Parameters

<password>	Specify a bootloader password in clear text. The password must be at least 6 characters. This option functions the same as the **0 <password>** parameter and is provided for backward compatibility.
0 <password>	Specify a bootloader password in clear text.
7 <password>	Specify a bootloader password with an encrypted string. The encrypted string is the hash of the clear text password and is 35 bytes long. The first 3 bytes indicate the hash algorithm and the next 32 bytes are the hash values.

Example

```
amnesiac (config) # boot bootloader password 0 182roy
amnesiac (config) # boot bootloader password 7 $1$qyP/PKii$2v9FOFcXB5a3emuvLKO3M
```

Product

Interceptor appliance, Steelhead appliance

Related Topics

"show images"

boot system

Description

Boots the specified partition the next time the system is rebooted.

Syntax

boot system <partition>

Parameters

<partition>	Specify the partition to boot: **1** or **2**

Example

```
amnesiac (config) # boot system 1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show images"

hardware nic slot

Description

Configures network interface settings.

Syntax

hardware nic slot <slot> mode <mode>

Parameters

slot <slot>	Specify the network interface card slot. You cannot modify slot 0.
mode <mode>	Specify the network interface slot mode: • **data** - Specify to select data mode. • **inpath** - Specify to select in-path mode, which is the default mode.

Usage

You can use the **hardware nic slot mode data** command option to support features such as Granite. These non-optimization processes typically use the primary and auxiliary interfaces. In a large deployment, iSCSI traffic could easily flood these interfaces. The data mode provides support for converting additional NICs added through an external card for use as data interfaces.

Data interfaces are identified by **ethX_Y** notation, where **eth** denotes a data NIC, **X** denotes the slot, and **Y** denotes the interface/port on the slot.

A reboot is required after changing modes.

This command is not supported on the Steelhead EX560 and EX760 models.

Example

```
amnesiac (config) # hardware nic slot 1 mode data
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"show hardware nic slots," "show interfaces"

hardware spec activate

Description

Activates hardware specification settings.

Syntax

hardware spec activate <spec>

Parameters

<spec>	Specify the specification to activate.

Usage

This command is valid only after you have installed a hardware upgrade license.

Example

```
amnesiac (config) # hardware spec activate 1520
```

Product

Steelhead appliance, CSH

Related Topics

"show hardware spec"

hardware upgrade model

Description

Upgrades hardware settings to reflect the new hardware model.

Syntax

hardware upgrade model

Parameters

None

Usage

This command is valid only after you have installed a hardware upgrade license.

Example

```
amnesiac (config) # hardware upgrade model
```

Product

Steelhead appliance, CSH

Related Topics

"show hardware spec"

image boot

Description

Boots the specified system image by default.

Syntax

image boot <partition>

Parameters

<partition>	Specify the partition to boot: **1** or **2**.

Example

```
amnesiac (config) # image boot 1
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show version"

image check upgrades

Description

Checks for available software upgrades for the release running on the appliance.

Syntax

image check upgrades [version <version>]

Parameters

version <version>	Optionally, specify the target version that you want to upgrade to. This must be a valid version found on the Riverbed support site.

Usage

Use this command to display a list of available software upgrades for the release running on the appliance. You can download one of the versions from the output of the command by using the **image fetch version** command.

The **image check upgrades version** command provides more granularity by displaying the recommended software upgrade path for the release running on the appliance.

Example

```
amnesiac (config) # image check upgrades
Available upgrades:
8.5.3
8.5.3a
8.5.4
8.5.5
9.0.0

amnesiac (config) # image check upgrades version 10.0.0

Upgrade path:
8.5.5 > 9.0.0 > 10.0.0
```

Product

CMC, Steelhead appliance, Steelhead EX appliance

Related Topics

"image fetch version,""show version"

image fetch version

Description

Downloads a version of a software image directly from the Riverbed Support Site.

Syntax

image fetch version <version> [<image-filename>]

Parameters

version <version>	Specify the version of the image to download from the Riverbed Support Site.
<image-filename>	Optionally, specify a local filename for the image.

Usage

Use the **image check upgrades** command to display a list of software versions (delta images) that are available to the appliance for download. The **image fetch version** command is a configuration mode command. The **image fetch** command is available in enable mode.

You can use the version of the downloaded image in the **image install** and **image upgrade** commands. This delta image includes only the incremental changes. The smaller size means a faster download and less load on the network.

Example

```
amnesiac (config) # image fetch version 8.0.1 image.img
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead EX appliance, Steelhead Mobile Controller

Related Topics

"image check upgrades," "image fetch," "image install," "image upgrade," "show images," "show bootvar," "show info," "show version"

image flash backup

Description

Backs up the current image to flash memory.

Syntax

image flash backup <image version>

Parameters

<image version>	Specify the filename under which to store the image on the flash disk.

Example

```
amnesiac (config) # image flash backup image 19
```

Product

Steelhead appliance

Related Topics

"show hardware spec"

image flash restore

Description

Restores the system to an image in flash memory.

Syntax

image flash restore <flash recovery image>

Parameters

<flash recovery image>	The name of the image saved on the flash disk.

Example

```
amnesiac (config) # image flash restore image 19
```

Product

Steelhead appliance,

Related Topics

"show hardware spec"

license autolicense enable

Description

Enables automatic license retrieval.

Syntax

[no] license autolicense enable

Parameters

None

Usage

The **license autolicense enable** command enables the Steelhead appliance, after it is connected to the network, to contact a server managing appliance licenses and download all applicable license keys automatically. This feature eliminates the need to manually fetch and install the licenses from the license portal.

The autolicense process attempts to retrieve the license keys from the server five times, in 5-minute intervals. If no license is downloaded after the five attempts, the autolicense process tries again once a day.

The **no** version of the command disables automatic license retrievals.

Example

```
amnesiac (config) # license autolicense enable
```

Product

CMC, Interceptor appliance, Steelhead appliance

Related Topics

"show autolicense status"

license autolicense fetch

Description

Immediately initiates the retrieval of an automatic license.

Syntax

license autolicense fetch

Parameters

None

Usage

The **license autolicense fetch** command allows you to perform on-demand license retrieval. This command is useful if you need to immediately force a license retrieval (such as the purchase of a new license) and you do not want to wait until the next automatic license retrieval.

Example

```
amnesiac (config) # license autolicense fetch
```

Product

CMC, Interceptor appliance, Steelhead appliance

Related Topics

"show autolicense status"

license autolicense server

Description

Configures autolicense server settings.

Syntax

license autolicense server {<hostname> | <ip-address>}

Parameters

<hostname>	Specify the hostname of the autolicensing server.
<ip-address>	Specify the IP address of the autolicensing server.

Usage

The **license autolicense server** command configures the Steelhead appliance to contact the specified server for license retrieval requests.

Example

```
amnesiac (config) # license autolicense server licensing.company1.com
```

Product

CMC, Interceptor appliance, Steelhead appliance

Related Topics

"show autolicense status"

license client fetch

Description

Forces the license client to update immediately.

Syntax

license client fetch

Parameters

None

Usage

If there is a change in your account (such as if Riverbed has given you an extra license), and the change will be updated whenever the license client runs next, but you want to force it to run immediately, then you can use the **license client fetch** command.

Example

```
amnesiac # license client fetch
```

Product

CMC, Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show license-client"

license client init

Description

Initializes the license client.

Syntax

license client init <license number>

Parameters

<license number>	Specify the license number.

Usage

The license client communicates with the license server. It has two main functions:

- It periodically contacts the license server and checks out and renews the license or lease.
- It enables you to query available features, licenses and other metadata such as serial number.

You can configure the license client to communicate with the license server at the company headquarters or the local license server.

The **no** command option deletes the one-time token or license.

Example

```
amnesiac (config) # license client init 4
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show licenses"

license delete

Description

Deletes the specified license key.

Syntax

license delete <license number>

Parameters

<license number>	Specify the license number.

Example

```
amnesiac (config) # license delete 4
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show licenses"

license install

Description

Installs a new software license key.

Syntax

[no] license install <license key>

Parameters

<license key>	Specify the license key.

Usage

The **no** command option disables this command.

Example

```
amnesiac (config) # license install SH10_B-0000-1-7F14-FC1F
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show licenses"

license request gen-key

Description

Displays a new license request string.

Syntax

license request gen-key

Parameters

None

Example

```
amnesiac (config) # license request gen-key
```

Product

Virtual Steelhead

Related Topics

"show licenses"

license request set-token

Description

Specifies the Riverbed-generated token for Virtual Steelhead.

Syntax

license request set-token

Parameters

None

Example

```
amnesiac (config) # license request set-token
```

Product

Virtual Steelhead

Related Topics

"show licenses"

System Administration and Service Commands

This section describes the system administration and service commands.

hardware watchdog enable

Description

Enables the hardware watchdog, which monitors the system for hardware errors.

Syntax

hardware watchdog enable

Parameters

None

Example

```
amnesiac (config) # hardware watchdog enable
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"show hardware error-log"

hardware watchdog shutdown

Description

Shuts down the hardware watchdog.

Syntax

hardware watchdog shutdown

Parameters

None

Example

```
amnesiac (config) # hardware watchdog shutdown
```

Product

CMC, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"show hardware error-log"

service default-port

Description

Sets the default service port.

Syntax

service default-port <port>

Parameters

<port>	Specify the new target port. The default service ports are 7800 and 7810.

Usage

Service ports are the ports used for inner connections between Steelhead appliances.

You can configure multiple service ports on the server-side of the network for multiple QoS mappings. You define a new service port and then map destination ports to that port, so that QoS configuration settings on the router are applied to that service port.

Example

```
amnesiac (config) # service default-port 7880
```

Product

Steelhead appliance, CSH

Related Topics

"show service ports"

service map-port

Description

Sets a target port for service port mapping.

Syntax

[no] service map-port <dest port> <service port>

Parameters

<dest port>	Specify the destination port to which you want to map.
<service port>	Specify the service port to which you want to map.

Usage

Setting multiple service ports on inner connections enables you to identify the type of traffic and apply QoS settings based on a port.

For example, in an in-path deployment, CIFS and MAPI could be mapped to port 9800 and HTTP to port 9802. You can configure the WAN router to tag packets for port 9800 with the same priority as for port 9802, therefore CIFS and MAPI have the same priority as HTTP. Or you can create a hierarchical mapping where port 9800 receives a higher priority than 9802, and so on.

In the out-of-path deployment, you define which port to listen to on the server Steelhead appliance, and you define an in-path, fixed-target rule on the client Steelhead appliance to point to the service ports for the traffic to which you want to apply QoS.

You cannot map the following ports:

- **Port 22** - Reserved for SSH.
- **Port 80**, **443**, and **446** - Reserved for the Management Console.
- **Port 139**, **445**, and **977** - Reserved for PFS. These ports are only excluded if you have enabled PFS.
- **Port 7800-7899** - Reserved by Riverbed (except 7800 and 7810).
- **Port 8777** - Reserved for CIFS transparent prepopulation. This port is excluded only if you have enabled CIFS prepopulation.

The **no** command option disables the service map.

Example

```
amnesiac (config) # service map-port 7018 8000
```

Product

Steelhead appliance, CSH

Related Topics

"show service ports"

service neural-framing

Description

Dumps or enables neural-framing statistics.

Syntax

[no] service neural-framing [dump | iterations | stats enable]

Parameters

dump	Dumps neural-framing debug files, which are used by **sysdump**.
iterations	Resets iterations before determining heuristic. Used only with the **no** option. For example: **no service-neural framing iterations**.
stats enable	Enables collection of neural-framing statistics.

Usage

By default, neural-framing statistics are disabled. Neural framing enables the Steelhead appliance to select the optimal packet framing boundaries for SDR. SDR encoding provides the best optimization results when the largest buffer is available before a flush is performed.

Neural framing creates a set of heuristics to intelligently determine the optimal moment to flush TCP buffers. The Steelhead appliance continuously evaluates these heuristics and uses the optimal heuristic to maximize the amount of buffered data transmitted in each flush, while minimizing the amount of idle time that the data sits in the buffer.

You must set the neural framing mode (algorithm) for in-path rules for which you want to apply neural framing.

The **no** command option disables neural-framing statistics.

Example

```
amnesiac (config) # service neural-framing stats enable
```

Product

Steelhead appliance, CSH

Related Topics

"show service neural-framing"

service port

Description

Sets a new service port to add for multiple service ports. Service ports are the ports used for inner connections between Steelhead appliances.

Syntax

[no] service port <port>

Parameters

<port>	Specify the new port to add. The default service ports are 7800 and 7810.

Usage

You can configure multiple service ports on the server side of the network for multiple QoS mappings. You define a new service port and then map CIFS ports to that port, so that QoS configuration settings on the router are applied to that service port.

The **no** command option disables the service port.

Example

```
amnesiac (config) # service port 7800
```

Product

Steelhead appliance, CSH

Related Topics

"show service ports"

Steelhead Appliance Feature Configuration Commands

This section describes commands you use to configure Steelhead appliance features. It includes the following sections:

- "In-Path and Virtual In-Path Support Commands" on page 319
- "Management In-Path Interface Commands" on page 358
- "WAN Visibility (Transparency) Commands" on page 360
- "Out-of-Path Support" on page 365
- "Connection Pooling Commands" on page 366
- "Failover Support and Out-of-Band Failure Detection Commands" on page 366
- "Packet-Mode Optimization Commands" on page 372
- "Peering Commands" on page 373
- "High-Speed TCP and Satellite Optimization Commands" on page 381

- "Data Store Configuration Commands" on page 406
- "Data Store Replication and Protection Commands" on page 413
- "WCCP Support Commands" on page 418
- "Simplified Routing Support Commands" on page 425
- "Asymmetric Route Detection Commands" on page 429
- "Connection Forwarding" on page 435
- "Subnet-Side Rule Commands" on page 443
- "Data Flow Support Commands" on page 445
- "Top Talkers Commands" on page 450
- "Path Selection Commands" on page 451
- "QoS Support Commands" on page 456
- "Host Label Commands" on page 498
- "Port Label Commands" on page 500
- "FTP Support Commands" on page 501
- "Domain and Workgroup Commands" on page 502
- "Windows Domain Health Check Commands" on page 509
- "CIFS, SMB, SMB2, and SMB3 Support Commands" on page 518
- "CIFS Prepopulation Support Commands" on page 533
- "HTTP Support Commands" on page 542
- "Oracle Forms Support Commands" on page 558
- "MAPI Support Commands" on page 560
- "MS-SQL Blade Support Commands" on page 568
- "NFS Support Commands" on page 577
- "Lotus Notes Commands" on page 584
- "Citrix Support Commands" on page 588
- "FCIP Support Commands" on page 592
- "SRDF Support Commands" on page 595
- "SnapMirror Support Commands" on page 600
- "Windows Domain Authentication Delegation Commands" on page 604
- "Windows Domain Authentication Replication Commands" on page 610
- "Remote Packet Analysis Integration Commands" on page 611
- "PFS Support Commands" on page 613
- "DNS Cache Commands" on page 625
- "RSP Commands" on page 634
- "IPSec Commands" on page 668
- "SSL Support Commands" on page 672

In-Path and Virtual In-Path Support Commands

This section describes the in-path and virtual in-path support commands.

in-path broadcast support enable

Description

Enables broadcast network support.

Syntax

[no] in-path broadcast support enable

Parameters

None

Usage

The **no** command option disables in-path broadcast support.

Example

```
amnesiac (config) # in-path broadcast support enable
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path"

in-path enable

Description

Enables in-path support. An in-path configuration is a configuration in which the appliance is in the direct path of the client and the server.

Syntax

[no] in-path enable

Parameters

None

Usage

For details, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

The **no** command option disables in-path support.

Example

```
amnesiac (config) # in-path enable
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path"

in-path interface enable

Description

Enables the in-path interface for optimization.

Syntax

[no] in-path interface <interface> enable

Parameters

<interface>	Specify the IP address of the in-path interface. For example, **inpath0_0.**

Usage

The **in-path interface enable** command is only useful when there are multiple NIC cards enabled (for example, with Four-Port LX Single Mode Fiber Gigabit-Ethernet PCI-E cards).

You can force master/backup pairs and connection forwarding connections from a particular interface.

Suppose you have a *quad* deployment in which you have two Steelhead master/backup pairs at different locations (with the master closest to the LAN) and each Steelhead appliance points to the remote Steelhead appliances as connection forwarding neighbors.

In addition, suppose you want to use only fiber interfaces and not the copper interface built into the system. To ensure that the TCP connection for the master/backup pair (default on port 7820) is sourced from the interface you want, you must to ensure that any *lower* in-path interfaces are disabled for usage. Thus, if you do not want to use the copper interfaces built into the Steelhead appliance (that is, inpath0_0 and inpath0_1), but a fiber interface (inpath1_0), you would execute:

```
no in-path interface inpath0_0 enable
no in-path interface inpath0_1 enable
```

Make sure that the following text is displayed in the running configuration ("show configuration running"):

```
in-path interface inpath1_0 enable
```

Then define the failover buddy address to be the **inpath1_0** of the other Steelhead appliance in the master/backup pair. For details about master and backup commands, see "failover enable," "failover master," and "failover enable".

The **no** command option disables the in-path interface.

Example

```
amnesiac (config) # in-path interface inpath0_0 enable
```

Product

Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show ip"

in-path interface vlan

Description

Enables VLAN support for an in-path interface on a trunked link.

Syntax

[no] in-path interface <interface> vlan <id>

Parameters

<interface>	Specify the in-path appliance for which the VLAN applies. For example, **inpath0_0.**
<id>	Specify the VLAN identification number. The VLAN identification number is a value with a range from 0-4094 (0 specifies no tagging).

Usage

The **in-path interface vlan** command enables you to set which VLAN to use for connections. It does not define which VLAN to optimize.

To define which VLAN to optimize, you must define in-path rules and apply them to all VLANs or a specific VLAN.

The **no** command option disables the VLAN support.

Example

```
amnesiac (config) # in-path interface inpath0_0 vlan 26
```

Product

Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show interfaces"

in-path kickoff

Description

Resets open connections upon start up.

Syntax

[no] in-path kickoff

Parameters

None

Usage

When the Steelhead service restarts with kickoff enabled, it breaks existing connections and forces clients to open new connections.

With kickoff disabled, open connections are not broken, but they are unoptimized. New connections are optimized.

When the appliance is not powered on or the Steelhead service is not running, the failover appliance takes over so that connections continue to be made to the WAN.

Generally, connections are short lived and kickoff is not necessary; kickoff is suitable for very challenging remote environments. For example, in an environment with 128 Kbps and 1.5 seconds of latency, you might want to cancel an HTTP download so that your traffic is optimized; whereas in a remote branch-office with a T1 and 35 ms round-trip time, you would want connections to migrate to optimization gracefully, rather than risk interruption with kickoff.

Do not enable kickoff for in-path Steelhead appliances that use auto-discovery or if you do not have a Steelhead appliance on the remote side of the network. If you do not set any in-path rules, the default behavior is to auto-discover all connections. If kickoff is enabled, all connections that existed before the Steelhead appliance started are reset.

The **no** command option disables the in-path kickoff feature.

Example

```
amnesiac (config) # in-path kickoff
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path peering rules"

in-path lsp enable

Description

Enables link state propagation. For example, if the LAN interface drops the link then the WAN also drops the link. Link-state propagation is on by default.

Syntax

[no] in-path lsp enable

Parameters

None

Usage

If you require a Steelhead appliance to fail-to-wire (bypass) when the LAN or WAN ports become disconnected, enable this feature. This feature is similar to what ISPs do in order to follow the state of a link.

You cannot reach a MIP interface when link state propagation (LSP) is also enabled and the corresponding in-path interface fails. In physical in-path deployments, LSP shortens the recovery time of a link failure. LSP communicates link status between the devices connected to the Steelhead appliance and is enabled by default in RiOS v6.0 and later.

The **no** command option disables the link-state propagation.

Example

```
amnesiac (config) # in-path lsp enable
```

Product

Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show in-path lsp"

in-path multi-path maintain

Description

Configures multi-path settings.

Syntax

[no] in-path multi-path maintain

Parameters

None

Usage

The **no** command option disables multi-path support.

Example

```
amnesiac (config) # in-path multi-path maintain
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path peering oobtransparency,"

in-path oop enable

Description

Enables in-path support for networks that utilize Layer-4 switches, PBR, WCCP, and Interceptor appliances.

Syntax

[no] in-path oop enable

Parameters

None

Usage

For details, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

The **no** command option disables OOPsupport.

Example

```
amnesiac (config) # in-path oop enable
```

Product

Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show out-of-path"

in-path rule auto-discover

Description

Adds an auto-discovery rule.

Use the auto-discovery process to determine if a remote Steelhead appliance is able to optimize the connection attempting to be created by this SYN packet. By default, auto-discovery is applied to all IP addresses and ports that are not secure, interactive, or default Riverbed ports. Defining in-path rules modifies this default setting.

Syntax

[no] in-path rule auto-discover [scraddr {<IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstport <port>] | [optimization {normal | sdr-only | sdr-m |compr-only | none}] [preoptimization {ssl | oracle-forms | oracle-forms+ssl | none}] [latency-opt {citrix | http | outlook-anywhr | normal | none}] [vlan <vlan tag ID>] [neural-mode {always | dynamic | never | tcphints}] [cloud-accel <mode>] [wan-visibility {correct | port | full {wan-vis-opt fwd-reset | none}] [description <description>] [auto-kickoff {enable | disable}] [rule-enable {true | false}] [rulenum <rulenum>]

Parameters

srcaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4 -** All IPv4 addresses • **all-ipv6 -** All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6} dstport <port>	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
preoptimization {ssl |oracle-forms | oracle-forms+ssl | none}	Specify a preoptimization policy: • **ssl** - Specify **ssl** to enable SSL preoptimization processing for traffic via SSL secure ports. • **oracle-forms** - Specify **oracle-forms** to enable preoptimization processing for the Oracle Forms browser plug-in. This policy is not compatible with IPv6. • **oracle-forms+ssl** - Specify to enable preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side Steelhead appliance. This policy is not compatible with IPv6. • **none** - Preoptimization processing is set to **none** by default. If SSL or Oracle Forms preoptimization processing is turned on and you want to turn it off for a port, specify **none**. In RiOS v6.0 and later, traffic to port 443 always uses a preoptimization policy of SSL, even if an in-path rule on the client-side Steelhead appliance sets the preoptimization policy to None. To disable the SSL preoptimization for traffic to port 443, you can either: – Disable the SSL optimization on the client or server-side Steelhead appliance. or – Modify the peering rule on the server-side Steelhead appliance by setting the SSL capability control to No Check. **Important:** Make sure you specify **latency-opt** to **none** to ensure that SSL connections are optimized. For Citrix latency optimization to work, set the preoptimization policy to the **preoptimization ssl** option.

optimization {normal | sdr-only | sdr-m |compr-only | none}	Specify an optimization policy: • **normal** - The **normal** optimization policy is the default. The normal process performs LZ compression and SDR. • **sdr-only** - Specify this option to turn off LZ compression. • **sdr-m** - Performs data reduction entirely in memory, which prevents the Steelhead appliance from reading and writing to and from the disk. Enabling this option can yield high LAN-side throughput because it eliminates all disk latency. • **compr-only** - Specify this option to turn off SDR but perform LZ compression. • **none** - Specify this option to turn off LZ compression and SDR. To configure optimization policies for the FTP data channel, define an in-path rule with the destination port 20 and set its optimization policy. Setting QoS for port 20 on the client-side Steelhead appliance affects passive FTP, while setting the QoS for port 20 on the server-side Steelhead appliance affects active FTP. To configure optimization policies for the Messaging Application Protocol Interface (MAPI) connection, define an in-path rule with the destination port 7830 and set its optimization policy.
latency-opt {citrix | http | normal |outlook-anywhr | none}	Specify a latency-optimization policy: • **citrix** - Always use Citrix optimization on connections matching this rule. Citrix optimizations are ICA/CGP over SSL optimizations. For Citrix latency optimization to work, set the preoptimization policy to the **preoptimization ssl** option. This policy is not compatible with IPv6. • **http** - Perform HTTP optimization on connections matching this rule. • **normal** - Perform HTTP optimization on ports 80, 8080, and (with SSL pre-optimization) 443. This is the default setting. • **outlook-anywhr** - Always use Outlook-Anywhere optimization on the connection. This policy is not compatible with IPv6. • **none** - Do not perform latency optimization on connections matching this rule.
vlan <vlan tag ID>	Specify the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0-4094. Specify 0 to mark the link untagged.

neural-mode {always | dynamic | never | tcphints}	Enables neural framing in the Steelhead appliance. Enabling neural framing makes your WAN more efficient by gathering data to select the optimal packet framing boundaries for SDR. If you specify a neural mode, your network experiences a trade-off between the compression and SDR performance, and the latency added to the connection. For different types of traffic, one algorithm might be better than others. Specify one of the following modes: • **always** - Always use the Nagle algorithm. This is the default setting (always wait 6 ms). All data is passed to the codec which attempts to coalesce consume calls (if needed) to achieve better fingerprinting. A timer (6 ms) backs it up and causes leftover data to be consumed. Neural heuristics are computed in this mode but are not used. This mode is not compatible with IPv6. • **dynamic** - Dynamically adjust the Nagle parameters. The Steelhead appliance picks the best algorithm to use by learning what algorithm is best and adapting if the traffic characteristic changes. This mode is not compatible with IPv6. • **never** - Never use the Nagle algorithm. All the data is immediately encoded without waiting for timers to fire or application buffers to fill past a specified threshold. Neural heuristics are computed in this mode but are not used. • **tcphints** - Base setting on TCP hints. If data is received from a partial frame packet or a packet with the TCP PUSH flag set, the encoder encodes the data instead of immediately coalescing it. Neural heuristics are computed in this mode but are not used. This mode is not compatible with IPv6. To configure neural framing for an FTP data channel, define an in-path rule with the destination port 20 and set its optimization policy. To configure neural framing for a MAPI connection, define an in-path rule with the destination port 7830 and set its optimization policy.
cloud-accel <mode>	Specify a cloud action mode for this rule. After you subscribe to a SaaS platform and enable it, ensure that cloud acceleration is ready and enabled. If cloud acceleration is enabled, then by default, connections to the subscribed SaaS platform will be optimized by the SCA. You do not need to add an in-path rule unless you want to optimize specific users and not others. Then, select one of these modes: • **auto** - If the in-path rule matches, the connection is optimized by the SCA connection. • **passthru** - If the in-path rule matches, the connection is not optimized by the SCA, but it follows the rule's other parameters so that the connection might be optimized by this Steelhead appliance with other Steelhead appliances in the network, or it might be passed through.

wan-visibility {correct | port |full [wan-vis-opt fwd-reset | none]}	Enables WAN visibility, which pertains to how packets traversing the WAN are addressed. RiOS v5.0 or later offers three types of WAN visibility modes: correct addressing, port transparency, and full address transparency. You configure WAN visibility on the client-side Steelhead appliance (where the connection is initiated). The server-side Steelhead appliance must also support WAN visibility (RiOS v5.0 or later). • **correct** - Turns WAN visibility off. Correct addressing uses Steelhead appliance IP addresses and port numbers in the TCP/IP packet header fields for optimized traffic in both directions across the WAN. This is the default setting. • **port** - Port address transparency preserves your server port numbers in the TCP/IP header fields for optimized traffic in both directions across the WAN. Traffic is optimized while the server port number in the TCP/IP header field appears to be unchanged. Routers and network monitoring devices deployed in the WAN segment between the communicating Steelhead appliances can view these preserved fields. Use port transparency if you want to manage and enforce QoS policies that are based on destination ports. If your WAN router is following traffic classification rules written in terms of client and network addresses, port transparency enables your routers to use existing rules to classify the traffic without any changes. Port transparency enables network analyzers deployed within the WAN (between the Steelhead appliances) to monitor network activity and to capture statistics for reporting by inspecting traffic according to its original TCP port number. Port transparency does not require dedicated port configurations on your Steelhead appliances. **Note:** Port transparency only provides server port visibility. It does not provide client and server IP address visibility, nor does it provide client port visibility. • **full** - Full address transparency preserves your client and server IP addresses and port numbers in the TCP/IP header fields for optimized traffic in both directions across the WAN. It also preserves VLAN tags. Traffic is optimized while these TCP/IP header fields appear to be unchanged. Routers and network monitoring devices deployed in the WAN segment between the communicating Steelhead appliances can view these preserved fields. If both port transparency and full address transparency are acceptable solutions, port transparency is preferable. Port transparency avoids potential networking risks that are inherent to enabling full address transparency. For details, see the *Steelhead Appliance Deployment Guide*. However, if you must see your client or server IP addresses across the WAN, full transparency is your only configuration option. If you specify **full**, further specify one of the following options: • **wan-vis-opt fwd-reset** - Enables full address transparency and also sends a reset between the probe response and inner SYN. The reset ensures that the packet header uses the same IP address and port numbers as the initial client and server connection. Because the reset creates a fresh inner connection, you can use full transparency in systems with firewalls that perform stateful packet inspection to track the connection state. • **none** - Specify to set the WAN visibility option to none. **Important:** Enabling full address transparency requires symmetrical traffic flows between the client and server. Should any asymmetry exist on the network, enabling full address transparency might yield unexpected results, up to and including loss of connectivity. For details about how to configure WAN visibility, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide.*
description <description>	Specify a description to facilitate communication about network administration.

auto-kickoff {enable | disable}	Enables kickoff, which resets established connections to force them to go through the connection creation process again. Specify one of the following values: • **enable** - Enables kickoff. • **disable** - Disables kickoff. If you enable kickoff, connections that exist when the optimization service is started and restarted are disconnected. When the connections are retried they are optimized. Generally, connections are short lived and kickoff is not necessary. It is suitable for certain long-lived connections, such as data replication, and very challenging remote environments. For example, in an environment with 128 Kbps and 1.5 seconds of latency, you might want to use kickoff to interrupt an HTTP download so that your other traffic is optimized. In a remote branch-office with a T1 and a 35 ms round-trip time, you would want connections to migrate to optimization gracefully, rather than risk interruption with kickoff. RiOS v6.5 provides two ways to enable kickoff: globally and per in-path rule. In most deployments, you do not want to set automatic kickoff globally because it disrupts all connections. When you enable kick off for an in-path rule, once the Steelhead sees any packets that match the IP and port specified in the rule, it sends an RST packet to the client and server maintaining the connection to try to close it. Next, it sets an internal flag to prevent any further kickoffs until the optimization service is once again restarted. By default, auto kickoff per in-path rule is disabled. **Important:** Specifying automatic kickoff per in-path rule enables kickoff even when you disable the global kickoff feature. When global kickoff is enabled, it overrides this setting. You set the global kickoff feature using the Reset Existing Client Connections on Start Up feature, which appears on the Configure > Optimization > General Service Settings page.
rule-enable {true | false}	Specify to enable or disable an in-path rule.
rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**. The rule is inserted into the list at the specified position. For example, if you specify **rulenum** as **3**, the new rule will be #3, the old rule #3 will become #4, and subsequent rules, if any, will also move down the list. Specify **start** for the rule to be the first rule and **end** for the rule to be the last rule. If you do not specify a rule number, the rule is added to the end of the list.

Usage

With regular auto-discovery, the Steelhead appliance finds the first remote Steelhead appliance along the connection path of the TCP connection and optimization occurs there. For example, if you had a deployment with four Steelhead appliances (A, B, C, D) where D represents the appliance that is furthest from A, the Steelhead appliance automatically finds B, then C, and finally D and optimization takes place in each.

With enhanced auto-discovery (automatic peering) the Steelhead appliance automatically finds the furthest Steelhead appliance along the connection path of the TCP connection and optimization occurs there. For example, in a deployment with four Steelhead appliances (A, B, C, D), where D represents the appliance that is furthest from A, the Steelhead appliance automatically finds D. This simplifies configuration and makes your deployment more scalable. For details, see “in-path peering auto”.

Auto-discovery of Steelhead appliances is supported for IPv6 TCP traffic. However, TCP inner connections between the peer Steelhead appliances are strictly IPv4.

By default, enhanced auto-discovery is enabled. If you do not enable enhanced auto-discovery, the Steelhead appliance uses regular auto-discovery. For details, see the Management Console online help or the *Steelhead Appliance Deployment Guide*.

Preventing an Unknown (or Unwanted) Steelhead Appliance from Peering

Automatic peering (enhanced auto-discovery) greatly reduces the complexities and time it takes to deploy Steelhead appliances. It works so seamlessly that occasionally it has the undesirable effect of peering with Steelheads on the Internet that are not in your organization's management domain or your corporate business unit. When an unknown (or unwanted) Steelhead appliance appears connected to your network, you can create a peering rule to prevent it from peering and remove it from your list of connected appliances. The peering rule defines what to do when a Steelhead appliance receives an auto-discovery probe from the unknown Steelhead appliance. To prevent an unknown Steelhead appliance from peering you must add a pass-through peering rule that passes through traffic from the unknown Steelhead appliance in the remote location. For details, see the "in-path peering rule"or the Management Console online help.

The no command option disables the rule. The no command option has the following syntax: **no in-path rule <rulenum>**

Example

```
amnesiac (config) # in-path rule auto-discover srcaddr 10.10.10.1/24 port 2121 dstaddr
10.24.24.24.1/24 rulenum 2
```

Product

Steelhead appliance, CSH

Related Topics

"in-path rule edit auto-discover," "show in-path," "show in-path rules"

in-path rule edit auto-discover

Description

Edits an auto-discovery rule.

Use the auto-discovery process to determine if a remote Steelhead appliance is able to optimize the connection attempting to be created by this SYN packet. By default, auto-discovery is applied to all IP addresses and ports that are not secure, interactive, or default Riverbed ports. Defining in-path rules modifies this default setting.

Syntax

in-path rule edit rulenum <rulenum> auto-discover [scraddr {<IPv4-addr> | <IPv6-addr> | all-ip | all-ipv4 | all-ipv6>}] [dstaddr {<IPv4-addr > | <IPv6-addr> | all-ip | all-ipv4 | all-ipv6>}] [dstport <port>] [optimization {normal | sdr-only | sdr-m | compr-only | none}] [preoptimization {ssl | oracle-forms | oracle-forms+ssl | none}] [latency-opt {citrix | http | outlook-anywhr | normal | none}] [vlan <vlan tag ID>] [neural-mode {always | dynamic | never | tcphints}] [wan-visibility correct | port | full {wan-vis-opt fwd-reset | none}] [description <description>] [auto-kickoff {enable | disable}] [rule-enable {true | false}]

Parameters

rulenum <rulenum>	Specify the rule number to edit: **1-N** or **start** or **end**.
srcaddr {<IPv4-addr| IPv6-addr | all-ip |all-ipv4 | all-ipv6>}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>} dstport <port>	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
optimization {normal | sdr-only | sdr-m |compr-only | none}	Specify an optimization policy: • **normal** - The **normal** optimization policy is the default. The normal process performs LZ compression and SDR. • **sdr-only** - Specify this option to turn off LZ compression. • **sdr-m** - Performs data reduction entirely in memory, which prevents the Steelhead appliance from reading and writing to and from the disk. Enabling this option can yield high LAN-side throughput because it eliminates all disk latency. • **compr-only** - Specify this option to turn off SDR but perform LZ compression. • **none** - Specify this option to turn off LZ compression and SDR. To configure optimization policies for the FTP data channel, define an in-path rule with the destination port 20 and set its optimization policy. Setting QoS for port 20 on the client-side Steelhead appliance affects passive FTP, while setting the QoS for port 20 on the server-side Steelhead appliance affects active FTP. To configure optimization policies for the Messaging Application Protocol Interface (MAPI) connection, define an in-path rule with the destination port 7830 and set its optimization policy.

preoptimization {**ssl** |**oracle-forms** | **oracle-forms+ssl** | **none**}	Specify a preoptimization policy: • **ssl** - Specify **ssl** to enable SSL preoptimization processing for traffic via SSL secure ports. • **oracle-forms** - Specify **oracle-forms** to enable preoptimization processing for the Oracle Forms browser plug-in. This policy is not compatible with IPv6. • **oracle-forms+ssl** - Specify to enable preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side Steelhead appliance. This policy is not compatible with IPv6. • **none** - Preoptimization processing is set to **none** by default. If SSL or Oracle Forms preoptimization processing is turned on and you want to turn it off for a port, specify **none**. In RiOS v6.0 and later, traffic to port 443 always uses a preoptimization policy of SSL even if an in-path rule on the client-side Steelhead appliance sets the preoptimization policy to None. To disable the SSL preoptimization for traffic to port 443, you can either: – Disable the SSL optimization on the client or server-side Steelhead appliance. or – Modify the peering rule on the server-side Steelhead appliance by setting the SSL capability control to No Check. **Important:** Make sure you specify **latency-opt** to **none** to ensure that SSL connections are optimized. For Citrix latency optimization to work, set the preoptimization policy to the **preoptimization ssl** option.
latency-opt {**citrix** | **http** | **normal** |**outlook-anywhr** | **none**}	Specify a latency-optimization policy: • **citrix** - Always use Citrix optimization on connections matching this rule. Citrix optimizations are ICA/CGP over SSL optimizations. For Citrix latency optimization to work, set the preoptimization policy to the **preoptimization ssl** option. This policy is not compatible with IPv6. • **http** - Perform HTTP optimization on connections matching this rule. • **normal** - Perform HTTP optimization on ports 80, 8080, and (with SSL pre-optimization) 443. This is the default setting. • **outlook-anywhr** - Always use Outlook-Anywhere optimization on the connection. This policy is not compatible with IPv6. • **none** - Do not perform latency optimization on connections matching this rule.
vlan <vlan tag ID>	Specify the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0-4094. Specify 0 to mark the link untagged.

neural-mode {always | dynamic | never | tcphints}	Enables neural framing in the Steelhead appliance. Enabling neural framing makes your WAN more efficient by gathering data to select the optimal packet framing boundaries for SDR. If you specify a neural mode, your network experiences a trade-off between the compression and SDR performance, and the latency added to the connection. For different types of traffic, one algorithm might be better than others. Specify one of the following modes: • **always** - Always use the Nagle algorithm. This is the default setting (always wait 6 ms). All data is passed to the codec which attempts to coalesce consume calls (if needed) to achieve better fingerprinting. A timer (6 ms) backs it up and causes leftover data to be consumed. Neural heuristics are computed in this mode but are not used. This mode is not compatible with IPv6. • **dynamic** - Dynamically adjust the Nagle parameters. The Steelhead appliance picks the best algorithm to use by learning what algorithm is best and adapting if the traffic characteristic changes. This mode is not compatible with IPv6. • **never** - Never use the Nagle algorithm. All the data is immediately encoded without waiting for timers to fire or application buffers to fill past a specified threshold. Neural heuristics are computed in this mode but are not used. • **tcphints** - Base setting on TCP hints. If data is received from a partial frame packet or a packet with the TCP PUSH flag set, the encoder encodes the data instead of immediately coalescing it. Neural heuristics are computed in this mode but are not used. This mode is not compatible with IPv6. To configure neural framing for an FTP data channel, define an in-path rule with the destination port 20 and set its optimization policy. To configure neural framing for a MAPI connection, define an in-path rule with the destination port 7830 and set its optimization policy.

wan-visibility {correct | port |full [wan-vis-opt fwd-reset | none]}	Enables WAN visibility, which pertains to how packets traversing the WAN are addressed. RiOS v5.0 or later offers three types of WAN visibility modes: correct addressing, port transparency, and full address transparency. You configure WAN visibility on the client-side Steelhead appliance (where the connection is initiated). The server-side Steelhead appliance must also support WAN visibility (RiOS v5.0 or later). • **correct** - Turns WAN visibility off. Correct addressing uses Steelhead appliance IP addresses and port numbers in the TCP/IP packet header fields for optimized traffic in both directions across the WAN. This is the default setting. • **port** - Port address transparency preserves your server port numbers in the TCP/IP header fields for optimized traffic in both directions across the WAN. Traffic is optimized while the server port number in the TCP/IP header field appears to be unchanged. Routers and network monitoring devices deployed in the WAN segment between the communicating Steelhead appliances can view these preserved fields. Use port transparency if you want to manage and enforce QoS policies that are based on destination ports. If your WAN router is following traffic classification rules written in terms of client and network addresses, port transparency enables your routers to use existing rules to classify the traffic without any changes. Port transparency enables network analyzers deployed within the WAN (between the Steelhead appliances) to monitor network activity and to capture statistics for reporting by inspecting traffic according to its original TCP port number. Port transparency does not require dedicated port configurations on your Steelhead appliances. **Note:** Port transparency only provides server port visibility. It does not provide client and server IP address visibility, nor does it provide client port visibility. • **full** - Full address transparency preserves your client and server IP addresses and port numbers in the TCP/IP header fields for optimized traffic in both directions across the WAN. It also preserves VLAN tags. Traffic is optimized while these TCP/IP header fields appear to be unchanged. Routers and network monitoring devices deployed in the WAN segment between the communicating Steelhead appliances can view these preserved fields. If both port transparency and full address transparency are acceptable solutions, port transparency is preferable. Port transparency avoids potential networking risks that are inherent to enabling full address transparency. For details, see the *Steelhead Appliance Deployment Guide*. However, if you must see your client or server IP addresses across the WAN, full transparency is your only configuration option. If you specify **full**, further specify one of the following options: • **wan-vis-opt fwd-reset** - Enables full address transparency and also sends a reset between the probe response and inner SYN. The reset ensures that the packet header uses the same IP address and port numbers as the initial client and server connection. Because the reset creates a fresh inner connection, you can use full transparency in systems with firewalls that perform stateful packet inspection to track the connection state. • **none** - Specify to set the WAN visibility option to none. **Important:** Enabling full address transparency requires symmetrical traffic flows between the client and server. Should any asymmetry exist on the network, enabling full address transparency might yield unexpected results, up to and including loss of connectivity. For details about how to configure WAN visibility, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide.*
description <description>	Specify a description to facilitate communication about network administration.

auto-kickoff {**enable** | **disable**}	Enables kickoff, which resets established connections to force them to go through the connection creation process again. Specify one of the following values: • **enable** - Enables kickoff. • **disable** - Disables kickoff. If you enable kickoff, connections that exist when the optimization service is started and restarted are disconnected. When the connections are retried they are optimized. Generally, connections are short lived and kickoff is not necessary. It is suitable for certain long-lived connections, such as data replication, and very challenging remote environments. For example, in an environment with 128 Kbps and 1.5 seconds of latency, you might want to use kickoff to interrupt an HTTP download so that your other traffic is optimized. In a remote branch-office with a T1 and a 35 ms round-trip time, you would want connections to migrate to optimization gracefully, rather than risk interruption with kickoff. RiOS v6.5 provides two ways to enable kickoff: globally and per in-path rule. In most deployments, you do not want to set automatic kickoff globally because it disrupts all connections. When you enable kick off for an in-path rule, once the Steelhead sees any packets that match the IP and port specified in the rule, it sends an RST packet to the client and server maintaining the connection to try to close it. Next, it sets an internal flag to prevent any further kickoffs until the optimization service is once again restarted. By default, auto kickoff per in-path rule is disabled. **Important:** Specifying automatic kickoff per in-path rule enables kickoff even when you disable the global kickoff feature. When global kickoff is enabled, it overrides this setting. You set the global kickoff feature using the Reset Existing Client Connections on Start Up feature, which appears on the Configure > Optimization > General Service Settings page.
rule-enable {**true** | **false**}	Specify to enable or disable an in-path rule.

Usage

The **in-path rule auto-discover** command adds an auto-discovery rule.

When you edit a rule of the same type (for example, **in-path rule auto-discover** to **in-path rule edit auto-discover**), the parameters you specify in the edit command are applied and the other parameters remain the same as the default value or the previously configured value of the **in-path rule auto-discover** command. However, if you change the rule type (for example, **in-path rule auto-discover** to **in-path rule edit fixed-target**), the parameters you specify in the edit command are applied and the rest of the parameters are reset to the default of the new rule type (in this example, resets to in-path fixed-target rules).

Example

```
amnesiac (config) # in-path rule edit rulenum 2 auto-discover srcaddr 10.10.10.1/24 port 2121
dstaddr 10.24.24.24.1/24
```

Product

Steelhead appliance, CSH

Related Topics

"in-path rule auto-discover," "show in-path," "show in-path rules"

in-path rule deny

Description

Adds an in-path rule that rejects connection requests.

Syntax

[no] in-path rule deny [scraddr {<IPv4-addr> | <IPv6-addr>| all-ip |all-ipv4 | all-ipv6}] [dstaddr {<IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}] [dstport <port>] | [vlan <vlan tag ID>] | [rule-enable {true | false}] | [rulenum <rulenum>] [description <description>]

Parameters

srcaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6} **dstport <port>**	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
vlan <vlan tag ID>	Specify the VLAN tag ID (if any). The VLAN tag ID is a number with a range from 0-4094. Specify 0 to mark the link untagged.
rule-enable {true | false}	Specify to enable or disable an in-path rule.
rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**. The rule is inserted into the list at the specified position. For example, if you specify **rulenum** as 3, the new rule will be #3, the old rule #3 will become #4, and subsequent rules, if any, will also move down the list. Specify start for the rule to be the first rule and end for the rule to be the last rule. If you do not specify a rule number, the rule is added to the end of the list.
description <description>	Specify a description to facilitate network administration.

Usage

The Steelhead appliance automatically intercepts traffic on all IP addresses (**0.0.0.0**) and ports (**all**) and optimizes according to default settings.

Specify deny rules for traffic you want to reject and return a message to the client that the request has been denied.

The **no** command option disables the rule. The **no** command option syntax is:

no in-path rule <rulenum>

Example

```
amnesiac (config) # in-path rule deny srcaddr 10.0.0.1/24 dstaddr 10.0.0.2/24 rulenum 5 description
test
```

Product

Steelhead appliance, CSH

Related Topics

"in-path rule edit deny," "show in-path," "show in-path rules"

in-path rule edit deny

Description

Edits an in-path rule that rejects connection requests.

Syntax

in-path rule edit rulenum <rulenum> deny [scraddr {<IPv4-addr> | <IPv6-addr>| all-ip |all-ipv4 | all-ipv6}] [dstaddr {<IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}] [dstport <port>] [vlan <vlan tag ID>] [rule-enable {true | false}] [description <description>]

Parameters

rulenum <rulenum>	Specify the rule number to edit: **1-N** or **start** or **end**.
srcaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6} dstport <port>	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
vlan <vlan tag ID>	Specify the VLAN tag ID (if any). The VLAN tag ID is a number with a range from 0-4094. Specify 0 to mark the link untagged.
rule-enable {true | false}	Specify to enable or disable an in-path rule.
description <description>	Specify a description to facilitate network administration.

Usage

Use the **in-path rule deny** command to add an in-path rule that rejects connection requests.

Example

```
amnesiac (config) # in-path rule edit rulenum 5 deny srcaddr 10.0.0.1/24 dstaddr 10.0.0.2/24
description test
```

Product

Steelhead appliance, CSH

Related Topics

"in-path rule deny," "show in-path," "show in-path rules"

in-path rule discard

Description

Adds an in-path rule that drops connections.

Syntax

[no] in-path rule discard [scraddr {<IPv4-addr> | <IPv6-addr>| all-ip |all-ipv4 | all-ipv6}] [dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstport <port>] [vlan <vlan tag ID>] |[rule-enable {true | false}] [rulenum <rulenum>] [description <description>]

Parameters

srcaddr {<IPv4-addr>| <IPv6-addr>| all-ip |all-ipv4 | all-ipv6}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6} **dstport <port>**	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
vlan <vlan tag ID>	Specify the VLAN tag ID (if any). The VLAN tag ID is a number with a range from 0-4094. Specify 0 to mark the link untagged.
rule-enable {true | false}	Specify to enable or disable an in-path rule.
rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**. The rule is inserted into the list at the specified position. For example, if you specify **rulenum** as 3, the new rule will be #3, the old rule #3 will become #4, and subsequent rules, if any, will also move down the list. Specify start for the rule to be the first rule and end for the rule to be the last rule. If you do not specify a rule number, the rule is added to the end of the list.
description <description>	Specify a description to facilitate communication about network administration.

Usage

The Steelhead appliance automatically intercepts traffic on all IP addresses (**0.0.0.0**) and ports (**all**) and optimizes according to default settings.

Specify discard rules for traffic that you want to drop silently instead of optimizing or passing through.

The **no** command option disables the rule. The **no** command option has the following syntax:

no in-path rule <rulenum>.

Example

```
amnesiac (config) # in-path rule discard srcaddr 10.0.0.2 dstaddr 10.0.0.1 port 1234 rulenum 2
```

Product

Steelhead appliance, CSH

Related Topics

"in-path rule edit discard," "show in-path," "show in-path rules"

in-path rule edit discard

Description

Edits an in-path rule that drops connections.

Syntax

[no] in-path rule edit rulenum <rulenum> discard [scraddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstport <port>] [vlan <vlan tag ID>] |rule-enable {true | false} [description <description>]

Parameters

rulenum <rulenum>	Specify the rule number to edit: **1-N** or **start** or **end**.
srcaddr {<IPv4-addr>| <IPv6-addr>| all-ip |all-ipv4 | all-ipv6}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6} **dstport <port>**	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
vlan <vlan tag ID>	Specify the VLAN tag ID (if any). The VLAN tag ID is a number with a range from 0-4094. Specify 0 to mark the link untagged.
rule-enable {true | false}	Specify to enable or disable an in-path rule.
description <description>	Specify a description to facilitate network administration.

Usage

Use the **in-path rule discard** command to add an in-path rule that drops connections.

Example

```
amnesiac (config) # in-path rule edit rulenum 2 discard srcaddr 10.0.0.2 dstaddr 10.0.0.1 port 1234
```

Product

Steelhead appliance, CSH

Related Topics

"in-path rule discard," "show in-path," "show in-path rules"

in-path rule edit disable

Description

Disables a single in-path rule.

Syntax

in-path rule edit rulenum <rule number> disable

Parameters

rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**.

Example

```
amnesiac (config) # in-path rule edit rulenum 3 disable
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path," "show in-path rules"

in-path rule edit enable

Description

Enables a single in-path rule.

Syntax

in-path rule edit rulenum <rule number> enable

Parameters

rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**.

Example

```
amnesiac (config) # in-path rule edit rulenum 3 enable
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path," "show in-path rules"

in-path rule edit fixed-target

Description

Edits a fixed-target in-path rule.

Syntax

in-path rule edit rulenum <rulenum> fixed-target target-addr {<IPv4-addr >| <IPv6-addr>} [target-port <port>] [dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}] [dstport <port>] [scraddr {<IPv4-addr | IPv6-addr | all-ip |all-ipv4 | all-ipv6>}] [backup-addr <IPv4-addr> | <IPv6-addr>] [backup-port <port>] [optimization {normal | sdr-only |sdr-m | compr-only | none}] [preoptimization {ssl |oracle-forms |oracle-forms+ssl | none}] [latency-opt {citrix | http | normal| outlook-anywhr | none}] [neural-mode {always | dynamic | never | tcphints}] [vlan <vlan tag ID>] [description <description>] [auto-kickoff {enable | disable}]| [rule-enable {true| false}]

Parameters

rulenum <rulenum>	Specify the rule number to edit: **1-N** or **start** or **end**.
target-addr {<IPv4-addr> | <IPv6-addr>} target-port <port>	Specify the target appliance address for this rule. For the network address, use the format XXX.XXX.XXX.XXX for IPv4 or X:X:X::X/XXX for IPv6. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
backup-addr {<IPv4-addr> | <IPv6-addr>} backup-port <port>	Specify a backup appliance address for this rule (if any). For the network address, use the format XXX.XXX.XXX.XXX for IPv4 or X:X:X::X/XXX for IPv6. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
srcaddr <IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6} dstport <port>}	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
optimization {normal | sdr-only | sdr-m | compr-only | none}	Specify an optimization policy: • **normal** - The **normal** optimization policy is the default. The normal process performs LZ compression and SDR. • **sdr-only -** Specify this option to turn off LZ compression. • **sdr-m -** Performs data reduction entirely in memory, which prevents the Steelhead appliance from reading and writing to and from the disk. Enabling this option can yield high LAN-side throughput because it eliminates all disk latency. • **compr-only** - Specify this option to turn off SDR but perform LZ compression. • **none -** Specify this option to turn off LZ compression and SDR. To configure optimization policies for the FTP data channel, define an in-path rule with the destination port 20 and set its optimization policy. Setting QoS for port 20 on the client-side Steelhead appliance affects passive FTP, while setting the QoS for port 20 on the server-side Steelhead appliance affects active FTP. To configure optimization policies for the MAPI connection, define an in-path rule with the destination port 7830 and set its optimization policy.

preoptimization {**ssl** |**oracle-forms** | **oracle-forms+ssl** | **none**}	Specify a preoptimization policy: • **ssl** - Specify **ssl** to enable SSL preoptimization processing for traffic via SSL secure ports. • **oracle-forms** - Specify **oracle-forms** to enable preoptimization processing for the Oracle Forms browser plug-in. This policy is not compatible with IPv6. • **oracle-forms+ssl** - Specify to enable preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side Steelhead appliance. This policy is not compatible with IPv6. • **none** - Preoptimization processing is set to **none** by default. If SSL or Oracle Forms preoptimization processing is turned on and you want to turn it off for a port, specify **none**. In RiOS v6.0 and later, traffic to port 443 always uses a preoptimization policy of SSL even if an in-path rule on the client-side Steelhead appliance sets the preoptimization policy to None. To disable the SSL preoptimization for traffic to port 443, you can either: – Disable the SSL optimization on the client or server-side Steelhead appliance. or – Modify the peering rule on the server-side Steelhead appliance by setting the SSL capability control to No Check. **Important:** Make sure you specify **latency-opt** to **none** to ensure that SSL connections are optimized. For Citrix latency optimization to work, set the preoptimization policy to the **preoptimization ssl** option.
latency-opt {**citrix** | **http** | **normal** |**outlook-anywhr** | **none**}	Specify a latency-optimization policy: • **citrix** - Always use Citrix optimization on connections matching this rule. Citrix optimizations are ICA/CGP over SSL optimizations. For Citrix latency optimization to work, set the preoptimization policy to the **preoptimization ssl** option. This policy is not compatible with IPv6. • **http** - Perform HTTP optimization on connections matching this rule. • **normal** - Perform HTTP optimization on ports 80, 8080, and (with SSL pre-optimization) 443. This is the default setting. • **outlook-anywhr** - Always use Outlook-Anywhere optimization on the connection. This policy is not compatible with IPv6. • **none** - Do not perform latency optimization on connections matching this rule.

neural-mode {always | dynamic | never | tcphints}	Enables neural framing in the Steelhead appliance. Enabling neural framing makes your WAN more efficient by gathering data to select the optimal packet framing boundaries for SDR. If you specify a neural mode, your network will experience a trade-off between the compression and SDR performance, and the latency added to the connection. For different types of traffic, one algorithm might be better than others. Specify one of the following modes: • **always -** Always use the Nagle algorithm. This is the default setting (always wait 6 ms). All data is passed to the codec which attempts to coalesce consume calls (if needed) to achieve better fingerprinting. A timer (6 ms) backs it up and causes leftover data to be consumed. Neural heuristics are computed in this mode but are not used. This mode is not compatible with IPv6. • **dynamic -** Dynamically adjust the Nagle parameters. The Steelhead appliance picks the best algorithm to use by learning what algorithm is best and adapting if the traffic characteristic changes. This mode is not compatible with IPv6. • **never -** Never use the Nagle algorithm. All the data is immediately encoded without waiting for timers to fire or application buffers to fill past a specified threshold. Neural heuristics are computed in this mode but are not used. • **tcphints -** Base setting on TCP hints. If data is received from a partial frame packet or a packet with the TCP PUSH flag set, the encoder encodes the data instead of immediately coalescing it. Neural heuristics are computed in this mode but are not used. This mode is not compatible with IPv6. To configure neural framing for an FTP data channel, define an in-path rule with the destination port 20 and set its optimization policy. To configure neural framing for a MAPI connection, define an in-path rule with the destination port 7830 and set its optimization policy.
vlan <vlan tag ID>	Specify the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0-4094. Specify 0 to mark the link untagged.
description <description>	Specify a description to facilitate network administration.
rule-enable {true | false}	Specify to enable or disable an in-path rule.

auto-kickoff {**enable** | **disable**}	Enables kickoff, which resets established connections to force them to go through the connection creation process again. Specify one of the following values: • **enable** - Enables kickoff. • **disable** - Disables kickoff. If you enable kickoff, connections that exist when the optimization service is started and restarted are disconnected. When the connections are retried they are optimized. Generally, connections are short lived and kickoff is not necessary. It is suitable for certain long-lived connections, such as data replication, and very challenging remote environments. For example, in an environment with 128 Kbps and 1.5 seconds of latency, you might want to use kickoff to interrupt an HTTP download so that your other traffic is optimized. In a remote branch-office with a T1 and a 35 ms round-trip time, you would want connections to migrate to optimization gracefully, rather than risk interruption with kickoff. RiOS v6.5 provides two ways to enable kickoff: globally and per in-path rule. In most deployments, you do not want to set automatic kickoff globally because it disrupts all connections. When you enable kick off for an in-path rule, once the Steelhead sees any packets that match the IP and port specified in the rule, it sends an RST packet to the client and server maintaining the connection to try to close it. Next, it sets an internal flag to prevent any further kickoffs until the optimization service is once again restarted. By default, auto kickoff per in-path rule is disabled. **Important:** Specifying automatic kickoff per in-path rule enables kickoff even when you disable the global kickoff feature. When global kickoff is enabled, it overrides this setting. You set the global kickoff feature using the Reset Existing Client Connections on Start Up feature, which appears on the Configure > Optimization > General Service Settings page.
rule-enable {**true** | **false**}	Specify to enable or disable an in-path rule.

Usage

The **in-path rule fixed-target** command adds a fixed-target in-path rule.

When you edit a rule of the same type (for example, **in-path rule fixed-target** to **in-path rule edit fixed-target**), the parameters you specify in the edit command are applied and the other parameters remain the same as the default value or the previously configured value of the **in-path rule fixed-target** command. However, if you change the rule type (for example, **in-path rule fixed-target** to **in-path rule edit auto-discover**), the parameters you specify in the edit command are applied and the rest of the parameters are reset to the default of the new rule type (in this example, resets to in-path auto-discover rules).

Example

```
amnesiac (config) # in-path rule edit rulenum 1 fixed-target target-addr 10.4.40.101 dstaddr
10.4.49.88/32
```

Product

Steelhead appliance, CSH

Related Topics

"in-path rule fixed-target," "show in-path," "show in-path rules"

in-path rule fixed-target

Description

Adds a fixed-target in-path rule.

Syntax

[no] in-path rule fixed-target target-addr {<IPv4-addr> | <IPv6-addr>} [target-port <port>] [dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}] [dstport <port>] [scraddr {<IPv4-addr> | <IPv6-addr>| all-ip |all-ipv4 | all-ipv6>}] [backup-addr {<IPv4-addr> | <IPv6-addr>}] [backup-port <port>] [optimization {normal | sdr-only |sdr-m | compr-only | none}] | [preoptimization {ssl |oracle-forms | oracle-forms+ssl |none}] [latency-opt {citrix | http | normal| outlook-anywhr | none}] [neural-mode {always | dynamic | never | tcphints}] [vlan <vlan tag ID>] [description <description>] [auto-kickoff {enable | disable}] [rulenum <rulenum>] [rule-enable {true | false}]

Parameters

target-addr {<IPv4-addr | IPv6-addr>} target-port <port>	Specify the fixed-target appliance address. For the network address, use the format XXX.XXX.XXX.XXX for IPv4 or X:X:X:X/XXX for IPv6. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
backup-addr <IPv4-addr> | <IPv6-addr> backup-port <port>	Specify a backup appliance for this rule (if any). For the network address, use the format XXX.XXX.XXX.XXX for IPv4 or X:X:X::X/XXX for IPv6. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
dstaddr <IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6} dstport <port>	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
srcaddr <IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
optimization {normal | sdr-only | sdr-m | compr-only | none}	Specify an optimization policy: • **normal** - The **normal** optimization policy is the default. The normal process performs LZ compression and SDR. • **sdr-only -** Specify this option to turn off LZ compression. • **sdr-m -** Performs data reduction entirely in memory, which prevents the Steelhead appliance from reading and writing to and from the disk. Enabling this option can yield high LAN-side throughput because it eliminates all disk latency. • **compr-only** - Specify this option to turn off SDR but perform LZ compression. • **none -** Specify this option to turn off LZ compression and SDR. To configure optimization policies for the FTP data channel, define an in-path rule with the destination port 20 and set its optimization policy. Setting QoS for port 20 on the client-side Steelhead appliance affects passive FTP, while setting the QoS for port 20 on the server-side Steelhead appliance affects active FTP. To configure optimization policies for the MAPI connection, define an in-path rule with the destination port 7830 and set its optimization policy.

preoptimization {**ssl** |**oracle-forms** | **oracle-forms+ssl** | **none**}	Specify a preoptimization policy: • **ssl** - Specify **ssl** to enable SSL preoptimization processing for traffic via SSL secure ports. • **oracle-forms** - Specify **oracle-forms** to enable preoptimization processing for the Oracle Forms browser plug-in. This policy is not compatible with IPv6. • **oracle-forms+ssl** - Specify to enable preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side Steelhead appliance. This policy is not compatible with IPv6. • **none** - Preoptimization processing is set to **none** by default. If SSL or Oracle Forms preoptimization processing is turned on and you want to turn it off for a port, specify **none**. In RiOS v6.0 and later, traffic to port 443 always uses a preoptimization policy of SSL even if an in-path rule on the client-side Steelhead appliance sets the preoptimization policy to None. To disable the SSL preoptimization for traffic to port 443, you can either: – Disable the SSL optimization on the client or server-side Steelhead appliance. or – Modify the peering rule on the server-side Steelhead appliance by setting the SSL capability control to No Check. **Important:** Make sure you specify **latency-opt** to **none** to ensure that SSL connections are optimized. For Citrix latency optimization to work, set the preoptimization policy to the **preoptimization ssl** option.
latency-opt {**citrix** | **http** | **normal** |**outlook-anywhr** | **none**}	Specify a latency-optimization policy: • **citrix** - Always use Citrix optimization on connections matching this rule. Citrix optimizations are ICA/CGP over SSL optimizations. For Citrix latency optimization to work, set the preoptimization policy to the **preoptimization ssl** option. This policy is not compatible with IPv6. • **http** - Perform HTTP optimization on connections matching this rule. • **normal** - Perform HTTP optimization on ports 80, 8080, and (with SSL pre-optimization) 443. This is the default setting. • **outlook-anywhr** - Always use Outlook-Anywhere optimization on the connection. This policy is not compatible with IPv6. • **none** - Do not perform latency optimization on connections matching this rule.

neural-mode {**always** | **dynamic** | **never** | **tcphints**}	Enables neural framing in the Steelhead appliance. Enabling neural framing makes your WAN more efficient by gathering data to select the optimal packet framing boundaries for SDR. If you specify a neural mode, your network will experience a trade-off between the compression and SDR performance, and the latency added to the connection. For different types of traffic, one algorithm might be better than others. Specify one of the following modes: • **always -** Always use the Nagle algorithm. This is the default setting (always wait 6 ms). All data is passed to the codec which attempts to coalesce consume calls (if needed) to achieve better fingerprinting. A timer (6 ms) backs it up and causes leftover data to be consumed. Neural heuristics are computed in this mode but are not used. This mode is not compatible with IPv6. • **dynamic -** Dynamically adjust the Nagle parameters. The Steelhead appliance picks the best algorithm to use by learning what algorithm is best and adapting if the traffic characteristic changes. This mode is not compatible with IPv6. • **never -** Never use the Nagle algorithm. All the data is immediately encoded without waiting for timers to fire or application buffers to fill past a specified threshold. Neural heuristics are computed in this mode but are not used. • **tcphints -** Base setting on TCP hints. If data is received from a partial frame packet or a packet with the TCP PUSH flag set, the encoder encodes the data instead of immediately coalescing it. Neural heuristics are computed in this mode but are not used. This mode is not compatible with IPv6. To configure neural framing for an FTP data channel, define an in-path rule with the destination port 20 and set its optimization policy. To configure neural framing for a MAPI data channel, define an in-path rule with the destination port 7830 and set its optimization policy.
vlan <vlan tag ID>	Specify the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0-4094. Specify 0 to mark the link untagged.
description <description>	Specify a description to facilitate network administration.

auto-kickoff {enable | disable}	Enables kickoff, which resets established connections to force them to go through the connection creation process again. Specify one of the following values: • **enable** - Enables kickoff. • **disable** - Disables kickoff. If you enable kickoff, connections that exist when the optimization service is started and restarted are disconnected. When the connections are retried they are optimized. Generally, connections are short lived and kickoff is not necessary. It is suitable for certain long-lived connections, such as data replication, and very challenging remote environments. For example, in an environment with 128 Kbps and 1.5 seconds of latency, you might want to use kickoff to interrupt an HTTP download so that your other traffic is optimized. In a remote branch-office with a T1 and a 35 ms round-trip time, you would want connections to migrate to optimization gracefully, rather than risk interruption with kickoff. RiOS v6.5 provides two ways to enable kickoff: globally and per in-path rule. In most deployments, you do not want to set automatic kickoff globally because it disrupts all connections. When you enable kick off for an in-path rule, once the Steelhead sees any packets that match the IP and port specified in the rule, it sends an RST packet to the client and server maintaining the connection to try to close it. Next, it sets an internal flag to prevent any further kickoffs until the optimization service is once again restarted. By default, auto kickoff per in-path rule is disabled. **Important:** Specifying automatic kickoff per in-path rule enables kickoff even when you disable the global kickoff feature. When global kickoff is enabled, it overrides this setting. You set the global kickoff feature using the Reset Existing Client Connections on Start Up feature, which appears on the Configure > Optimization > General Service Settings page.
rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**. The rule is inserted into the list at the specified position. For example, if you specify **rulenum** as **3**, the new rule will be #3, the old rule #3 will become #4, and subsequent rules, if any, will also move down the list. Specify **start** for the rule to be the first rule and **end** for the rule to be the last rule. If you do not specify a rule number, the rule is added to the end of the list.
rule-enable {true | false}	Specify to enable or disable an in-path rule.

Usage

Defining a fixed-target rule uses a specified remote Steelhead appliance as an optimization peer.

You must specify at least one remote target Steelhead appliance to optimize (and, optionally, which ports and backup Steelhead appliances), and add rules to specify the network of servers, ports, port labels, and out-of-path Steelhead appliances to use.

The Steelhead appliance automatically intercepts traffic on all IP addresses (**0.0.0.0**) and ports (**all**) and optimizes according to default settings.

Specify fixed-target rules to set out-of-path Steelhead appliances near the target server that you want to optimize.

The **no** command option disables the rule. The **no** command option has the following syntax:

```
no in-path rule <rulenum>.
```

Note: In out-of-path deployments, to optimize MAPI Exchange 2003 by destination port, you must define fixed-target, in-path rules that specify the following ports on the client-side Steelhead appliance: the Microsoft end-point mapper port: 135; the Steelhead appliance port for Exchange traffic: 7830; the Steelhead appliance port for Exchange Directory Name Service Provider Interface (NSPI) traffic: 7840.

Example

```
amnesiac (config) # in-path rule fixed-target target-addr 10.11.2.25 target-port all dstaddr
192.168.0.0/16 rulenum 1
```

Product

Steelhead appliance, CSH

Related Topics

"in-path rule edit fixed-target," "show in-path," "show in-path rules"

in-path rule edit fixed-target packet-mode-uni

Description

Edits a fixed-target packet-mode optimization rule.

Syntax

in-path rule edit rulenum <rulenum> fixed-target packet-mode-uni target-addr {<IPv4-addr> | <IPv6-addr>} [target-port <port>] [protocol {tcp|udp |any}] [backup-addr {<IPv4-addr> | <IPv6-addr>}] [backup-port <port>] [scraddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}] [scrport <port>] [dstaddr {<IPv4-addr> | IPv6-addr | all-ip |all-ipv4 | all-ipv6}] [dstport <port>] [optimization {normal | sdr-only |sdr-m | compr-only | none}] [vlan <vlan tag ID>] [description <description>]

Parameters

rulenum <rulenum>	Specify the rule number to edit: **1-N** or **start** or **end**.
target-addr {<IPv4-addr> | <IPv6-addr>} target-port <port>	Specify the fixed-target appliance address. For the network address, use the format XXX.XXX.XXX.XXX for IPv4 or X:X:X:X/XXX for IPv6. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
protocol {tcp | udp | any}	Specify a protocol to optimize: • **tcp** - Specify the TCP protocol for TCPv4 and TCPv6 connections. • **udp** - Specify the UDP protocol for UDPv4 and UDPv6 connections**.** • **any** - Specify to optimize all traffic.
backup-addr {<IPv4-addr | IPv6-addr>} backup-port <port>	Specify a backup appliance for this rule (if any). For the network address, use the format XXX.XXX.XXX.XXX for IPv4 or X:X:X:X/XXX for IPv6. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
srcaddr {<IPv4-addr>| <IPv6-addr>| all-ip |all-ipv4 | all-ipv6>}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4 -** All IPv4 addresses • **all-ipv6 -** All IPv6 addresses
srcport <port>	Specify the source port. Packet-mode optimization is unidirectional, and this port is used on the Steelhead appliance to match the source port in return traffic. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
dstaddr {<IPv4-subnet | IPv6-subnet | all-ip |all-ipv4 | all-ipv6>} dstport <port>	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify; • **all-ip** - All IPv4 and all IPv6 addresses • **all-ipv4** - All IPv4 addresses • **all-ipv6**- All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
optimization {normal | sdr-only | sdr-m | compr-only | none}	Specify an optimization policy: • **normal** - The **normal** optimization policy is the default. The normal process performs LZ compression and SDR. • **sdr-only -** Specify this option to turn off LZ compression. • **sdr-m -** Performs data reduction entirely in memory, which prevents the Steelhead appliance from reading and writing to and from the disk. Enabling this option can yield high LAN-side throughput because it eliminates all disk latency. • **compr-only** - Specify this option to turn off SDR but perform LZ compression. • **none -** Specify this option to turn off LZ compression and SDR.
vlan <vlan tag ID>	Specify the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0 through 4094. Specify 0 to mark the link untagged.
description <description>	Specify a description to facilitate network administration.

Usage

Use the **in-path rule edit fixed-target packet-mode-uni** command to edit a fixed-target packet-mode optimization rule. Use the **show flows** command to display packet-mode optimization flow information.

Example

```
amnesiac (config) # in-path rule edit rulenum 1 fixed-target packet-mode-uni target-addr 10.0.0.1/
24 protocol udp optimization sdr-only
```

Product

Steelhead appliance

Related Topics

"in-path rule fixed-target packet-mode-uni," "packet-mode enable," "show flows,""show in-path," "show in-path rules"

in-path rule fixed-target packet-mode-uni

Description

Adds a fixed-target packet-mode optimization rule.

Syntax

[no] in-path rule fixed-target packet-mode-uni target-addr {<IPv4-addr> | <IPv6-addr>} [target-port <port>] [protocol {tcp|udp | any}] [backup-addr {<IPv4-addr> | <IPv6-addr>} [backup-port <port>]] [scraddr {<IPv4-addr>| <IPv6-addr>| all-ip |all-ipv4 | all-ipv6>}] [scrport <port>] [dstaddr {<IPv4-addr>| <IPv6-addr>| all-ip |all-ipv4 | all-ipv6>}] [dstport <port>] [optimization {normal | sdr-only |sdr-m | compr-only | none}] [vlan <vlan tag ID>] [description <description>] [rule-enable {true | false}] [rulenum <rulenum>]

Parameters

target-addr {<IPv4-addr> | IPv6-addr>} target-port <port>	Specify the fixed-target appliance address. For the network address, use the format XXX.XXX.XXX.XXX for IPv4 or X:X:X:X/XXX for IPv6. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
protocol {tcp | udp |any}	Specify a protocol to optimize: • **tcp** - Specify TCP for TCPv4 and TCPv6 connections. • **udp** - Specify UDP for UDPv4 and UDPv6 connections. • **any** - Specify to optimize all traffic.
backup-addr {<IPv4-addr> | <IPv6-addr>} backup-port <port>	Specify a backup appliance IP address for this rule (if any). For the network address, use the format XXX.XXX.XXX.XXX for IPv4 or X:X:X:X/XXX for IPv6. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
srcaddr {<IPv4-addr>| IPv6-addr| all-ip |all-ipv4 | all-ipv6>}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify; • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6**- All IPv6 addresses
srcport <port>	Specify the source port. Packet-mode optimization is unidirectional, and this port is used on the Steelhead appliance to match the source port in return traffic. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
dstaddr {<IPv4-addr>| IPv6-subnet | all-ip |all-ipv4 | all-ipv6>} dstport <port>	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify; • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6**- All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
optimization {normal | sdr-only | sdr-m | compr-only | none}	Specify an optimization policy: • **normal** - The **normal** optimization policy is the default. The normal process performs LZ compression and SDR. • **sdr-only -** Specify this option to turn off LZ compression. • **sdr-m -** Performs data reduction entirely in memory, which prevents the Steelhead appliance from reading and writing to and from the disk. Enabling this option can yield high LAN-side throughput because it eliminates all disk latency. • **compr-only** - Specify this option to turn off SDR but perform LZ compression. • **none -** Specify this option to turn off LZ compression and SDR.
vlan <vlan tag ID>	Specify the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0 through 4094. Specify 0 to mark the link untagged.
description <description>	Specify a description to facilitate network administration.

rule-enable {true | false}	Specify to enable or disable a fixed-target packet-mode optimization rule.
rulenum <rulenum>	Specify the rule number to edit: **1-N** or **start** or **end**.

Usage

Packet-mode optimization skips the auto-discovery process and uses a specified remote Steelhead appliance as an optimization peer to perform bandwidth optimization on TCPv4, TCPv6, UDPv4, or UDPv6 connections. Packet-mode optimization rules support both physical in-path and master/backup Steelhead configurations.

When you create a fixed-target packet-mode optimization rule, you define the inner channel characteristics using the following controls: source and destination subnet and source destination port or port labels.

You must specify which TCPv4, TCPv6, UDPv4, or UDPv6 connections need optimization, at least one remote target Steelhead appliance, and, optionally, which ports and backup Steelhead appliances to use. For IPv6 traffic, you must enable IPv6 on base interfaces (IPv6 is enabled by default).

The packet-mode optimization rule does not take effect until packet-mode optimization is enabled. Use the **packet-mode enable** command to enable packet-mode optimization.

Use the **show flows** command to display information about packet-mode optimization flows.

Example

```
amnesiac (config) # in-path rule fixed-target packet-mode-uni target-addr 10.0.0.1/24 protocol udp
optimization sdr-only rulenum 1
```

Product

Steelhead appliance

Related Topics

“in-path rule edit fixed-target packet-mode-uni,” “packet-mode enable,” “show flows,”“show in-path,” “show in-path rules”

in-path rule edit pass-through

Description

Edits a pass-through in-path rule.

Syntax

[no] in-path rule edit rulenum <rulenum> pass-through [scraddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}] [srcport <port>] [dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}] [dstport <port>] [protocol {tcp | udp |any}] [vlan <vlan tag ID>] [description <description>] [rule-enable {true | false}]

Parameters

rulenum <rulenum>	Specify the rule number to edit: **1-N** or **start** or **end**.
srcaddr {<IPv4-addr>| IPv6-addr| all-ip |all-ipv4 | all-ipv6>} **srcport <port>**	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
dstaddr {<IPv4-addr>| IPv6-addr| all-ip |all-ipv4 | all-ipv6>} **dstport <port>**	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6**- All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
protocol {tcp | udp |any}	Specify the protocol traffic to pass through: • **tcp** - Specify TCP to pass through TCPv4 and TCPv6 traffic. • **udp** - Specify UDP to pass through UDPv4 and UDPv6 traffic. • **any** - Specify to pass through all TCP and UDP traffic.
vlan <vlan tag ID>	Specify the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0-4094. Specify **0** to mark the link untagged.
description <description>	Specify a description to facilitate communication about network administration.
rule-enable {true | false}	Specify to enable or disable a pass-through in-path rule.

Usage

Use the **in-path rule pass-through** command to add a pass-through in-path rule.

Example

```
amnesiac (config) # in-path rule edit rulenum 25 pass-through srcaddr 10.10.10.1
```

Product

Steelhead appliance, CSH

Related Topics

"in-path rule pass-through," "show in-path," "show in-path rules"

in-path rule move

Description

Moves an in-path rule in the rule list to the specified position.

Syntax

in-path rule move rulenum <rulenum> to <rulenum>

Parameters

<rulenum>	Specify the rule number or **start** or **end**.

Example

```
amnesiac (config) # in-path rule move rulenum 25 to 10
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path rules"

in-path rule pass-through

Description

Adds a pass-through in-path rule.

Syntax

[no] in-path rule pass-through [scraddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}] [srcport <port>] [dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}] [dstport <port>] [protocol {tcp | udp | any}] [vlan <vlan tag ID>] [saas_action <mode>] [description <description>] [rule-enable {true | false}] [rulenum <rulenum>]

Parameters

srcaddr {<IPv4-addr>| IPv6-addr| all-ip |all-ipv4 | all-ipv6>} **srcport <port>**	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
dstaddr {<IPv4-addr>| IPv6-addr| all-ip |all-ipv4 | all-ipv6>} **dstport <port>**	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6**- All IPv6 addresses For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
protocol {tcp | udp |any}	Specify the protocol traffic to pass through: • **tcp** - Specify TCP to pass through TCPv4 and TCPv6 traffic. • **udp** - Specify UDP to pass through UDPv4 and UDPv6 traffic. • **any** - Specify to pass through all TCP and UDP traffic.
vlan <vlan tag ID>	Specify the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0-4094. Specify **0** to mark the link untagged.
saas_action <mode>	Specify a SaaS action mode for this rule. After you subscribe to a SaaS platform and enable it, ensure that cloud acceleration is ready and enabled. If cloud acceleration is enabled, then by default, connections to the subscribed SaaS platform will be optimized by the SCA. You do not need to add an in-path rule unless you want to optimize specific users and not others. Then, select one of these modes: • **auto** - If the in-path rule matches, the connection is optimized by the SCA connection. • **passthru** - If the in-path rule matches, the connection is not optimized by the SCA, but it follows the rule's other parameters so that the connection might be optimized by this Steelhead appliance with other Steelhead appliances in the network, or it might be passed through.
description <description>	Specify a description to facilitate communication about network administration.
rule-enable {true | false}	Specify to enable or disable
rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**. The rule is inserted into the list at the specified position. For example, if you specify **rulenum** as 3, the new rule will be **3**, the old rule **3** will become **4**, and subsequent rules will also move down the list. Specify **start** for the rule to be the first rule and **end** for the rule to be the last rule. If you do not specify a rule number, the rule is added to the end of the list.

Usage

The Steelhead appliance automatically intercepts traffic on all IP addresses (**0.0.0.0**) and ports (**all**) and optimizes according to default settings.

Specify pass-through rules for traffic that you want to pass through to its destination without optimization by the Riverbed system.

This pass-through rule allows the SYN packet to pass through the Steelhead appliance unoptimized. No optimization is performed on the TCP connection initiated by this SYN packet. You define pass-through rules to exclude subnets from optimization. Traffic is also passed through when the Steelhead appliance is in bypass mode. (Pass through of traffic might occur because of in-path rules or because the connection was established before the Steelhead appliance was put in place or before the Steelhead service was enabled.)

The **no** command option disables the rule. The **no** command option has the following syntax:

no in-path rule <rulenum>.

Example

```
amnesiac (config) # in-path rule pass-through srcaddr 10.10.10.1 rulenum 25
```

Product

Steelhead appliance, CSH

Related Topics

"in-path rule edit pass-through," "show in-path," "show in-path rules"

ip in-path-gateway

Description

Configures the default gateway for the in-path interface.

Syntax

[no] ip in-path-gateway <interface> <destination addr>

Parameters

<interface>	Specify the interface name. For example, **in-path0_0**, **in-path1_1**
<destination addr>	Specify the destination IP address of the in-path gateway.

Usage

This command is used to set the default gateway for a particular bypass pair, for in-path optimization configurations.

in-pathX_X represents the bypass pair. Examples are **in-path0_0**, **in-path1_0**, and **in-path1_1**. For the in-path interfaces, this command should be used to set the default gateway.

The **no** command option disables the default gateway.

Example

```
amnesiac (config) # ip in-path-gateway in-path0_0 10.0.0.1
```

Product

Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show in-path"

ip in-path route

Description

Adds a static in-path route.

Syntax

[no] ip in-path route <interface> <network prefix> <network mask> <next hop IP address or WAN gateway>>

Parameters

<interface>	Specify the interface name: **aux**, **lan0_0**, **wan0_0**, **primary**, **in-path0_0**
<network prefix>	Specify the network prefix.
<network mask>	Specify the netmask.
<next hop IP address or WAN gateway>	Specify the next hop IP address in this route or WAN gateway.

Usage

In-path interfaces use routes from an in-path route table. To configure in-path routes, you set a new in-path route that points to your WAN gateway. You must also copy any static routes that you have added to the main table, if they apply to the in-path interface.

The **no** command option removes an in-path route.

Example

```
amnesiac (config) # ip in-path route inpath0_0 190.160.0.0 255.255.0.0 193.162.0.0
```

Product

Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show ip default-gateway"

Management In-Path Interface Commands

This section describes the Management In-Path Interface (MIP) commands. For details, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

in-path interface mgmt-interface enable

Description

Enables a management in-path (MIP) interface.

Syntax

[no] in-path interface <interface> mgmt-interface enable

Parameters

<interface>	Specify the MIP interface. For example, inpath0_0.

Usage

In a typical in-path deployment, optimized and pass-through traffic flows through the Steelhead appliance LAN and WAN interfaces and Riverbed network management traffic flows through the auxiliary interface. You can also use the auxiliary interface to connect the appliance to a non-Riverbed network management device. Some deployments do not allow access to the auxiliary management interface when plugged into a private subnet with a separate IP address space. In this type of deployment you cannot use the auxiliary interface to manage the Steelhead appliance.

RiOS v6.1 provides a way to configure a secondary MIP interface that you can reach through the physical in-path LAN and WAN interfaces. Configuring a secondary MIP interface is a way to manage Steelhead appliances from a private network while maintaining a logical separation of network traffic. This configuration eliminates the need to deploy a switch or borrow a switchport. You can configure one MIP interface for each LAN and WAN interface pair.

A MIP interface is accessible from both the LAN and WAN side and you can reach it even when:

- the primary interface is unavailable.
- the optimization service is not running.

- the (logical) in-path interface fails.

A MIP interface is not accessible if the (physical) LAN and WAN interfaces fail.

For details, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

Note: You cannot reach a MIP interface when Link State Propagation (LSP) is also enabled and the corresponding in-path interface fails. In physical in-path deployments, LSP shortens the recovery time of a link failure. LSP communicates link status between the devices connected to the Steelhead appliance and is enabled by default in RiOS v6.0 and later.

The **no** command option disables the management in-path (MIP) interface.

Note: This command requires you to also configure "in-path interface mgmt-interface ip" and "in-path interface mgmt-interface vlan".

Example

```
amnesiac (config) # in-path interface inpath0_0 mgmt-interface enable
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"in-path interface mgmt-interface ip", "in-path interface mgmt-interface vlan," "show in-path mgmt-interface"

in-path interface mgmt-interface ip

Description

Specifies the static IP address and network mask for the management in-path (MIP) interface.

Syntax

[no] in-path interface <interface> mgmt-interface ip <ip-addr>

Parameters

<interface>	Specify the MIP interface. For example, inpath0_0.
<ip-addr>	Specify the IP address for the MIP interface.

Usage

The MIP interface must reside in its own subnet and cannot share the same subnet with any other interfaces on the Steelhead appliance.

For details, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

The **no** command option disables in-path support.

Note: This command requires you to also configure "in-path interface vlan" and "in-path interface mgmt-interface vlan".

Example

```
amnesiac (config) # in-path interface inpath0_0 mgmt-interface ip 90.55.0.1
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"in-path interface vlan," "in-path interface mgmt-interface vlan," "show in-path mgmt-interface"

in-path interface mgmt-interface vlan

Description

Specifies the VLAN ID for the management in-path (MIP) interface.

Syntax

[no] in-path interface <interface> mgmt-interface vlan <vlan>

Parameters

<interface>	Specify the MIP interface. For example, inpath0_0.
<vlan>	Specify a numeric VLAN Tag ID. When you specify the VLAN tag ID for the MIP interface, all packets originating from the Steelhead appliance are tagged with that identification number. Specify the VLAN tag that the appliance uses to communicate with other Steelhead appliances in your network. The VLAN Tag ID might be the same value or a different value than the in-path interface VLAN tag ID. The MIP interface could be un-tagged and in-path interface could be tagged and vice versa. A zero (0) value specifies non-tagged (or native VLAN) and is the correct setting if there are no VLANs present. For example, if the MIP interface is 192.168.1.1 in VLAN 200, you would specify tag 200.

Usage

For details, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

The **no** command option resets the MIP VLAN.

Note: This command requires you to also configure "in-path interface vlan" and "in-path interface mgmt-interface ip".

Example

```
amnesiac (config) # in-path interface inpath0_0 mgmt-interface vlan 26
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"in-path interface mgmt-interface ip", "show in-path mgmt-interface", "in-path interface vlan"

WAN Visibility (Transparency) Commands

This section describes WAN Visibility commands.

For details about WAN Visibility and configuring WAN transparency, see the *Steelhead Appliance Deployment Guide*.

in-path mac-match-vlan

Description

Enables VLAN IDs to be used in simplified routing table look-ups for WAN visibility.

Syntax

[no] in-path mac-match-vlan

Parameters

None

Usage

VLAN transparency configuration requires:

- "in-path rule auto-discover," (configure the WAN visibility mode)
- "in-path peering auto"
- "in-path probe-caching enable" (set to **no**)
- "in-path vlan-conn-based"

- "in-path mac-match-vlan"
- "in-path probe-ftp-data"
- "in-path simplified routing"
- "steelhead communication fwd-vlan-mac" (only necessary for VLAN transparent networks with neighbor Steelhead appliances)

For details, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables.

Example

```
amnesiac (config) # in-path mac-match-vlan
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show in-path probe-caching," "in-path rule auto-discover," "show in-path peering oobtransparency"

in-path multi-path maintain

Description

Maintains the multi-path properties of the connection in transparency deployments.

Syntax

[no] in-path multi-path maintain

Parameters

None

Usage

Use this command when you are configuring VLAN transparency and asymmetric routing, when you want to maintain the asymmetric flow of data (instead of having the server-side Steelhead appliance use the in-path interface that on which it first saw an incoming probe. For details about VLAN transparency, see the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # in-path multi-path maintain
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show in-path probe-caching,""in-path rule auto-discover," "show in-path peering oobtransparency"

in-path peering oobtransparency mode

Description

Enables out-of-band (OOB) connection destination transparency. The OOB connection is a single, unique TCP connection that is established by a pair of Steelhead appliances that are optimizing traffic. The pair of Steelhead appliances use this connection strictly to communicate internal information required by them to optimize traffic.

For details about WAN visibility, see "in-path rule auto-discover" on page 323 and the *Steelhead Appliance Deployment Guide*.

Syntax

[no] in-path peering oobtransparency mode [none | destination | full] | [port <port>]

Parameters

[none | destination | full]	Enables OOB mode. Specify one of the following options: • **none** - Specify correct addressing. The OOB connection is established between the two Steelhead appliances, without any TCP/IP header manipulation. This is the default setting. • **destination** - Specify destination mode. In this mode, the OOB connection has the form C-SHip:C-SHport<->Sip:Sport, where C-SHip is the client-side Steelhead appliance IP address, C-SHport is an ephemeral port chosen by C-SH, Sip is the server IP address, and Sport is the server port number. The Sip and Sport parameters are taken from the first connection optimized by the pair of Steelhead appliances. • **full** - Specify full mode. In this mode, the OOB connection has the form Cip:C-SHfixed<->Sip:Sport, where Cip is the client IP address, C-SHfixed is a pre-determined port chosen by the client-side Steelhead appliance, Sip is the server IP address, and Sport is the server port number. The Cip, Sip, and Sport parameters are taken from the first connection optimized by the pair of Steelhead appliances.
[port <port>]	Changes the pre-determined port in **full** mode (C-SHfixed). The default value is 708.

Usage

With RiOS v5.0.x or later, and if you use WAN visibility full address transparency, you have the following transparency options for the OOB connection: OOB connection destination transparency and OOB connection full transparency.

You configure OOB transparent addressing on the client-side Steelhead appliance (where the connection is initiated). By default, the OOB connection uses correct addressing. Correct addressing uses the client-side Steelhead appliance IP address, port number, and VLAN ID, and the server-side Steelhead appliance IP address, port number, and VLAN ID.

If you are using OOB connection correct addressing and the client-side Steelhead appliance cannot establish the OOB connection to the server-side Steelhead appliance, OOB connection transparency can resolve this issue. For example, if you have a server on a private network that is located behind a NAT device. You configure OOB connection transparency so that the client-side Steelhead appliance uses the server IP address and port number as the remote IP address and port number. Steelhead appliances route packets on the OOB connection to the NAT device. The NAT device then translates the packet address to that of the server-side Steelhead appliance.

If both of the OOB connection transparency options are acceptable solutions, OOB connection destination transparency is preferable. OOB connection destination transparency mitigates the slight possibility of port number collisions which can occur with OOB connection full transparency.

When OOB connection transparency is enabled and the OOB connection is lost, the Steelhead appliances re-establish the connection using the server IP address and port number from the next optimized connection.

OOB connection destination transparency uses the client-side Steelhead appliance IP address and an ephemeral port number chosen by the client-side Steelhead appliance, plus the server IP address and port number in the TCP/IP packet headers in both directions across the WAN

Steelhead appliances use the server IP address and port number from the first optimized connection.

Use OOB connection destination transparency if the client-side Steelhead appliance cannot establish the OOB connection to the server-side Steelhead appliance.

For details about configuring in-path IP addresses and OOB connections for WAN visibility, see the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # in-path peering oobtransparency mode none
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show in-path probe-caching,""in-path rule auto-discover," "show in-path peering oobtransparency"

in-path probe-caching enable

Description

Enable probe caching for WAN visibility. By default, probe caching is disabled in RiOS v5.5 and later.

Syntax

[no] in-path probe-caching enable

Parameters

None

Usage

With probe caching, the client-side Steelhead appliance caches the auto-discovery probe response from the server-side Steelhead appliance when trying to reach a specific server. On subsequent attempts to reach the same server, the Steelhead appliance uses the already cached probe response. On those attempts, the client-side Steelhead appliance sets up a session directly to the peer Steelhead appliance within the 7800 inner channel, bypassing the auto-discovery process since it was successful with the previous attempt. By default, probes are cached for 10 seconds.

With probe caching enabled, Steelhead appliances still perform auto-discovery. Probe caching simply saves some steps during auto-discovery if you are going to the same destination host. With probe caching disabled, every new TCP session performs auto-discovery, instead of just some of the new TCP sessions.

To determine if probe-caching is enabled on the Steelhead in RiOS v5.x and later

```
show in-path probe-caching
Probe Caching Enabled: yes
```

To disable probe-caching in RiOS v5.x and later

```
no in-path probe-caching enable
```

Note: By default, probe caching is disabled in RiOS v5.5 and later.

When the server-side Steelhead appliance is on a VLAN trunk and simplified routing is enabled, Riverbed recommends disabling probe caching on all the remote Steelhead appliances. This is because the connection request inside the 7800 inner channel might not have the correct VLAN ID. Because the request arrived on the inner channel, the VLAN ID in the request would be same as the Steelhead appliance in-path VLAN. If the server is on a different VLAN than the Steelhead appliance, the request will not have the correct VLAN ID and there is no easy way to determine it. With probe caching disabled, the Steelhead appliance will always get the SYN with original client and server IP addresses and the router adds the correct VLAN. You only need to disable probe caching on client-side Steelhead appliances.

If you have multiple Steelhead appliances connected with WCCP, you might see many forwarded connections and a larger than expected amount of data sent in the Neighbor Statistics report. (You configure neighbors when you enable connection forwarding.)

The probe caching mechanism allows some sessions to get established on the *wrong* Steelhead appliance. Disabling this mechanism ensures the routers have a chance to redirect every SYN packet to the correct Steelhead appliance, preventing connection forwarding from occurring.

To avoid incorrect forwarded connections, disable probe caching on the client-side Steelhead appliance.

For details, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables probe caching.

Example

```
amnesiac (config) # in-path probe-caching enable
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show in-path probe-caching,""in-path rule auto-discover," "show in-path peering oobtransparency"

in-path probe-ftp-data

Description

Probes FTP data connections to learn VLAN information. Enables full address transparency for WAN visibility. For details, see the *Steelhead Appliance Deployment Guide*.

Syntax

[no] in-path probe-ftp-data

Parameters

None

Usage

The **no** command option disables this command.

Example

```
amnesiac (config) # in-path probe-ftp-data
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show in-path probe-ftp-data," "in-path rule auto-discover,""show in-path peering oobtransparency"

in-path probe-mapi-data

Description

Probes MAPI connections. Enables full address transparency for WAN visibility. For details, see the *Steelhead Appliance Deployment Guide*.

Syntax

[no] in-path probe-mapi-data

Parameters

None

Usage

The **no** command option disables this command.

Example

The following example configures full-address transparency for a VLAN.

```
amnesiac (config) # in-path peering auto
amnesiac (config) # in-path vlan-conn-based
amnesiac (config) # in-path mac-match-vlan
amnesiac (config) # no in-path probe-caching enable
amnesiac (config) # in-path probe-ftp-data
amnesiac (config) # in-path probe-mapi-data
amnesiac (config) # write memory
amnesiac (config) # service restart
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"in-path rule auto-discover," "show in-path peering oobtransparency," "show in-path probe-caching," "show in-path probe-mapi-data"

in-path vlan-conn-based

Description

Enables VLAN connection based mapping for WAN visibility. For details, see the *Steelhead Appliance Deployment Guide*.

Syntax

[no] in-path vlan-conn-based

Parameters

None

Usage

This command learns and uses the correct connection for the VLAN.

The **no** command option disables VLAN connection based mapping.

Example

```
amnesiac (config) # in-path vlan-conn-based
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show in-path vlan-conn-based,""show in-path probe-caching,""in-path rule auto-discover," "show in-path peering oobtransparency"

Out-of-Path Support

This section describes the out-of-path support command.

out-of-path enable

Description

Enables an out-of-path configuration.

Syntax

[no] out-of-path enable

Parameters

None

Usage

For details, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

The **no** command option disables out-of-path configuration.

Example

```
amnesiac (config) # out-of-path enable
```

Product

Steelhead appliance, CSH

Related Topics

"show out-of-path"

Connection Pooling Commands

This section describes the connection pooling commands.

service connection pooling

Description

Enables a pool of connections to a peer Steelhead appliance.

Syntax

[no] service connection pooling <max-pool-size>

Parameters

<max-pool-size>	Specify the maximum connection pooling size.

Usage

Connection pooling enables you to save an extra round-trip for the initial connection setup. Connection pooling is useful for protocols that open a number of short lived connections, such as HTTP.

Any change in the connection pooling parameter requires you to restart the Steelhead service.

The **no** command option disables connection pooling.

Example

```
amnesiac (config) # service connection pooling 20
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show service connection pooling"

Failover Support and Out-of-Band Failure Detection Commands

This section describes the failover support and out-of-band failure detection commands.

failover connection

Description

Sets failover connection settings.

Syntax

[no] failover connection {attempts <attempts> | failed <timeout> | timeout <timeout>}

Parameters

attempts <attempts>	Sets the number of times the backup Steelhead appliance attempts to reconnect to the master Steelhead appliance after a read time-out has expired. The default value is five attempts.
failed <timeout>	Sets the connection failed timeout setting.
timeout <timeout>	Sets the number of milliseconds the Steelhead appliance waits before aborting the reconnection attempt to the master Steelhead appliance. The default value is 2000 ms.

Usage

You can adjust the timers for faster master appliance and backup appliance failover. In a steady, normal operating state, the backup Steelhead appliance periodically sends keep-alive messages to the master Steelhead appliance on TCP port 7820. If the master Steelhead appliance does not respond to the keep-alive message within five seconds, the backup Steelhead appliance drops the connection and attempts to reconnect to the master Steelhead appliance. The backup Steelhead appliance attempts to reconnect a maximum of five times, and each time it waits for two seconds before aborting the connection.

If all connection attempts fail, the backup Steelhead appliance transitions into an active state and starts optimizing the connections. If you use the default value failover settings, it can take as long as 15 seconds before the backup Steelhead appliance starts optimizing connections.

Use the **failover connection** command to adjust the number of times the backup Steelhead appliance attempts to reconnect to the master Steelhead appliance after a read time-out has expired. You can adjust the read time-out value by using the **failover read timeout** command.

The **no** command option resets the failover connection settings to the default values.

Example

```
amnesiac (config) # failover connection timeout 1000
amnesiac (config) # failover connection attempts 4
```

Product

Steelhead appliance

Related Topics

"failover read timeout,""show failover"

failover enable

Description

Enables a failover appliance. A failover appliance is a backup appliance. If the master fails, the failover appliance takes over.

Syntax

[no] failover enable

Parameters

None

Usage

For a physical in-path failover deployment, you configure a pair of Steelhead appliances: one as a master and the other as a backup. The master Steelhead appliance in the pair (usually the Steelhead appliance closest to the LAN) is active and the backup Steelhead appliance is passive. The master Steelhead appliance is active unless it fails for some reason. The backup is passive while the master is active and becomes active if either the master fails or the master reaches its connection limit and enters *admission control* status. A backup Steelhead appliance does not intercept traffic while the master appliance is active. It **ping**s the master Steelhead appliance to make sure that it is alive and processing data. If the master Steelhead appliance fails, the backup takes over and starts processing all of the connections. When the master Steelhead appliance comes back up, it sends a message to the backup that it has recovered. The backup Steelhead appliance stops processing new connections (but continues to serve old ones until they end).

For an out-of-path failover deployment, you deploy two server-side Steelhead appliances and add a fixed-target rule to the client-side Steelhead appliance to define the master and backup target appliances. When both the master and backup Steelhead appliances are functioning properly, the connections traverse the master appliance. If the master Steelhead appliance fails, subsequent connections traverse the backup Steelhead appliance.

The master Steelhead appliance uses an Out-of-Band (OOB) connection. The OOB connection is a single, unique TCP connection that communicates internal information. If the master Steelhead appliance becomes unavailable, it loses this OOB connection and the OOB connection times out in approximately 40-45 seconds. Once the OOB connection times out, the client-side Steelhead appliance declares the master Steelhead appliance unavailable and connects to the backup Steelhead appliance.

During the 40-45 second delay before the client-side Steelhead appliance declares a peer unavailable, it passes through any incoming new connections; they are not black-holed.

While the client-side Steelhead appliance is using the backup Steelhead appliance for optimization, it attempts to connect to the master Steelhead appliance every 30 seconds. If the connection succeeds, the client-side Steelhead appliance reconnects to the master Steelhead appliance for any new connections. Existing connections remain on the backup Steelhead appliance for their duration. This is the only time, immediately after a recovery from a master failure, that connections are optimized by both the master Steelhead appliance and the backup.

If both the master and backup Steelhead appliances become unreachable, the client-side Steelhead appliance tries to connect to both appliances every 30 seconds. Any new connections are passed through the network unoptimized.

In addition to enabling failover and configuring buddy peering, you must synchronize the data stores for the master-backup pairs to ensure optimal use of SDR for *warm* data transfer. With warm transfers, only new or modified data is sent, dramatically increasing the rate of data transfer over the WAN.

The **no** command option disables failover.

Example

```
amnesiac (config) # failover enable
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show failover"

failover master

Description

Sets the appliance as the master appliance of a failover pair. If the master fails, traffic is routed automatically through the failover appliance.

Syntax

[no] failover master

Parameters

None

Usage

You must specify valid values for the failover appliance IP address and failover appliance port.

The **no** command option sets the appliance as the failover buddy.

Example

```
amnesiac (config) # failover master
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show failover"

failover port

Description

Sets the port on the master appliance with which to communicate with the failover appliance. A failover appliance is a backup appliance. If the master fails, the failover appliance takes over.

Syntax

[no] failover port <port>

Parameters

<port>	Specify the port number.

Usage

The default value is 7820.

The **no** command option resets the port to the default value.

Example

```
amnesiac (config) # failover port 2515
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show failover"

failover read timeout

Description

Specifies the failover read settings.

Syntax

[no] failover read timeout <timeout>

Parameters

<timeout>	Specifies the failover read time-out value, in milliseconds. The default value is 5000 milliseconds.

Usage

You can adjust the timers for faster master and backup failover for Steelhead appliances. In a steady, normal operating state, the backup Steelhead appliance periodically sends keep-alive messages to the master Steelhead appliance on TCP port 7820. If the master Steelhead appliance does not respond to the keep-alive message within five seconds, the backup Steelhead appliance drops the connection and attempts to reconnect to the master Steelhead appliance. The backup Steelhead appliance attempts to reconnect a maximum of five times, and each time it waits for two seconds before aborting the connection.

If all connection attempts fail, the backup Steelhead appliance transitions into an active state and starts optimizing the connections. If you use the default value failover settings, it can take as long as 15 seconds before the backup Steelhead appliance starts optimizing connections.

Use the **failover read timeout** command to adjust the amount of time, in milliseconds, that the backup Steelhead appliance waits for the master Steelhead appliance to respond to its keep-alive messages.

The **no** command option resets the failover read settings to the default value.

Example

```
amnesiac (config) # failover read timeout 1000
```

Product

Steelhead appliance

Related Topics

"show failover"

failover steelhead addr

Description

Sets the IP address for a failover Steelhead appliance. A failover Steelhead appliance is a backup appliance. If the master fails, the failover appliance takes over.

Syntax

[no] failover steelhead addr <addr>

Parameters

<addr>	Specify the IP address for the failover, backup machine. The default value is 0.0.0.0. If you have installed multiple bypass cards, you must specify the IP address for the inpath0_0 slot.

Usage

The default value is 0.0.0.0.

The **no** command option resets the failover IP address to the default value.

Example

```
amnesiac (config) # failover steelhead addr 10.10.10.1
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show failover"

failover steelhead port

Description

Sets the port for a failover Steelhead appliance. A failover Steelhead appliance is a backup appliance. If the master fails, the failover appliance takes over.

Syntax

[no] failover steelhead port <port>

Parameters

<port>	Specify the port number.

Usage

The default value is 7820.

You cannot specify the failover steelhead port for the Interceptor appliance.

The **no** command option resets the port to the default value.

Example

```
amnesiac (config) # failover steelhead port 2515
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show failover"

protocol connection lan on-oob-timeout

Description

Configures out-of-band LAN timeout settings.

Syntax

[no] protocol connection lan on-oob-timeout {drop all | drop same-inpath enable}

Parameters

drop all	Configure OOB connection shutdown on loss of connection.
drop same-inpath enable	Configure on OOB connection shutdown on in-path loss of connection.

Usage

Losing the OOB connection does not affect the optimized sessions, because the optimized sessions have a one-to-one mapping between the outer channel (the LAN-side TCP connection between the client and server, and the Steelhead appliance) and the inner channel (the WAN-side TCP connection between the Steelhead appliances). The disadvantage to this approach is that the application does not notice when the peer is unavailable and the application might appear as if it is not working to the end user.

To address this, you can disconnect the inner and outer channels when the Steelhead appliance loses its OOB connection with the **protocol connection lan on-oob-timeout drop all** command. For Steelhead appliances with multiple in-path interfaces, this command disconnects all the optimized sessions even if there are other OOB connections originating from other in-path interfaces.

To configure the Steelhead appliance to drop only the connections related to a specific in-path interface, use the **protocol connection lan on-oob-timeout drop same-inpath enable** command.

Example

```
amnesiac (config) # protocol connection lan on-oob-timeout drop all

amnesiac (config) # protocol connection lan on-oob-timeout drop same-inpath enable
```

Product

Steelhead appliance

Related Topics

"show protocol connection"

protocol connection wan keep-alive oob def-count

Description

Specifies the out-of-band WAN keep-alive message count.

Syntax

[no] protocol connection wan keep-alive oob def-count <count>

Parameters

<count>	Specify the WAN keep-alive count. The default number of keep-alive messages sent is 2.

Usage

A Steelhead appliance uses the out-of-band (OOB) connection to inform a peer Steelhead appliance of its capabilities. The OOB connection is also used to detect failures. By default, a Steelhead appliance sends a keep-alive message every 20 seconds, and it declares a peer down after sending two keep-alive messages (40 seconds) with no response is received. If you want faster peer failure detection, use the **protocol connection wan keep-alive oob def-count** command to adjust the number of keep-alive messages sent. You can use the **protocol connection wan keep-alive oob def-intvl** command to adjust the interval in which the messages are sent.

Example

```
amnesiac (config) # protocol connection wan keep-alive oob def-count 3
```

Product

Steelhead appliance

Related Topics

"protocol connection wan keep-alive oob def-intvl," "show protocol connection"

protocol connection wan keep-alive oob def-intvl

Description

Specifies the out-of-band WAN keep-alive message interval.

Syntax

[no] protocol connection wan keep-alive oob def-intvl <seconds>

Parameters

<seconds>	Specify the interval in seconds. The default interval is 20 seconds with a minimum of 5 seconds.

Usage

A Steelhead appliance uses the OOB connection to inform a peer Steelhead appliance of its capabilities. The OOB connection is also used to detect failures. By default, a Steelhead appliance sends a keep-alive message every 20 seconds, and it declares a peer down after sending two keep-alive messages (40 seconds) with no response received. You can use the **protocol connection wan keep-alive oob def-intvl** command to adjust the interval in which the messages are sent.

If you want faster peer failure detection, use the **protocol connection wan keep-alive oob def-count** command to adjust the number of keep-alive messages sent.

Example

```
amnesiac (config) # protocol connection wan keep-alive oob def-intvl 10
```

Product

Steelhead appliance

Related Topics

"protocol connection wan keep-alive oob def-count," "show protocol connection"

Packet-Mode Optimization Commands

This section describes the packet-mode optimization commands.

packet-mode enable

Description

Enables packet-mode optimization.

Syntax

[no] packet-mode enable

Parameters

None

Usage

RiOS performs packet-by-packet SDR bandwidth optimization on TCP IPv4, TCP IPv6, UDP IPv4, and UDP IPv6 connections using fixed-target, packet-mode optimization in-path rules. This type of in-path rule optimizes bandwidth for applications over any transport protocol. Use the **in-path rule fixed-target packet-mode-uni** command to specify a packet-mode optimization in-path rule. Use the **show flows** command to view packet-mode flow information.

You must enable packet-mode optimization on both the client-side Steelhead appliance and the server-side Steelhead appliance. Enabling packet-mode optimization requires an optimization service restart.

The **no** command option disables packet-mode optimization.

For details on packet-mode optimization, see the *Steelhead Appliance Deployment Guide* and the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # packet-mode enable
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"in-path rule fixed-target packet-mode-uni," "show flows," "show packet-mode ip-channels," "show packet-mode status"

Peering Commands

This section describes the peering commands. For details about peering, see the Management Console online help and the *Steelhead Appliance Deployment Guide*.

in-path peering auto

Description

Enables enhanced auto-discovery (automatic peering) for serial cascade and serial cluster deployments.

Syntax

[no] in-path peering auto

Parameters

None

Usage

With enhanced auto-discovery the Steelhead appliance automatically finds the furthest Steelhead appliance in a network and optimization occurs there. For example, in a deployment with four Steelhead appliances (A, B, C, D), where D represents the appliance that is furthest from A, the Steelhead appliance automatically finds D. This simplifies configuration and makes your deployment more scalable.

By default, enhanced auto-discovery is enabled. When enhanced auto-discovery is disabled, the Steelhead appliance uses regular auto-discovery. With regular auto-discovery, the Steelhead appliance finds the first remote Steelhead appliance along the connection path of the TCP connection and optimization occurs there. For example, if you had a deployment with four Steelhead appliances (A, B, C, D) where D represents the appliance that is furthest from A, the Steelhead appliance automatically finds B, then C, and finally D and optimization takes place in each.

In some deployments, enhanced auto-discovery can simplify configuration and make your deployments more scalable. For a details about deployments that require enhanced auto-discovery, see the *Steelhead Appliance Deployment Guide*.

RiOS v5.5.x or higher supports a large number of peers (up to 32,768) per Steelhead appliance. This feature is available only on Steelhead appliance models 5520, 6020, 6050, and 6120. After enabling extended peer table support, you must clear the data store and stop and restart the service.

For details about enhanced auto-discovery, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

Preventing an Unknown (or Unwanted) Steelhead Appliance from Peering

Automatic peering (enhanced auto-discovery) greatly reduces the complexities and time it takes to deploy Steelhead appliances. It works so seamlessly that occasionally it has the undesirable effect of peering with Steelheads on the Internet that are not in your organization's management domain or your corporate business unit. When an unknown (or unwanted) Steelhead appliance appears connected to your network, you can create a peering rule to prevent it from peering and remove it from your list of connected appliances. The peering rule defines what to do when a Steelhead appliance receives an auto-discovery probe from the unknown Steelhead appliance. To prevent an unknown Steelhead appliance from peering you must add a pass-through peering rule that passes through traffic from the unknown Steelhead appliance in the remote location. For details, see the Management Console online help and the *Steelhead Appliance Deployment Guide*.

The **no** command option disables enhanced auto-discovery.

Example

```
amnesiac (config) # in-path peering auto
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path peering rules"

in-path peering disc-outer-acpt

Description

Discovers the outer connection for accept rules.

Syntax

[no] in-path peering disc-outer-acpt

Parameters

None

Usage

Alters the discovery protocol when you are doing double interception, VLAN transparency, and asymmetric VLANs.

The **no** command option disables discovery of the outer connection.

Example

```
amnesiac (config) # in-path peering disc-outer-acpt
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path peering disc-outer-acpt"

in-path peering edit-rule

Description

Modifies an in-path peering rule description.

Syntax

in-path peering edit-rule rulenum <number> description <description>

Parameters

rulenum <number>	Specify the rule number.
description <description>	Specify a description to help you identify the rule. Enclosed the text in quotation marks (“).

Example

```
amnesiac (config) # in-path peering edit-rule rulenum 5 description “this is an example”
```

Product

Steelhead appliance, CSH

Related Topics

“show in-path peering disc-outer-acpt”

in-path peering move-rule

Description

Moves the rule to the specified position in the rule list.

Syntax

[no] in-path peering move-rule <rulenum> to <rulenum>

Parameters

<rulenum>	Specify the rule number.

Usage

Rules in the rule list are consulted from first to last. Use this command to reorder an in-path peering rule in the rule list. The **no** command option disables the rule.

Example

```
amnesiac (config) # in-path peering move-rule 3 to 1
```

Product

Steelhead appliance, CSH

Related Topics

“show in-path peering auto”

in-path peering rule

Description

Configures in-path peering rules.

Syntax

[no] in-path peering rule {auto | pass | accept} | [peer <peer ip-addr>]| [ssl-capability cap | in-cap | no-check] | [src {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}] | [dest {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}| dest-port <port>] | [rulenum <rulenum>] | [description <description>]

Parameters

auto | pass | accept	Specify one of the following rules: • **auto** - Automatically determines the response for peering requests (performs the best peering possible). • **pass** - Allows pass-through peering requests that match the source and destination port pattern. • **accept** - Accepts peering requests that match the source-destination-port pattern.
peer <peer ip-addr>	Specify the in-path IP address of the probing Steelhead appliance. If more than one in-path interface is present on the probing Steelhead appliance, apply multiple peering rules, one for each in-path interface. The peer client-side Steelhead appliance IP address is IPv4 only.
ssl-capability [cap | in-cap | no-check]	Specify one of the following options to determine how to process attempts to create secure SSL connections: • **cap (capable)** - The peering rule checks whether the server-side Steelhead appliance is present for the particular destination IP address and port combination. If the destination IP address and port are of an SSL server that is properly configured and enabled on the server-side Steelhead appliance, and if there is no temporary or short-lived error condition, the SSL-capable check is a success. The Steelhead appliance accepts the condition and, assuming all other proper configurations and that the peering rule is the best match for the incoming connection, optimizes SSL. The default peering rule with the SSL capable flag matches those connections to the destination IP/port combination for which there is an SSL server configuration added. The Steelhead appliance considers the SSL server a match even if it is defined on a port number that is not the standard port 443. For all connections that match, the Steelhead appliance performs both auto-discovery and SSL optimization. • **incap (incapable)** - If the destination IP address and port are not an SSL server that is properly configured and enabled on the server-side Steelhead appliance, or if there is a temporary or short-lived error condition, the SSL-capable check fails. The Steelhead appliance passes the connection through unoptimized without affecting connection counts. The default peering rule with the SSL incap flag matches any SSL connection to port 443 for which there is no SSL server configuration on the Steelhead appliance. • **no-check** - The peering rule does not determine whether the server Steelhead appliance is present for the particular destination IP address and port combination. This default rule catches any connection that did not match the first two default rules. The Steelhead appliance performs auto-discovery and does not optimize SSL. This rule always appears last in the list and you cannot remove it.
src {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}	Specify the source subnet IP address and netmask for this rule. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4 -** All IPv4 addresses • **all-ipv6 -** All IPv6 addresses
dest {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6} **dstport <port>**	Specify the destination subnet IP address and netmask for this rule. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify; • **all-ip** - All IPv4 and all IPv6 addresses • **all-ipv4** - All IPv4 addresses • **all-ipv6**- All IPv6 addresses
dest-port <port>	Specify the destination port for this rule. You can specify a port label, or **all** for all ports.

rulenum <rulenum>	Specify the rule number. The system evaluates the rules in numerical order starting with rule **1**. If the conditions set in the rule match, then the rule is applied. If the conditions set in the rule do not match, then the rule is not applied and the system moves on to the next rule. For example, if the conditions of rule **1** do not match, rule **2** is consulted. If rule **2** matches the conditions, it is applied, and no further rules are consulted. The type of a matching rule determines which action the Steelhead appliancee takes on the connection.
description <description>	Specify a description to facilitate communication about network administration.

Usage

You can provide increased optimization by deploying two or more Steelhead appliances back-to-back in an in-path configuration to create a serial cluster.

Appliances in a serial cluster process the peering rules you specify in a spill-over fashion. When the maximum number of TCP connections for a Steelhead appliance is reached, that appliance stops intercepting new connections. This allows the next Steelhead appliance in the cluster the opportunity to intercept the new connection, if it has not reached its maximum number of connections. The in-path peering rules and in-path rules tell the Steelhead appliance in a cluster not to intercept connections between themselves.

You configure peering rules that define what to do when a Steelhead appliance receives an auto-discovery probe from another Steelhead appliance.

You can deploy serial clusters on the client or server-side of the network.

Important: For environments that want to optimize MAPI or FTP traffic which require all connections from a client to be optimized by one Steelhead appliance, Riverbed strongly recommends using the master and backup redundancy configuration instead of a serial cluster. For larger environments that require multi-appliance scalability and high availability, Riverbed recommends using the Interceptor appliance to build multi-appliance clusters. For details, see the *Interceptor Appliance Deployment Guide*, and the *Interceptor Appliance User's Guide*.

Notes:

- When you combine two Steelhead appliances that have a bandwidth limit of 20 Mbps each, the serial cluster still has a limit of 20 Mbps.
- If the active Steelhead appliance in the cluster enters a degraded state because the CPU load is too high, it continues to accept new connections.

Preventing an Unknown (or Unwanted) Steelhead Appliance from Peering

To prevent an unknown Steelhead appliance from peering you must add a pass-through peering rule that passes through traffic from the unknown Steelhead appliance in the remote location. For details, see the Management Console online help and the *Steelhead Appliance Deployment Guide*.

Example

This is an example of how to configure a cluster of three in-path appliances in a data center.

```
WAN----SH1----SH2----SH3----LAN

SH1 ip address is 10.0.1.1 on a /16
SH2 ip address is 10.0.1.2 on a /16
SH3 ip address is 10.0.1.3 on a /16
```

In this example, you configure each Steelhead appliance with in-path peering rules to prevent peering with another Steelhead appliance in the cluster, and with in-path rules to not optimize connections originating from other Steelhead appliances in the same cluster.

SH1 configuration:

```
SH1 > enable
SH1 # configure terminal
SH1 (config) # in-path peering rule pass peer 10.0.1.2 rulenum 1
SH1 (config) # in-path peering rule pass peer 10.0.1.3 rulenum 1
SH1 (config) # in-path rule pass-through srcaddr 10.0.1.2/32 rulenum 1
SH1 (config) # in-path rule pass-through srcaddr 10.0.1.3/32 rulenum 1
SH1 (config) # wr mem
```

```
SH1 (config) # show in-path peering rules
Rule  Type   Source Network     Dest Network       Port  Peer Addr
----- ------ ------------------ ------------------ ----- ---------------
    1 pass   *                  *                  *     10.0.1.3
    2 pass   *                  *                  *     10.0.1.2
  def auto   *                  *                  *     *
SH1 (config) # show in-path rules
Rule  Type Source Addr        Dest Addr          Port  Target Addr     Port
----- ---- ------------------ ------------------ ----- --------------- -----
    1 pass 10.0.1.3/32        *                  *     --              --
    2 pass 10.0.1.2/32        *                  *     --              --
  def auto *                  *                  *     --              --
```

SH2 configuration

```
SH2 > enable
SH2 # configure terminal
SH2 (config) # in-path peering rule pass peer 10.0.1.1 rulenum 1
SH2 (config) # in-path peering rule pass peer 10.0.1.3 rulenum 1
SH2 (config) # in-path rule pass-through srcaddr 10.0.1.1/32 rulenum 1
SH2 (config) # in-path rule pass-through srcaddr 10.0.1.3/32 rulenum 1
SH2 (config) # wr mem
SH2 (config) # show in-path peering rules
Rule  Type   Source Network     Dest Network       Port  Peer Addr
----- ------ ------------------ ------------------ ----- ---------------
    1 pass   *                  *                  *     10.0.1.3
    2 pass   *                  *                  *     10.0.1.1
  def auto   *                  *                  *     *
SH1 (config) # show in-path rules
Rule  Type Source Addr        Dest Addr          Port  Target Addr     Port
----- ---- ------------------ ------------------ ----- --------------- -----
    1 pass 10.0.1.3/32        *                  *     --              --
    2 pass 10.0.1.1/32        *                  *     --              --
  def auto *
                *                  *     --              --
```

SH3 configuration

```
SH3 > enable
SH3 # configure terminal
SH3 (config) # in-path peering rule pass peer 10.0.1.1 rulenum 1
SH3 (config) # in-path peering rule pass peer 10.0.1.2 rulenum 1
SH3 (config) # in-path rule pass-through srcaddr 10.0.1.1/32 rulenum 1
SH3 (config) # in-path rule pass-through srcaddr 10.0.1.2/32 rulenum 1
SH3 (config) # wr mem
SH3 (config) # show in-path peering rules
Rule  Type   Source Network     Dest Network       Port  Peer Addr
----- ------ ------------------ ------------------ ----- ---------------
SH1 (config) # show in-path rules
Rule  Type Source Addr        Dest Addr          Port  Target Addr     Port
----- ---- ------------------ ------------------ ----- --------------- -----
    1 pass 10.0.1.2/32        *                  *     --              --
    2 pass 10.0.1.1/32        *                  *     --              --
  def auto *                  *                  *     --              --
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path peering rules"

in-path probe direct

Description

Sets probing with the Steelhead appliance IP address.

Syntax

[no] in-path probe direct

Parameters

None

Usage

This command causes the probe responder to make the destination of the probe return a SYN/ACK for the in-path address of the client-side Steelhead appliance. It is useful when you are configuring correct addressing for WAN Visibility (transparency) and when you can only redirect LAN to WAN traffic at the client site. For details about WAN Visibility, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables the probe.

Example

```
amnesiac (config) # in-path probe direct
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path peering rules"

in-path probe version

Description

Sets probing with the in-path probe version settings.

Syntax

[no] in-path probe version <1 or 2>

Parameters

<1 or 2>	Specify the in-path probe version settings.

Usage

The **no** command option disables the version.

Example

```
amnesiac (config) # in-path probe version 1
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path probe-caching"

peer

Description

Configures the connection protocol version. Use only to harmonize connection protocol versions in deployments with a mix of v1.2 and v2.x appliances.

Syntax

[no] peer <ip-addr> version [min <version> | max <version>]

Parameters

<ip-addr>	Specify the in-path or out-of-path (or both) Steelhead appliance.
min <version>	Specify the protocol version number: **5** or **8**.
max <version>	Specify the protocol version number: **5** or **8**.

Usage

For each v1.2 Steelhead appliance peer, enter the following commands:

```
sh> peer <addr> version min 5
sh> peer <addr> version max 5
```

After all the v1.2 Steelhead appliances in the network have been upgraded to v2.x Steelhead appliances, remove the version settings:

```
sh> no peer <addr> version min
sh> no peer <addr> version max
```

If you are unable to discover all v1.2 Steelhead appliances in the network, configure all v2.1 Steelhead appliances to use v5 protocol by default with all peers by specifying 0.0.0.0 as the peer address:

```
sh> peer 0.0.0.0 version min 5
sh> peer 0.0.0.0 version max 5
```

Note: Version 5 does not support some optimization policy features. Ultimately, you need to upgrade all appliances to v2.1 or later.

The **no** command option resets the protocol version to the default.

Example

```
amnesiac (config) # peer 10.0.0.1 version min 5
amnesiac (config) # peer 10.0.0.2 version max 5
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path peering rules"

High-Speed TCP and Satellite Optimization Commands

This section describes the High-Speed TCP (HS-TCP) and satellite optimization commands.

protocol connection lan receive buf-size

Description

Sets the LAN receive buffer size for HS-TCP.

Syntax

[no] protocol connection lan receive buf-size <bytes>

Parameters

<bytes>	Specify the LAN receive buffer size. The default value is 32768.

Usage

To support High-Speed TCP (HS-TCP), you must increase your LAN buffer size to 1 MB.

The **no** command option resets the buffer size to the default.

Example

```
amnesiac (config) # protocol connection lan receive buf-size 1000000
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol connection"

protocol connection lan send buf-size

Description

Sets the LAN send buffer size for HS-TCP.

Syntax

[no] protocol connection lan send buf-size <bytes>

Parameters

<bytes>	Specify the LAN send buffer size. The default value is 81920.

Usage

To support HS-TCP, you must increase your LAN buffer size to 1 MB.

The **no** command option resets the buffer size to the default.

Example

```
amnesiac (config) # protocol connection lan send buf-size 1000000
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol connection"

protocol connection wan receive def-buf-size

Description

Sets the WAN receive buffer size for HS-TCP.

Syntax

[no] protocol connection wan receive def-buf-size <bytes>

Parameters

<bytes>	Specify the WAN receive buffer size. The default value is 262140.

Usage

To configure your WAN buffer you must increase the WAN buffers to twice Bandwidth Delay Product (BDP) or 10 MB. You can calculate the BDP WAN buffer size. For example:

Bandwidth = 155000000 Mbps
Delay = 100 ms

For a link of 155 Mbps and 100 ms round-trip delay, set the WAN buffers to

```
2 * 155000000 * 0.1 / 8 = 3875000
```

To calculate the BDP for a link

```
bandwidth * delay / 8 / MTU = X
```

If X is greater than default (256 KB), enable HS-TCP with the correct buffer size.

The **no** command option resets the buffer size to the default.

Example

```
amnesiac (config) # protocol connection wan receive def-buf-size 3875000
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol connection"

protocol connection wan send def-buf-size

Description

Sets the WAN send buffer size for HS-TCP.

Syntax

[no] protocol connection wan send def-buf-size <bytes>

Parameters

<bytes>	Specify the WAN send buffer size. The default value is 262140.

Usage

To configure your WAN buffer you must increase the WAN buffers to twice Bandwidth Delay Product (BDP) or 10 MB. You can calculate the BDP WAN buffer size. For example:

Bandwidth = 155000000 Mbps
Delay = 100 ms

For a link of 155 Mbps and 100 ms round-trip delay, set the WAN buffers to

```
2 * 155000000 * 0.1 / 8 = 3875000
```

To calculate the BDP for a link

```
bandwidth * delay / 8 / MTU = X
```

If X is greater than the default (256 KB), enable HS-TCP with the correct buffer size.

The **no** command option resets the buffer size to the default.

Example

```
amnesiac (config) # protocol connection wan send def-buf-size 3875000
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol connection"

single-ended rule optimized scps-discover

Description

Adds a single-ended optimization rule for SCPS discovery.

Syntax

single-ended rule optimized scps-discover [scraddr {IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstport <port(s)>] [allow-tcp-proxy {enable | disable}] [vlan <vlan>] [cong-ctrl-algo <cong-ctrl-algo>] [rate-pacing {enable | disable}] [rulenum <rulenum>]

Parameters

srcaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstport <port(s)>	Specify a destination port or port label for this rule. You can specify: • a single port number. • a comma-separated list of ports with or without ranges (for example, 1,2,4-10,12). • any user-defined port labels. Valid port labels include – Granite – Interactive – RBT-Proto – Secure For details on port labels, see "port-label" on page 500.
allow-tcp-proxy {enable | disable}	Specify **enable** to allow only SCPS peering and **disable** to allow SCPS and non-SCPS peering. This option is enabled by default.
vlan <vlan>	Specify a VLAN identification number from **1** to **4094** or **-1** to specify that the rule applies to all VLANs; or **0** to specify that the rule applies to untagged connections.
cong-ctrl-algo <cong-ctrl-algo>	Specify a method for congestion control for the rule: • **default** - Standard TCP optimization (RFC compliant) • **hstcp** - High-speed TCP optimization • **bw-est** - TCP bandwidth-estimation optimization • **per-conn-tcp** - SkipWare per-connection TCP. This option is not available without a SCPS license. • **err-tol-tcp** - SkipWare error-tolerant TCP optimization. This option is not available without a SCPS license.
rate-pacing {enable | disable}	Specify to enable or disable rate pacing on a per-rule basis. Rate pacing is disabled by default. Rate pacing applies only to MX-TCP traffic as classified by QoS.
rulenum <rulenum>	Specify a rule number from **1** to **N**, **start**, or **end**. The Steelhead appliances evaluate rules in numerical order, starting with rule **1**. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule **1** do not match, rule **2** is consulted. If rule **2** matches the conditions, it is applied, and no further rules are consulted.

Usage

You configure satellite optimization settings depending on the connection type. A single-ended interception (SEI) connection is a connection established between a single Steelhead appliance and a third-party device running TCP-PEP (Performance Enhancing Proxy). Both the Steelhead appliance and the TCP-PEP device are using the SCPS protocol to speed up the data transfer on a satellite link or other high-latency links.

You must have a SCPS license to use the **single-ended rule optimized scps-discover** command or to configure rate pacing on a per-rule basis. The Steelhead appliance uses the rules defined by this command to enable or pass through SCPS connections.

Rate pacing combines MX-TCP and a congestion control method of your choice for connections between peer Steelhead appliances and SEI connections (on a per-rule basis). The congestion control method runs as an overlay on top of MX-TCP and probes for the actual link rate. It then communicates the available bandwidth to MX-TCP. Rate pacing applies only to MX-TCP traffic as classified by QoS.

Use the **qos classification class** command to specify the MX-TCP queue method.

Use the **no single-ended rule <rule>** to remove a rule.

For details about satellite optimization, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # single-ended rule optimized scps-discover srcaddr all-ipv4 dstaddr all-ipv4
dstport secure rulenum 2
```

Product

Steelhead appliance

Related Topics

"qos classification class,""single-ended rule optimized tcp-proxy," "single-ended rule edit pass-through," "single-ended rule pass-through," "show connection," "show connections,""show single-ended rules," "show tcp rate-pacing status"

single-ended rule edit optimized scps-discover

Description

Edits a single-ended optimization rule for SCPS discovery.

Syntax

single-ended rule edit rulenum <rulenum> optimized scps-discover [scraddr {<IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstport <port(s)>] [allow-tcp-proxy {enable | disable}] [vlan <vlan>] [cong-ctrl-algo <cong-ctrl-algo>] [rate-pacing {enable | disable}]

Parameters

rulenum <rulenum>	Specify a rule number to edit.
srcaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstport <port(s)>	Specify a destination port or port label for this rule. You can specify: • a single port number. • a comma-separated list of ports with or without ranges (for example, 1,2,4-10,12). • any user-defined port labels. Valid port labels include – Granite – Interactive – RBT-Proto – Secure For more information on port labels, see “port-label” on page 500.
allow-tcp-proxy {enable | disable}	Specify **enable** to allow only SCPS peering and **disable** to allow SCPS and non-SCPS peering. This option is enabled by default.
vlan <vlan>	Specify a VLAN identification number from **1** to **4094** or **-1** to specify that the rule applies to all VLANs; or **0** to specify that the rule applies to untagged connections.
cong-ctrl-algo <cong-ctrl-algo>	Specify a method for congestion control for the rule: • **default** - Standard TCP optimization (RFC compliant) • **hstcp** - High-speed TCP optimization • **bw-est** - TCP bandwidth-estimation optimization • **per-conn-tcp** - SkipWare per-connection TCP. This option is not available without a SCPS license. • **err-tol-tcp** - SkipWare error-tolerant TCP optimization. This option is not available without a SCPS license.
rate-pacing {enable | disable}	Specify to enable or disable rate pacing on a per-rule basis. Rate pacing is disabled by default. Rate pacing applies only to MX-TCP traffic as classified by QoS.

Usage

Use this command to edit the rules defined by the **single-ended rule optimized scsp-discover** command.

Use the **no single-ended rule <rule>** to remove a rule.

Example

```
amnesiac (config) # single-ended rule edit rulenum 2 optimized scps-discover srcaddr all-ipv6
dstaddr all-ipv6 dstport interactive
```

Product

Steelhead appliance

Related Topics

"single-ended rule optimized tcp-proxy," "single-ended rule edit pass-through," "single-ended rule pass-through," "show connection," "show connections," "show single-ended rules"

single-ended rule move

Description

Changes the order of the existing SEI SCPS rules.

Syntax

[no] single-ended rule move <rulenum>] to <rulenum>

Parameters

rulenum <rulenum>	Specify a rule number from **1** to N, **start**, or **end**. Steelhead appliances evaluate rules in numerical order, starting with rule 1. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.

Example

```
amnesiac (config) # single-ended rule move 2 to 4
```

Product

Steelhead appliance

Related Topics

"single-ended rule optimized scps-discover," "single-ended rule optimized tcp-proxy," "show connection," "show single-ended rules"

single-ended rule optimized tcp-proxy

Description

Adds a single-ended optimization rule for TCP proxy.

Syntax

single-ended rule optimized tcp-proxy [scraddr {<IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstport <port(s)>] [vlan <vlan>] [cong-ctrl-algo <cong-ctrl-algo>] [rate-pacing {enable | disable}] [rulenum <rulenum>]]

Parameters

srcaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstport <port(s)>	Specify a destination port or port label for this rule. You can specify: • a single port number. • a comma-separated list of ports with or without ranges (for example, 1,2,4-10,12). • any user-defined port labels. Valid port labels include – Granite – Interactive – RBT-Proto – Secure For more information on port labels, see "port-label" on page 500.
vlan <vlan>	Specify a VLAN identification number from **1** to **4094** or **-1** to specify that the rule applies to all VLANs; or **0** to specify that the rule applies to untagged connections.
cong-ctrl-algo <cong-ctrl-algo>	Specify a method for congestion control for the rule: • **default** - Standard TCP optimization (RFC compliant) • **hstcp** - High-speed TCP optimization • **bw-est** - TCP bandwidth-estimation optimization • **per-conn-tcp** - SkipWare per-connection TCP. This option is not available without a SCPS license. • **err-tol-tcp** - SkipWare error-tolerant TCP optimization. This option is not available without a SCPS license.
rate-pacing {enable | disable}	Specify to enable or disable rate pacing on a per-rule basis. Rate pacing is disabled by default. Rate pacing applies only to MX-TCP traffic as classified by QoS.
rulenum <rulenum>	Specify a rule number from **1** to **N**, **start**, or **end**. The Steelhead appliances evaluate rules in numerical order, starting with rule **1**. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule **1** do not match, rule **2** is consulted. If rule **2** matches the conditions, it is applied, and no further rules are consulted.

Usage

The **single-ended rule optimized tcp-proxy** command allows you to configure single-ended connection optimization rules for TCP proxy.

Rate pacing combines MX-TCP and a congestion control method of your choice for connections between peer Steelhead appliances and SEI connections (on a per-rule basis). The congestion control method runs as an overlay on top of MX-TCP and probes for the actual link rate. It then communicates the available bandwidth to MX-TCP. Rate pacing applies only to MX-TCP traffic as classified by QoS.

Use the **qos classification class** command to specify the MX-TCP queue method.

Use the **no single-ended rule <rule>** to remove a rule.

The Steelhead appliance uses the rules defined by this command to enable or pass through TCP proxy connections.

Example

```
amnesiac (config) # single-ended rule optimized tcp-proxy
```

Product

Steelhead appliance

Related Topics

"single-ended rule optimized scps-discover," "single-ended rule edit pass-through," "single-ended rule pass-through," "show connection," "show connections," "show single-ended rules," "show tcp rate-pacing status"

single-ended rule edit optimized tcp-proxy

Description

Edits a single-ended optimization rule for TCP proxy.

Syntax

single-ended rule edit rulenum <rulenum> optimized tcp-proxy [scraddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstport <port(s)>] [vlan <vlan>] [cong-ctrl-algo <cong-ctrl-algo>] [rate-pacing {enable | disable}]

Parameters

rulenum <rulenum>	Specify a rule number to edit.
srcaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstport <port(s)>	Specify a destination port or port label for this rule. You can specify: • a single port number. • a comma-separated list of ports with or without ranges (for example, 1,2,4-10,12). • any user-defined port labels. Valid port labels include – Granite – Interactive – RBT-Proto – Secure For more information on port labels, see “port-label” on page 500.
vlan <vlan>	Specify a VLAN identification number from **1** to **4094** or **-1** to specify that the rule applies to all VLANs; or **0** to specify that the rule applies to untagged connections.
cong-ctrl-algo <cong-ctrl-algo>	Specify a method for congestion control for the rule: • **default** - Standard TCP optimization (RFC compliant) • **hstcp** - High-speed TCP optimization • **bw-est** - TCP bandwidth-estimation optimization • **per-conn-tcp** - SkipWare per-connection TCP. This option is not available without a SCPS license. • **err-tol-tcp** - SkipWare error-tolerant TCP optimization. This option is not available without a SCPS license.
rate-pacing {enable | disable}	Specify to enable or disable rate pacing on a per-rule basis. Rate pacing is disabled by default. Rate pacing applies only to MX-TCP traffic as classified by QoS.

Usage

Use this command to edit the rules defined by the **single-ended rule optimized tcp-proxy** command.

Use the **no single-ended rule <rule>** to remove a rule.

Example

```
amnesiac (config) # single-ended rule edit rulenum 2 optimized tcp-proxy srcaddr all-ip dstaddr all-
ipv4 dstport interactive
```

Product

Steelhead appliance

Related Topics

"single-ended rule optimized tcp-proxy," "single-ended rule edit pass-through," "single-ended rule pass-through," "show connection," "show connections," "show single-ended rules"

single-ended rule pass-through

Description

Adds a single-ended pass-through rule.

Syntax

single-ended rule pass-through [scraddr {<IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstport <port(s)>] [vlan <vlan>] [rulenum <rulenum>]

Parameters

srcaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstport <port(s)>	Specify a destination port or port label for this rule. You can specify: • a single port number. • a comma-separated list of ports with or without ranges (for example, 1,2,4-10,12). • any user-defined port labels. Valid port labels include – Granite – Interactive – RBT-Proto – Secure For more information on port labels, see "port-label" on page 500.
vlan <vlan>	Specify a VLAN identification number from **1** to **4094** or **-1** to specify that the rule applies to all VLANs; or **0** to specify that the rule applies to untagged connections.
rulenum <rulenum>	Specify a rule number from **1** to **N**, **start**, or **end**. The Steelhead appliances evaluate rules in numerical order, starting with rule **1**. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule **1** do not match, rule **2** is consulted. If rule **2** matches the conditions, it is applied, and no further rules are consulted.

Usage

Use the **single-ended rule passthrough** command to create a rule that allows SEI connections to pass through the Steelhead appliance unoptimized.

Use the **no single-ended rule <rule>** to remove a rule.

For details about satellite optimization, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # single-ended rule pass-through vlan 555
```

Product

Steelhead appliance

Related Topics

"single-ended rule optimized tcp-proxy," "single-ended rule edit pass-through," "single-ended rule pass-through," "show connection," "show connections," "show single-ended rules"

single-ended rule edit pass-through

Description

Edits a single-ended pass-through rule.

Syntax

single-ended rule edit rulenum <rulenum> pass-through [scraddr {<IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<IPv4-addr>| <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}] [dstport <port(s)>] [vlan <vlan>]

Parameters

rulenum <rulenum>	Specify the rule number to edit.
srcaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6>}	Specify the source subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip -** All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstaddr {<IPv4-addr> | <IPv6-addr> | all-ip |all-ipv4 | all-ipv6}	Specify the destination subnet IP address and netmask. Use the format XXX.XXX.XXX.XXX/XX for IPv4 and X:X:X::X/XXX for IPv6. You can also specify: • **all-ip** - All IPv4 and all IPv6 addresses. This is the default. • **all-ipv4** - All IPv4 addresses • **all-ipv6** - All IPv6 addresses
dstport <port(s)>	Specify a destination port or port label for this rule. You can specify: • a single port number. • a comma-separated list of ports with or without ranges (for example, 1,2,4-10,12). • any user-defined port labels. Valid port labels include – Granite – Interactive – RBT-Proto – Secure For details on port labels, see "port-label" on page 500.
vlan <vlan>	Specify a VLAN identification number from **1** to **4094** or **-1** to specify that the rule applies to all VLANs; or **0** to specify that the rule applies to untagged connections.

Usage

Use the **single-ended rule passthrough** command to create a rule that allows SEI connections to pass through the Steelhead appliance.

Example

```
amnesiac (config) # single-ended rule edit rulenum 2 pass-through srcaddr all-ipv6 dstaddr all-ipv6
```

Product

Steelhead appliance

Related Topics

"single-ended rule pass-through," "show connection," "show connections," "show single-ended rules"

tcp cong-ctrl mode

Description

Enables TCP congestion control settings.

Syntax

tcp cong-ctrl mode {auto | default | hstcp | bw-est |per-conn-tcp | err-tol-tcp}

Parameters

auto	Specify the automatic detection of TCP optimization. This mode detects the optimal TCP optimization by using the peer Steelhead appliance mode for inner connections, SkipWare when negotiated, or standard TCP for all other cases. Both the client-side and the server-side Steelhead appliances must be running RiOS v7.0. For single-ended interception connections, this mode uses SkipWare when possible, or standard TCP otherwise.
default	Specify standard TCP optimization (RFC compliant). This mode optimizes non-SCPS TCP connections by applying data and transport streamlining for TCP traffic over the WAN. For details on data and transport streamlining, see the *Steelhead Appliance Deployment Guide*. This option clears any advanced bandwidth congestion control that was previously set.
hstcp	Specify high-speed TCP optimization. This option allows for more complete use of long fat pipes (high-bandwidth, high-delay networks). Do not enable for satellite networks. Riverbed recommends that you enable high-speed TCP optimization only after you have carefully evaluated whether it benefits your network environment.
bw-est	Specify TCP bandwidth estimation optimization. This option calculates optimal transmission window sizes. Satellite networks typically have high latencies (order of 600ms to 1.2s), variable bandwidth, and packet losses (in chunks).
per-conn-tcp	Specify SkipWare per-connection TCP optimization. Applies TCP congestion control to each SCPS-capable connection. The congestion control uses: • a pipe algorithm that gates when a packet should be sent after receipt of an ACK. • the NewReno algorithm, which includes the sender's congestion window, slow start, and congestion avoidance. • timestamps, window scaling, appropriate byte counting, and loss detection.
err-tol-tcp	Specify SkipWare error-tolerant TCP optimization. Enables SkipWare optimization with the error rate detection and recovery mechanism on the Steelhead appliance. This option allows the per-connection congestion control to tolerate some amount of loss due to corrupted packets (bit errors), without reducing the throughput. Use caution when enabling error-tolerant TCP optimization, particularly in channels with coexisting TCP traffic, because it can adversely affect channel congestion with competing TCP flows.

Usage

TCP satellite network optimization uses a window congestion control mechanism that estimates the bandwidth available to TCP at the time of a perceived packet loss to provide an appropriate congestion window size for the traffic. Because the congestion window is sized according to available bandwidth, the satellite network performance improves.

Congestion control settings apply to inner connections. Outer connections use standard TCP.

Example

```
amnesiac (config) # tcp cong-ctrl mode bw-est
```

Product

Steelhead appliance

Related Topics

"show tcp cong-ctrl"

tcp highspeed enable

Description

Enables the HS-TCP feature, which provides acceleration and high throughput for high bandwidth networks where the WAN pipe is large but latency is high.

Syntax

[no] tcp highspeed enable

Parameters

None

Usage

HS-TCP is activated for all connections that have a Bandwidth Delay Product (BDP) larger than 100 packets. If you have a BDP of greater than 512 KB, and you are more interested in filling the WAN pipe than saving bandwidth, you should consider enabling HS-TCP.

You need to carefully evaluate whether HS-TCP will benefit your network environment. When enabling HS-TCP in high-available-bandwidth environments, Riverbed suggests that you test the throughput against various SDR and LZ settings. If you have an Optical Carrier-3 line or faster, turning off SDR makes sense and allows HS-TCP to reach its full potential.

To configure HS-TCP

- enable HS-TCP.
- disable LZ compression and SDR in the optimization policies if your WAN link capacity is 100 Mbps.
- enable in-path support.
- increase the WAN buffers to twice BDP or 10 MB. You can calculate the BDP WAN buffer size.
- increase the LAN buffers to 1 MB.

To calculate the BDP WAN buffer size

Bandwidth = 155000000 Mbps
Delay = 100 ms

For a link of 155 Mbps and 100 ms round-trip delay, the WAN buffers should be set to

```
2 * 155000000 * 0.1 / 8 = 3875000
```

To calculate the BDP for a link

```
bandwidth * delay / 8 / MTU = X
```

If X is greater than default (256 KB), enable HS-TCP with the correct buffer size.

The **no** command option disables HS-TCP.

Example

```
amnesiac (config) # tcp highspeed enable
amnesiac (config) # in-path rule auto-discover srcaddr 0.0.0.0/0 dstaddr 0.0.0.0/0 dstport 0
optimization none vlan -1 neural-mode always rulenum 1
amnesiac (config) # in-path enable
amnesiac (config) # protocol connection lan receive buf-size 1000000
amnesiac (config) # protocol connection lan send buf-size 1000000
amnesiac (config) # protocol connection wan receive def-buf-size 3875000
amnesiac (config) # protocol connection wan send def-buf-size 3875000
```

Product

Steelhead appliance, CSH

Related Topics

"show tcp highspeed"

tcp max-time-out

Description

Sets maximum time-out value for TCP connections. Riverbed recommends you contact Riverbed Support before you configure this setting.

Syntax

tcp max-time-out <seconds>

Parameters

<seconds>	Specify the maximum time-out value for TCP connections.

Example

```
amnesiac (config) # tcp max-time-out 60
```

Product

Steelhead appliance, CSH

Related Topics

"show tcp max-time-out"

tcp max-time-out mode enable

Description

Enables the TCP maximum time-out mode. Riverbed recommends you contact Riverbed Support before you configure this setting.

Syntax

tcp max-time-out mode enable

Parameters

None

Example

```
amnesiac (config) # tcp max-time-out mode enable
```

Product

Steelhead appliance, CSH

Related Topics

"show tcp max-time-out"

tcp rate-pacing enable

Description

Enables TCP rate pacing.

Syntax

[no] tcp rate-pacing enable

Parameters

None

Usage

When you enter the **tcp rate-pacing enable** command, a global data transmit limit is applied on the link rate for all SCPS connections between peer Steelhead appliances or on the link rate for a Steelhead appliance paired with a third-party device running TCP-PEP (Performance Enhancing Proxy).

Rate pacing applies only to MX-TCP traffic as classified by QoS using the **qos classification class** command.

You can also enable rate pacing for SEI connections by defining an SEI rule for each connection.

The **no** version of the command disables the rate pacing mechanism. Rate pacing is disabled by default and does not support IPv6. You must restart the optimization service for your changes to take effect.

For details about rate pacing, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # tcp rate-pacing enable
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"tcp sat-opt scps rule," "show tcp rate-pacing status"

tcp reordering threshold

Description

Enables the TCP reordering threshold. Riverbed recommends you contact Riverbed Support before you configure this setting.

Syntax

[no] tcp reordering threshold <value>

Parameters

<value>	Specify the TCP reordering threshold.

Example

```
amnesiac (config) # tcp reordering threshold
```

Product

Steelhead appliance, CSH

Related Topics

"show tcp reordering"

tcp sat-opt bw-est mode

Description

Specifies the TCP bandwidth estimation mode.

Syntax

[no] tcp sat-opt bw-est mode <mode>

Parameters

<mode>	Specify one of the following modes: • **refl-peer -** Automatically estimate the TCP bandwidth to control congestion if the peer Steelhead appliance is also estimating bandwidth. This setting makes satellite optimization easier to configure. Riverbed recommends this setting on the server-side Steelhead appliance in a satellite network. For example, suppose you have a large number of remote Steelheads communicating with a server-side Steelhead. Rather than defining an in-path rule for every subnet that communicates with a remote Steelhead over a satellite link, it is easier to enable the global **always** setting on the remote Steelhead appliance and this **refl-peer** setting on the server-side Steelhead. The server-side Steelhead can then detect the remote Steelhead during the connection setup and communicate with it over the satellite network. When this setting is enabled on both Steelheads, TCP bandwidth estimation does not occur. At least one peer Steelhead appliance must be set to **always** to estimate TCP bandwidth. Enabling this option requires an optimization service restart. • **always** - Always estimate the TCP bandwidth to control congestion globally on all traffic *sent* by this Steelhead appliance, regardless of the setting on the peer Steelhead appliance. Enabling this option also communicates this configuration to the peer Steelhead appliance so the peer can use TCP bandwidth estimation when it sends traffic to this Steelhead appliance. Riverbed recommends this setting on client-side and server-side Steelhead appliances in a satellite network. Enabling this option requires an optimization service restart. • **disable** - Disables bandwidth estimation mode. If this option is used, the TCP congestion control mode is set back to the default, which is standard TCP optimization.

Usage

Satellite channels have several characteristics that differ from terrestrial channels, such as dynamic bandwidth, asymmetric capability, and unconventional network architecture. These characteristics can cause problems that degrade the performance of TCP such as transmission errors, packet loss, and intermittent connectivity.

TCP satellite network optimization in RiOS v7.0 provides acceleration and high throughput for critical resources over satellite links. It improves TCP performance in a dynamic bandwidth environment, and is friendly with other real-time network traffic such as VoIP and video.

TCP satellite network optimization uses a window congestion control mechanism that estimates the bandwidth available to TCP at the time of a perceived packet loss to provide an appropriate congestion window size for the traffic. Because the congestion window is sized according to available bandwidth, the satellite network performance improves.

Example

```
amnesiac (config) # tcp sat-opt bw-est mode always
amnesiac (config) # config write
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"show tcp sat-opt settings"

tcp sat-opt scps legacy-comp enable

Description

Enables SkipWare legacy compression settings.

Syntax

[no] tcp sat-opt scps legacy-comp enable

Parameters

None

Usage

This command enables negotiation of SCPS-TP TCP header and data compression with a remote SCPS-TP device. This feature enables interoperation with RSP SkipWare packages and TurboIP devices that have also been configured to negotiate TCP header and data compression.

SkipWare legacy compression is not compatible with IPv6.

The **no** version disables SkipWare legacy compression settings.

Example

```
amnesiac (config) # tcp sat-opt scps legacy-comp enable
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"show tcp sat-opt settings"

tcp sat-opt scps legacy-comp process-batch

Description

Configures the maximum number of packets to process before yielding to the processor.

Syntax

[no] tcp sat-opt scps legacy-comp process-batch <number>

Parameters

<number>	Specify the maximum number of packets to process.

Usage

The **no** command option resets the maximum number of packets to process to the default value.

Example

```
amnesiac (config) # tcp sat-opt scps legacy-comp process-batch 500
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"show tcp sat-opt scps legacy-comp"

tcp sat-opt scps legacy-comp queuing-delay

Description

Sets an upper boundary on packets queued for module processing.

Syntax

[no] tcp sat-opt scps legacy-comp queuing-delay <ms>

Parameters

<ms>	Specify the queuing delay value, in milliseconds.

Usage

The **no** command option resets the maximum queing delay to the default value.

Example

```
amnesiac (config) # tcp sat-opt scps legacy-comp queuing-delay 1000
```

Product

Steelhead appliance

Related Topics

"show tcp sat-opt scps legacy-comp"

tcp sat-opt scps rule

Description

Configures Space Communications Protocol Standards (SCPS) rules for satellite optimization.

Syntax

[no] tcp sat-opt scps rule [srcaddr <network>] [dstaddr <network>] [dstport <port>] [allow-scps {enable | disable}] [scps-peer-only {enable | disable}] [vlan <tag ID>] [cong-ctrl-algo <mode>] [rate-pacing {enable | disable}] [rulenum <number>]

Parameters

srcaddr <network>	Specify an IPv4 address and mask for the traffic source. Use the format XXX.XXX.XXX.XXX/XX.
dstaddr <network>	Specify an IPv4 address and mask for the traffic destination. Use the format XXX.XXX.XXX.XXX/XX.
dstport <port(s)>	Specify a destination port or port label for this rule. You can specify: • a single port number. • a comma-separated list of ports with or without ranges (for example, 1,2,4-10,12). • any user-defined port labels. Valid port labels include – Interactive – RBT-Proto – Secure For details on port labels, see "port-label" on page 500.
allow-scps {enable | disable}	Specify an SCPS mode for this rule. • **enable** - Enable rule to optimize single-ended interception SCPS connections. • **disable** - Disable rule to optimize single-ended interception SCPS connections. If you choose this option, single-ended interception SCPS connections pass through the Steelhead appliance unoptimized.
scps-peer-only {enable | disable}	Specify an SCPS peering rule. • **enable** - Allow SCPS peering for single-ended interception SCPS connections. • **disable** - Allow both SCPS and non-SCPS peering (for example, proxy fallback) for single-ended interception connections.
vlan <tag ID>	Specify a VLAN tag ID for this rule. • 1 through 4094 • 0 (for untagged) • -1 (for all)
cong-ctrl-algo <mode>	Specify a method for congestion control for the rule: • **default** - Standard TCP optimization (RFC compliant) • **hstcp** - High-speed TCP optimization • **bw-est** - TCP bandwidth estimation • **per-conn-tcp** - SkipWare per-connection TCP. This is the default algorithm. • **err-tol-tcp** - SkipWare error-tolerant TCP optimization
rate-pacing {enable | disable}	Specify to enable or disable rate pacing. Rate pacing is disabled by default. Enabling rate pacing evenly spreads the transmission of a window of packets across the entire duration of the round-trip time.
rulenum <number>	Specify the number or order in the SCPS rule table for this rule. • 1 to *N* or start/end

Usage

Before configuring SCPS rules, you must have a valid SCPS license and you must enable the SCPS table using the **tcp sat-opt scps scps-table enable** command.

The **no** command option removes the rule. The **no** command option has the following syntax:

```
no tcp sat-opt scps rule <number>
```

Example

```
amnesiac (config) # tcp sat-opt scps rule srcaddr 1.1.1.1/32 dstaddr 2.2.2.2/32  allow-scps enable
vlan 2000 rulenum 2
```

Product

Steelhead appliance

Related Topics

"tcp cong-ctrl mode,""tcp sat-opt scps scps-table enable," "show tcp sat-opt scps rules"

tcp sat-opt scps rule edit

Description

Edits Space Communications Protocol Standards (SCPS) rules for satellite optimization.

Syntax

[no] tcp sat-opt scps rule edit rulenum <number> [srcaddr <network>] [dstaddr <network>] [dstport <port>] [allow-scps {enable | disable}] [scps-peer-only {enable | disable}] [vlan <tag ID>] [cong-ctrl-algo <mode>] [rate-pacing {enable | disable}]

Parameters

rule <number>	Specify the number in the SCPS rule table to edit.
srcaddr <network>	Specify an IPv4 address and mask for the traffic source. Use the format XXX.XXX.XXX.XXX/XX.
dstaddr <network>	Specify an IPv4 address and mask for the traffic destination. Use the format XXX.XXX.XXX.XXX/XX.
dstport <port(s)>	Specify a destination port or port label for this rule. You can specify: • a single port number. • a comma-separated list of ports with or without ranges (for example, 1,2,4-10,12). • any user-defined port labels. Valid port labels include – Interactive – RBT-Proto – Secure For details on port labels, see "port-label" on page 500.
allow-scps {enable | disable}	Specify an SCPS mode for this rule. • **enable** - Enable rule to optimize single-ended interception SCPS connections. • **disable** - Disable rule to optimize single-ended interception SCPS connections. If you choose this option, single-ended interception SCPS connections pass through the Steelhead appliance unoptimized.
scps-peer-only {enable | disable}	Specify an SCPS peering rule. • **enable** - Allow SCPS peering for single-ended interception SCPS connections. • **disable** - Allow both SCPS and non-SCPS peering (for example, proxy fallback) for single-ended interception connections.
vlan <tag ID>	Specify a VLAN tag ID for this rule. • 1 through 4094 • 0 (for untagged) • -1 (for all)
cong-ctrl-algo <mode>	Specify a method for congestion control for the rule: • **default** - Standard TCP optimization (RFC compliant) • **hstcp** - High-speed TCP optimization • **bw-est** - TCP bandwidth estimation • **per-conn-tcp** - SkipWare per-connection TCP. This is the default algorithm. • **err-tol-tcp** - SkipWare error-tolerant TCP optimization
rate-pacing {enable | disable}	Specify to enable or disable rate pacing. Enabling rate pacing evenly spreads the transmission of a window of packets across the entire duration of the round-trip time.

Usage

Before configuring SCPS rules, you must have a valid SkipWare license and you must enable the SCPS table using the **tcp sat-opt scps scps-table enable** command.

The **no** command option removes the rule. The **no** command option has the following syntax:

```
no tcp sat-opt scps rule <number>
```

Example

```
amnesiac (config) # tcp sat-opt scps rule srcaddr 1.1.1.1/32 dstaddr 2.2.2.2/32  allow-scps enable
vlan 2000 rulenum 2
```

Product

Steelhead appliance

Related Topics

"tcp cong-ctrl mode,""tcp sat-opt scps scps-table enable," "show tcp sat-opt scps rules"

tcp sat-opt scps rule move

Description

Changes the order of the existing SCPS rules in the SCPS rule table.

Syntax

[no] tcp sat-opt scps rule move <rule number> to <rule number>

Parameters

<rule number>	Specify the numbers corresponding to any existing rules in the SCPS rule table.

Usage

SCPS optimization requires a valid SCPS license.

Example

```
amnesiac (config) # tcp sat-opt scps rule move 4 to 3
```

Product

Steelhead appliance

Related Topics

"show tcp sat-opt scps rules"

tcp sat-opt scps scps-table enable

Description

Configures SCPS table settings.

Syntax

[no] tcp sat-opt scps scps-table enable

Parameters

None

Usage

SCPS optimization requires a valid SCPS license.

Example

```
amnesiac (config) # tcp sat-opt scps scps-table enable
```

Product

Steelhead appliance

Related Topics

"show tcp sat-opt settings"

Data Store Configuration Commands

This section describes the commands for configuring the following data store features:

- Warming branch Steelhead Mobile Clients
- Encrypting the data store
- Configuring data store notification and wrap-around
- Synchronizing the data store

datastore branchwarming enable

Description

Enables branch warming for Steelhead Mobile Clients. By default, branch warming is enabled.

Syntax

[no] datastore branchwarming enable

Parameters

None

Usage

Branch warming keeps track of data segments created while a Steelhead Mobile user is in a Steelhead appliance-enabled branch office and trickles the new data back to the Steelhead Mobile laptop. When the user goes back on the road, they receive warm performance.

Branch warming co-operates with and optimizes transfers for a server-side Steelhead appliance. New data transfers between the client and server are populated in the Steelhead Mobile data store, the branch Steelhead appliance data store, and the server-side Steelhead appliance data store.

When the server downloads data, the server-side Steelhead appliance checks if either the Steelhead Mobile Client or the branch Steelhead appliance has the data in their data store. If either device already has the data segments, the server-side Steelhead appliance sends only references to the data. The Mobile Client and the branch Steelhead appliance communicate with each other to resolve the references.

Other clients at a branch office benefit from branch warming as well, because data transferred by one client at a branch also populates the branch Steelhead appliance data store. Performance improves with all clients at the branch because they receive warm performance for that data.

The Steelhead Mobile Client must be running v2.1 or later.

Branch Warming does not improve performance for configurations using:

- SSL connections
- Out-of-path (fixed-target rules)

Steelhead Mobile Clients which communicate with multiple server-side appliances in different scenarios. For example, if a Steelhead Mobile Client home user peers with one server-side Steelhead appliance after logging in through a VPN network and peers with a different server-side Steelhead appliance after logging in from the branch office, branch warming does not improve performance.

The **no** command option disables this feature.

Example

```
amnesiac (config) # datastore branchwarming enable
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore branchwarming"

datastore encryption type

Description

Enables or disables encryption of the data store and specifies the type of encryption to use. Encrypting the data store significantly limits the exposure of sensitive data in the event that the system is compromised by loss, theft, or a security violation. Before you encrypt the data store, the secure vault must be unlocked. For details, see "secure-vault" on page 698.

Syntax

[no] datastore encryption type {NONE | AES_128 | AES_192 | AES_256}

Parameters

[NONE | AES_128 | AES_192 | AES_256]	Specify a data store encryption scheme: • **NONE** - Do not encrypt the data store. • **AES_128** - Use the Advanced Encryption Standard (AES) 128-bit cipher setting. • **AES_192** - Use the AES 192-bit cipher setting. • **AES_256** - Use the AES 256-bit cipher setting. This encryption scheme is the most secure. **Note:** Encryption types can be lower-case.

Usage

Encrypting the data store significantly limits the exposure of sensitive data in the event an appliance is compromised by loss, theft, or a security violation. The secure data is difficult for a third party to retrieve.

Before you encrypt the data store, the secure vault must be unlocked. The encryption key is stored in the secure vault.

Encrypting the data store can have performance implications; generally, higher security means less performance. Several encryption strengths are available to provide the right amount of security while maintaining the desired performance level. When selecting an encryption type, you must evaluate the network structure, the type of data that travels over it, and how much of a performance trade-off is worth the extra security.

You must clear the data store and reboot the Steelhead service on theSteelhead appliance after turning on, changing, or turning off the encryption type. After you clear the data store, the data cannot be recovered. If you do not want to clear the data store, reselect your previous encryption type and reboot the service. The Steelhead appliance uses the previous encryption type and encrypted data store.

To encrypt the data store

1. Make sure your secure vault is unlocked. The encryption key is stored in the secure vault.

```
secure-vault unlock
```

For details, see "secure-vault" on page 698.

2. Turn on data store encryption;

```
datastore encryption type AES_256
```

3. Clean the data store and restart the Steelhead service:

```
restart clean
```

Encrypted Data Store Downgrade Limitations

The Steelhead appliance cannot use an encrypted data store with an earlier RiOS software version, unless the release is an update (v4.x.x). For example, an encrypted data store created in v4.1.4 would work with v4.1.2, but not with v4.0.x.

Before downgrading to an earlier software version, you must select **none** as the encryption type, clear the data store, and restart the service. After you clear the data store, the data are removed from persistent storage and cannot be recovered.

To downgrade the data store

1. Turn off data store encryption.

```
datastore encryption type NONE
```

2. Clean the data store and restart the Steelhead service:

```
restart clean
```

If you return to a previous software version and there is a mismatch with the encrypted data store, the status bar indicates that the data store is corrupt. You can either:

- Use the backup software version after clearing the data store and rebooting the service.

Or

- Return to the software version in use when the data store was encrypted, and continue using it.
- For details, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # datastore encryption type AES_192
amnesiac (config) # restart clean
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore"

datastore notification enable

Description

Enables email notification when the data in the data store is replaced with new data.

Syntax

[no] datastore notification enable

Parameters

None

Usage

The **no** command option disables notification wrap-around.

Example

```
amnesiac (config) # datastore notification enable
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore"

datastore notification wrap-around

Description

Sets the number of days to elapse before sending an email message notifying you that the data in the data store has been replaced.

Syntax

[no] datastore notification wrap-around <days>

Parameters

<days>	Specify the number of days to elapse before sending an email message notifying you that the data in the data store has been replaced.

Usage

The **no** command option disables notification wrap-around.

Example

```
amnesiac (config) # datastore notification wrap-around 2
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore"

datastore safety-valve threshold

Description

Configures the data store safety-valve threshold settings.

Syntax

[no] datastore safety-valve threshold {<milliseconds> | default}

Parameters

<milliseconds>	Specify disk response threshold time in milliseconds.
default	Specify default threshold time.

Usage

The **datastore safety-valve threshold** command sets a threshold for when a disk-bypass mechanism starts in the event of high disk I/O latencies.

Example

```
amnesiac (config) # datastore safety-valve threshold 20000
```

Product

Steelhead appliance

Related Topics

"datastore safety-valve timeout," "show datastore safety-valve"

datastore safety-valve timeout

Description

Configures the data store safety-valve timeout settings.

Syntax

[no] datastore safety-valve timeout {<seconds> | default}

Parameters

<seconds>	Specify the timeout value in seconds.
default	Specify the default timeout value.

Usage

The **no** version of the command disables data store safety-valve timeout settings.

Example

```
amnesiac (config) # datastore safety-valve timeout 600
```

Product

Steelhead appliance

Related Topics

"datastore safety-valve threshold," "show datastore safety-valve"

show datastore safety-valve

Description

Displays the data store safety-valve settings.

Syntax

show datastore safety-valve

Parameters

None

Example

```
amnesiac (config) # show datastore safety-valve
Data Store Safety valve              : Off
Data Store Safety valve threshold    : 20000 milli seconds
Data Store Safety valve timeout      : 600 seconds
```

Product

Steelhead appliance

Related Topics

"datastore safety-valve threshold," "datastore safety-valve timeout"

datastore sync enable

Description

Enables pairs of Steelhead appliances on the same side of a WAN to automatically keep their data stores synchronized. This feature is also known as active-active synchronization.

Syntax

[no] datastore sync enable

Parameters

None

Usage

This feature provides for failover and overflow capacity without performance loss. Beginning with RiOS v4.0, you can enable this feature independent of whether or not you have enabled failover.

For deployments requiring the highest levels of redundancy and performance, RiOS supports warm standby between designated master and backup devices. Using automated data store synchronization, the data segments and the references created via data streamlining are automatically copied from the master to the backup appliance. In the event of a failure in the master appliance, the backup appliance takes its place with a *warm* data store, and can begin delivering fully-optimized performance immediately. Warm data transfers send only new or modified data, dramatically increasing the rate of data transfer over the WAN.

RiOS supports active-active configurations, in which each appliance is serving both as a master for some traffic and as a backup for the other appliance, with full data store synchronization. Automatic synchronization can include appliances in a serial or WCCP cluster, and appliances using connection forwarding.

Synchronization takes place over the primary or auxiliary port only.

Failover is not required for data store synchronization. Although the failover and synchronization features are typically enabled together, you can enable data store synchronization independently of standard failover.

In most implementations in which both failover and synchronization are enabled, the same Steelhead appliance serves as the master for both failover and data store synchronization. However, if you enable failover and synchronization, the failover master and the synchronization master do not have to be the same Steelhead appliance.

You configure two Steelhead appliances to enable synchronization, one as a server (the synchronization master) and the other as a backup. The synchronization master and its backup:

- must be on the same LAN.
- do not have to be in the same physical location. If they are in different physical locations, they must be connected via a fast, reliable LAN connection with minimal latency.
- must be running the same version of the RiOS software.
- must have the same hardware model.
- must be configured on the primary or auxiliary interface.

When you have configured the master and backup appliances, you must restart the Steelhead service on the backup Steelhead appliance. The master restarts automatically.

After you have enabled and configured synchronization, the data stores are actively kept synchronized. For details on how synchronized appliances replicate data and how data store synchronization is commonly used in high availability designs, see the *Steelhead Appliance Deployment Guide*.

If one of the synchronized Steelhead appliances is under high load, some data might not be copied. For detailed information, see the *Steelhead Appliance Deployment Guide*.

If data store synchronization is interrupted for any reason (such as a network interruption or if one of the Steelhead appliances is taken out of service), the Steelhead appliances continue other operations without disruption. When the interruption is resolved, data store synchronization resumes without risk of data corruption.

The **no** command option disables automatic synchronization.

Example

```
amnesiac (config) # datastore sync peer-ip 192.148.0.12
amnesiac (config) # datastore sync port 7744
amnesiac (config) # datastore sync reconnect 30
amnesiac (config) # datastore sync master
amnesiac (config) # datastore sync enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

“show datastore”

datastore sync master

Description

Sets the local appliance as the master appliance to which the data stores for other appliances synchronize.

Syntax

[no] datastore sync master

Parameters

None

Usage

The **no** command option removes the master status for the appliance data store.

Example

```
amnesiac (config) # datastore sync master
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore"

datastore sync peer-ip

Description

Sets the IP address for the peer appliance for which you want to push replicated data.

Syntax

datastore sync peer-ip <ip-addr>

Parameters

<ip-addr>	Specify the primary or the aux interface IP address of a backup appliance.

Example

```
amnesiac (config) # datastore sync peer-ip 10.0.0.3
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore"

datastore sync port

Description

Sets the port for the peer Steelhead appliance for which you want to push replicated data.

Syntax

[no] datastore sync port <port>

Parameters

<port>	Specify the port of the peer Steelhead appliance. The default value is 7744.

Usage

The **no** command option resets the port to the default value.

Example

```
amnesiac (config) # datastore sync port 1234
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore"

datastore sync reconnect

Description

Sets the reconnection interval for data store synchronization.

Syntax

[no] datastore sync reconnect <seconds>

Parameters

<seconds>	Specify the number of seconds for the reconnection interval. The default value is 30.

Usage

The **no** command option resets the reconnection interval to the default.

Example

```
amnesiac (config) # datastore sync reconnect 40
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore"

Data Store Replication and Protection Commands

Typically, the data store does not need to be modified. You modify data store settings for data replication and data protection environments. In addition to these commands, Riverbed recommends that you also configure high-speed TCP to improve data store performance for data protection environments. For details, see "High-Speed TCP and Satellite Optimization Commands" on page 381.

For details, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide* or the *Steelhead Appliance Deployment Guide*.

Important: Riverbed recommends you contact Riverbed Support before you change these default configuration settings.

datastore codec compression adaptive

Description

Enables adaptive LZ compression.

Syntax

[no] datastore codec compression adaptive

Parameters

None

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # datastore codec compression adaptive
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore disk"

datastore codec compression level

Description

Configures the data store LZ compression level.

Syntax

[no] datastore codec compression level <lz level>

Parameters

<lz level>	Specify the compression level. The range is **0-9**.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # datastore codec compression level
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore disk"

datastore codec multi-core-bal

Description

Enables data store multi-core balancing.

Syntax

[no] datastore codec multi-core-bal

Parameters

None

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # datastore codec multi-core-bal
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore disk"

datastore disk read-pressure interval

Description

Configures the data store disk read-pressure.

Syntax

[no] datastore disk read-pressure interval <seconds>

Parameters

<seconds>	Specify the data store read-pressure interval, in seconds.

Usage

The **no** command option disables the read pressure interval.

Example

```
amnesiac (config) # datastore disk read-pressure interval 5
```

Product

CMC appliance, Steelhead appliance, CSH

Related Topics

"show datastore disk"

datastore disklayout fifo

Description

Enables a replacement algorithm that replaces data in the order that they are received (first in, first out).

Before you enable the set of data replication commands, please contact Riverbed Support at https://support.riverbed.com.

Syntax

[no] datastore disklayout fifo

Parameters

None

Usage

The data store segment replacement policy selects the technique used to replace the data in the data store. While the default setting works best for most Steelhead appliances, occasionally Riverbed Support recommends changing the policy to improve performance.

The client-side and server-side Steelhead appliances must be running RiOS v6.0.x or later.

Enabling the LRU disk layout method may cause the data store wrap warning to occur earlier than expected when using the FIFO replacement policy. This is expected behavior.

The **no** command option disables anchor selection.

Example

```
amnesiac (config) # datastore disklayout fifo
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore disklayout"

datastore disklayout rvbdlru

Description

Enables a replacement algorithm that replaces the least recently used, evicting pages that have not been used on disk for the longest time. This is the default setting.

Before you enable the set of data replication commands, please contact Riverbed Support at https://support.riverbed.com.

Syntax

[no] datastore disklayout rvbdlru

Parameters

None

Usage

The data store segment replacement policy selects the technique used to replace the data in the data store. While the default setting works best for most Steelhead appliances, occasionally Riverbed Support recommends changing the policy to improve performance.

The client-side and server-side Steelhead appliances must be running RiOS v6.0.x or later.

The **no** command option disables this option.

Example

```
amnesiac (config) # datastore disklayout rvbdlru
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore disklayout"

datastore sdr-policy

Description

Configures the data store SDR policy.

Syntax

[no] datastore sdr-policy [default | sdr-a | sdr-m | sdr-a-advanced]

Parameters

default	Specify the default setting that works for most implementations. The default setting: • Provides the most data reduction. • Reduces random disk seeks and improves disk throughput by discarding very small data margin segments that are no longer necessary. This Margin Segment Elimination (MSE) process provides network-based disk defragmentation. • Writes large page clusters. • Monitors the disk write I/O response time to provide more throughput.
sdr-a	Includes the default settings described above, and also: • Balances writes and reads. • Monitors both read and write disk I/O response time to provide more throughput. **Important:** Use caution with this setting, particularly when you are optimizing CIFS or NFS with prepopulation. Please contact Riverbed Support for more information.
sdr-m	Performs data reduction entirely in memory, which prevents the Steelhead appliance from reading and writing to and from the disk. Enabling this option can yield high LAN-side throughput because it removes all disk latency. SDR-M is most efficient when used between two identical high-end Steelhead appliance models; for example, 6020 - 6020. When used between two different Steelhead appliance models, the smaller model limits the performance. **Important:** You must reboot the client-side and server-side Steelhead appliances if you enable SDR-M. **Important:** You cannot use peer data store synchronization with SDR-M.
sdr-a-advanced	Maximizes LAN-side throughput dynamically under different data work loads. This switching mechanism is governed with a throughput and bandwidth reduction goal using the available WAN bandwidth. If you have enabled SDR-Adaptive prior to upgrading to RiOS v6.0 and later, the default setting is SDR-Adaptive Legacy. If you did not change the SDR-Adaptive setting prior to upgrading to RiOS 6.0 or later, the default setting is SDR-Adaptive Advanced. **Important:** If you did not change the SDR-Adaptive setting prior to upgrading to RiOS 6.0 or later, the default setting is SDR-Adaptive Advanced.

Usage

An adaptive data streamlining mode determines how the Steelhead appliance stores and maintains the data references. It also optimizes disk access for data replication, if needed. The data streamlining approaches range from less to more aggressive. Changing the default setting is *optional*; you should select another setting only when it is critical and only with guidance from Riverbed Support.

Generally, the default setting provides the most data reduction. When choosing an adaptive streamlining mode for your network, you should contact Riverbed Support to help you evaluate the setting based on:

- the amount of data replication your data store is processing.
- how often the replication occurs (for example, as soon as a write occurs, or in a nightly batch).
- how much data reduction you can sacrifice for higher throughput.

The client-side and server-side Steelhead appliances must be running RiOS v6.0.x or later.

The no command option disables this option.

Example

```
amnesiac (config) # datastore sdr-policy sdr-a
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore sdr-policy"

datastore write-q-prior

Description

Enables priority for deferred writes.

Before you enable the set of data replication commands, please contact Riverbed Support at https://support.riverbed.com.

Syntax

[no] datastore write-q-prior

Parameters

None

Usage

Use this command if you are experiencing a gradual decline in optimization over time when using DR applications.

The **no** command option disables deferred writes.

Example

```
amnesiac (config) # datastore write-q-prior
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore write-q-prior"

disk reset

Description

Resets the specified disk.

Syntax

disk <disk number> reset

Parameters

<disk number>	Specify the disk number to be reset.

Example

```
amnesiac (config) # disk 2 reset
```

Product

Steelhead appliance, CSH

Related Topics

"show datastore disk"

WCCP Support Commands

This section describes the WCCP support commands.

wccp adjust-mss enable

Description

Enables the Adjust Maximum Segment Size (MSS) feature.

Syntax

[no] wccp adjust-mss enable

Parameters

None

Usage

The default for the Steelhead appliance is to have the Don't Fragment (DF) bit set to 1 so that packets are not fragmented. However, this occasionally causes issues with WCCP using GRE and when VPN tunnels are used for Steelhead appliance connections. The result is dropped packets.

This command shrinks the MSS to fit accordingly.

The **no** command disables this feature.

Example

```
amnesiac (config) # wccp adjust-mss enable
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

"show wccp"

wccp enable

Description

Enables WCCP support.

Syntax

[no] wccp enable

Parameters

None

Usage

For details about configuring WCCP, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

WCCP enables you to redirect traffic that is not in the direct physical path between the client and the server. To enable WCCP, the Steelhead appliance must join a service group at the router. A service group is a group of routers and Steelhead appliances which define the traffic to redirect, and the routers and Steelhead appliances the traffic goes through. You might use one or more service groups to redirect traffic to the Steelheads for optimization.

RiOS v6.1 and later provides additional WCCP configuration, allowing each individual Steelhead appliance in-path interface to be configured as a WCCP client. Each configured in-path interface participates in WCCP service groups as an individual WCCP client, providing flexibility to determine load balancing proportions and redundancy.

The **no** command option disables WCCP support.

Example

```
amnesiac (config) # wccp enable
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

"show wccp"

wccp interface service-group

Description

Defines a new WCCP service group.

Syntax

wccp interface <interface> service-group service group <service-id> <cr> | routers <routers> | protocol [tcp|udp|icmp] | flags <flags> | priority <priority> | ports <ports> | password <password> | weight <weight> | encap-scheme [either | gre | l2] | assign-scheme [either | hash | mask] | src-ip-mask <mask> | dst-ip-mask <mask> | src-port-mask <mask> | dst-port-mask <mask>

Parameters

<interface>	Select a Steelhead appliance interface to participate in a WCCP service group. RiOS v6.1 allows multiple Steelhead interfaces to participate in WCCP on one or more routers for redundancy (RiOS v6.0 and earlier allows a single Steelhead interface). If one of the links goes down, the router can still send traffic to the other active links for optimization. You must include an interface with the service group ID. More than one Steelhead appliance in-path interface can participate in the same service group. For WCCP configuration examples, see the *Steelhead Appliance Deployment Guide*. If multiple Steelhead appliances are used in the topology, they must be configured as neighbors.
service group <service-id>	Enables WCCP v2 support on all groups added to the Service Group list. Specify a number from 0 to 255 to identify the service group on the router. A value of 0 specifies the standard HTTP service group. Riverbed recommends that you use WCCP service groups 61 and 62. **Note:** The service group ID is local to the site where WCCP is used. **Note:** The service group number is not sent across the WAN.
routers <routers>	Specify a comma-separated list of IP addresses for routers. **Note:** You can specify up to 32 routers.
protocol <tcp | udp | icmp>	Specify one of the following traffic protocols: **tcp**, **udp**, or **icmp**. **Note:** The default value is tcp.
flags <flags>	Specify the service group flags. Specify a comma-separated list of the following flags, as needed: • **src-ip-hash** - Uses the source IP address as a hash key. • **dst-ip-hash** - Uses the destination IP address as a hash key. • **src-port-hash** - Uses the source port as a hash key. • **dst-port-hash** - Uses the destination port as a hash key. • **ports-dest** - Specifies the destination ports for redirection. • **ports-source** - Specifies the source ports for redirection.
priority <priority>	Specify the WCCP priority for traffic redirection. If a connection matches multiple service groups on a router, the router chooses the service group with the highest priority. The range is 0-255. The default value is 200. **Note:** The priority value must be consistent across all Steelhead appliances within a particular service group.
ports <ports>	Specify a comma-separated list of up to seven ports that the router will redirect. **Note:** Set this parameter only if the **flags** parameter specifies either **ports-dest** or **ports-source**.
password <password>	Optionally, assign a password to the Steelhead appliance. This password must be the same password that is on the router. WCCP requires that all routers in a service group have the same password. Passwords are limited to 8 characters.

weight <weight>	Specify a weight value in the range of 0-65535. You specify the percentage of connections that are redirected to a particular Steelhead appliance interface, which is useful for traffic load balancing and failover support. The number of TCP, UDP, or ICMP connections a Steelhead appliance supports determines its weight. The more connections a Steelhead appliance model supports, the heavier the weight of that model. In RiOS v6.1 you can modify the weight for each in-path interface to manually tune the proportion of traffic a Steelhead interface receives. A higher weight redirects more traffic to that Steelhead interface. The ratio of traffic redirected to a Steelhead interface is equal to its weight divided by the sum of the weights of all the Steelhead interfaces in the same service group. For example, if there are two Steelhead appliances in a service group and one has a weight of 100 and the other has a weight of 200, the one with the weight 100 receives 1/3 of the traffic and the other receives 2/3 of the traffic. However, since it is generally undesirable for a Steelhead appliance with two WCCP in-path interfaces to receive twice the proportion of traffic, for Steelhead appliances with multiple in-paths connected, each of the in-path weights is divided by the number of that Steelhead appliance interfaces participating in the service group. For example, if there are two Steelhead appliances in a service group and one has a single interface with weight 100 and the other has two interfaces each with weight 200, the total weight will still equal 300 (100 + 200/2 + 200/2). The one with the weight 100 receives 1/3 of the traffic and each of the other's in-path interfaces receives 1/3 of the traffic. The range is 0-65535. The default value corresponds to the number of TCP connections your Steelhead appliance supports. **Failover Support** To enable single in-path failover support with WCCP groups, define the service group weight to be 0 on the backup Steelhead appliance. If one Steelhead appliance has a weight 0, but another one has a non-zero weight, the Steelhead appliance with weight 0 does not receive any redirected traffic. If all the Steelhead appliances have a weight 0, the traffic is redirected equally among them. The best way to achieve multiple in-path failover support with WCCP groups in RiOS v6.1 is to use the same weight on all interfaces from a given Steelhead appliance for a given service group. For example, suppose you have Steelhead A and Steelhead B with two in-path interfaces each. When you configure Steelhead A with weight 100 from both inpath0_0 and inpath0_1 and Steelhead B with weight 200 from both inpath0_0 and inpath0_1, RiOS distributes traffic to Steelhead A and Steelhead B in the ratio of 1:2 as long as at least one interface is up on both Steelhead appliances. In a service group, if an interface with a non-zero weight fails, its weight transfers over to the weight 0 interface of the same service group. For details on using the weight parameter to balance traffic loads and provide failover support in WCCP, see the *Steelhead Appliance Deployment Guide*.
encap-scheme [either | gre | l2]	Specify one of the following methods for transmitting packets between a router or a switch and a Steelhead appliance interface: • **either** - Use Layer-2 first; if Layer-2 is not supported, GRE is used. This is the default value. • **gre** - Generic Routing Encapsulation. The GRE encapsulation method appends a GRE header to a packet before it is forwarded. This can cause fragmentation and imposes a performance penalty on the router and switch, especially during the GRE packet de-encapsulation process. This performance penalty can be too great for production deployments. • **l2** -Layer-2 redirection. The L2 method is generally preferred from a performance standpoint because it requires fewer resources from the router or switch than the GRE does. The L2 method modifies only the destination Ethernet address. However, not all combinations of Cisco hardware and IOS revisions support the L2 method. Also, the L2 method requires the absence of L3 hops between the router or switch and the Steelhead appliance.

assign-scheme [either | hash | mask]	Determines which Steelhead interface in a WCCP service group the router or switch selects to redirect traffic to for each connection. The assignment scheme also determines whether the Steelhead interface or the router processes the first traffic packet. The optimal assignment scheme achieves both load balancing and failover support. Specify one of the following schemes: • **either** - Uses Hash assignment unless the router does not support it. When the router does not support Hash, it uses Mask. This is the default setting. • **hash** - Redirects traffic based on a hashing scheme and the Weight of the Steelhead interface, providing load balancing and failover support. This scheme uses the CPU to process the first packet of each connection, resulting in slightly lower performance. However, this method generally achieves better load distribution. Riverbed recommends Hash assignment for most Steelhead appliances if the router supports it. The Cisco switches that do not support Hash assignment are the 3750, 4000, and 4500-series, among others. Your hashing scheme can be a combination of the source IP address, destination IP address, source port, or destination port. • **mask** - Redirects traffic operations to the Steelhead appliances, significantly reducing the load on the redirecting router. Mask assignment processes the first packet in the router hardware, using less CPU cycles and resulting in better performance. Mask assignment in RiOS v5.0.1 and earlier is limited to one Steelhead appliance per service group. The Steelhead appliance with the lowest in-path IP address receives all the traffic. This scheme provides high availability. You can have multiple Steelhead appliances in a service group but only the Steelhead appliance with the lowest in-path IP address receives all the traffic. If the Steelhead appliance with the lowest in-path IP address fails, the Steelhead appliance with the next lowest in-path IP address receives all of the traffic. When the Steelhead appliance with the lowest in-path IP address recovers, it again receives all of the traffic. Mask assignment in RiOS v5.0.2 and later supports load-balancing across multiple active Steelhead appliances. This scheme bases load-balancing decisions (for example, which Steelhead appliance in a service group optimizes a given new connection) on bits pulled out, or masked, from the IP address and the TCP port packet header fields. Mask assignment in RiOS v6.1 supports load-balancing across multiple active Steelhead appliance interfaces in the same service group. The default mask scheme uses an IP address mask of 0x1741, which is applicable in most situations. However, you can change the IP mask by clicking the service group ID and changing the service group settings and flags. In multiple Steelhead environments, it is often desirable to send all users in subnet range to the same Steelhead. Using mask provides a basic ability to leverage a branch subnet and Steelhead to the same Steelhead in a WCCP cluster. **Important:** If you use mask assignment you must ensure that packets on every connection and in both directions (client-to-server and server-to-client), are redirected to the same Steelhead appliance. For detailed information and best practices for using assignment schemes, see the *Steelhead Appliance Deployment Guide*.
src-ip-mask <mask>	Specify the service group source IP mask. The default value is 0x1741.
dst-ip-mask <mask>	Specify the service group destination IP mask.
src-port-mask <mask>	Specify the service group source port mask.
dst-port-mask <mask>	Specify the service group destination port mask.

Usage

WCCP must be enabled before configuring any WCCP service groups.

Follow these guidelines when configuring the weight parameter and failover support:

- To enable failover support for WCCP groups, set the **weight** parameter to **0** on the backup Steelhead appliance.
- If one Steelhead appliance has a weight 0, but another one has a non-zero weight, the Steelhead appliance with weight 0 does not receive any redirected traffic.
- To enable failover support with multi-inpath WCCP groups in RiOS v6.1, set the **weight** parameter to **0** on the backup Steelhead interface.

If one Steelhead interface has a weight 0, but another one has a non-zero weight, the Steelhead interface with weight 0 does not receive any redirected traffic.

Note: If all the Steelhead interfaces have a weight 0, the traffic is redirected equally among them.

Example

```
amnesiac (config) # wccp interface inpath0_0 service-group 61 routers 10.1.1.1,10.2.2.2
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

“show wccp” “show wccp interface service-group”

wccp mcast-ttl

Description

Sets the multicast TTL parameter for WCCP. The TTL determines the range over which a multicast packet is propagated in your intranet.

Syntax

[no] wccp mcast-ttl <value>

Parameters

<value>	Specify the multicast-TTL value.

Usage

For details about configuring WCCP, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables WCCP support.

Example

```
amnesiac (config) # wccp mcast-ttl 10
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

“show wccp”

wccp override-return route-no-gre

Description

Enables the Steelhead appliance to accept whatever return direction is negotiated, but it returns traffic by using the in-path routing table, and will not use GRE encapsulation. Typically, you use this where you have an in-path gateway, which means traffic is returned to the in-path gateway.

Syntax

[no] wccp override-return route-no-gre

Parameters

None

Usage

Typically, you configure the WCCP service group to specify either. By choosing either, the router and Steelhead appliance negotiate whether to use L2 or GRE for redirects, and separately, for returns as well. Certain platforms and I/OS's support L2 redirects to the Steelhead appliance (usually the 6500s or 7600s depending on their supervisor engine), and even fewer combinations support L2 return. (The 12.2(SXH) does support L2 return.) This command should only be used if there is an L2 hop between the Steelhead appliance and the next hop according to the routing table. For details, see the *Steelhead Appliance Deployment Guide*,

The **no** command option disables WCCP override support.

Example

```
amnesiac (config) # wccp override-return route-no-gre
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

"show wccp"

wccp override-return sticky-no-gre

Description

Enables track redirecting router for return destination and no GRE encapsulation.

Syntax

[no] wccp override-return sticky-no-gre

Parameters

None

Usage

The **no** command option disables WCCP override support.

Example

```
amnesiac (config) # wccp override-return sticky-no-gre
```

Product

Steelhead appliance, Interceptor appliance

Related Topics

"show wccp"

Simplified Routing Support Commands

This section describes the simplified routing support commands.

in-path mac-except-locl

Description

Disallows the Steelhead MAC address on the peer Steelhead appliance for simplified routing.

Syntax

[no] in-path mac-except-locl

Parameters

None

Usage

Use this command if you are using simplified routing on links where Steelhead appliances are be on the same subnet (client-side and server-side in-path addresses on the same subnet and VLAN).

When enabled, and if the peer Steelhead appliance is on the same subnet, the Steelhead appliance will not use the MAC address of the peer Steelhead appliance for any simplified routing entry except for the one corresponding to the peer Steelhead IP address.

For details, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables the in-path feature.

Example

```
amnesiac (config) # in-path mac-except-locl
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path macmap-except"

in-path mac-match-vlan

Description

Configures VLAN IDs in simplified routing table look-ups.

Syntax

[no] in-path mac-match-vlan

Parameters

None

Usage

When enabled, the Steelhead appliance tracks the VLAN ID and IP address against the MAC address. For details, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables the in-path feature.

This feature is enabled by default in RiOS v6.0 and later.

Example

```
amnesiac (config) # in-path mac-match-vlan
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path mac-match-vlan"

in-path peer-probe-cach

Description

Configures VLAN IDs in simplified routing table look-ups.

Syntax

[no] in-path peer-probe-cach

Parameters

None

Usage

In order for the Steelhead applianceto learn about the correct VLAN ID information, you must disable probe-caching. When probe-caching is disabled, the SYN packet of every connection has the probe-request attached to it (assuming the connection should be optimized based on the in-path rules).

You can turn off probe-caching on the server-side Steelhead appliance or on the client-side Steelhead appliance. The difference between the two methods is one of convenience. If there are 25 client-side Steelhead appliances and 1 server-side Steelhead appliance, it is easier to instruct the data center Steelhead appliance to inform the remote Steelhead appliances not to perform probe-caching. The alternative is to disable probe-caching on all 25 Steelhead appliances in the remote offices. Enter this command on the server-side Steelhead appliance. When enabled, the server-side Steelhead appliance instructs the client-side Steelhead appliance not to cache the probe-response.

For details, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables the in-path feature.

Example

```
amnesiac (config) # in-path peer-probe-cach
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path probe-caching"

in-path probe-caching enable

Description

Configures probe caching settings.

Syntax

[no] in-path probe-caching enable

Parameters

None

Usage

For the Steelhead appliance to learn about the correct VLAN ID information, you must disable probe-caching. When probe-caching is disabled, the SYN packet of every connection has the probe-request attached to it (assuming the connection should be optimized based on the in-path rules).

Enter this command on the client-side Steelhead appliance. This command instructs the client-side Steelhead appliance to not cache the probe-response.

For details, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables the in-path feature.

Example

```
amnesiac (config) # in-path probe-caching enable
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path probe-caching"

in-path simplified routing

Description

Enables simplified routing.

Syntax

[no] in-path simplified routing {none | all | dest-only | dest-source | mac-def-gw-only}

Parameters

none	Disables all options.
all	Collects source and destination MAC data. Also collects data for connections that are *un-natted* (connections that are not translated using NAT). This option cannot be used in connection forwarding deployments.
dest-only	Collects destination MAC data. This option can be used in connection forwarding. This option is the default setting.
dest-source	Collects destination and source MAC data. This option can be used in connection forwarding.
mac-def-gw-only	Simplified routing entries are only used when a packet is sent to the in-path default gateway. This option enables you to override any simplified routing learning by putting in static routes.

Usage

Simplified routing collects the IP address for the next hop MAC address from each packet it receives to address traffic. With simplified routing, you can use either the WAN or LAN-side device as a default gateway. The Steelhead appliance learns the right gateway to use by watching where the switch or router sends the traffic, and associating the next-hop Ethernet addresses with IP addresses. Enabling simplified routing eliminates the need to add static routes when the Steelhead appliance is in a different subnet from the client and the server.

Without simplified routing, if a Steelhead appliance is installed in a different subnet from the client or server, you must define one router as the default gateway and static routes for the other routers so that traffic is not redirected back through the Steelhead appliance. However, in some cases, even with static routes defined, the ACL on the default gateway can still drop traffic that should have gone through the other router. Enabling simplified routing eliminates this issue.

Simplified routing has the following constraints:

- WCCP cannot be enabled.
- The default route must exist on each Steelhead appliance in your network.
- Simplified routing requires a client-side and server-side Steelhead appliance.

Optionally, you can also enable enhanced autodiscovery. When you enable simplified routing, Riverbed recommends that you also enable enhanced autodiscovery because it gives the Steelhead appliance more information to associate IP addresses and MAC addresses (and potentially VLAN tags). For details, see "in-path peering auto" on page 373.

When deploying Steelhead appliances on a non-trunk link, using simplified routing is recommended but optional. However, when deploying Steelhead appliances on VLAN trunks, enabling simplified routing is mandatory. Simplified routing plays a bigger role in keeping track of the IP, VLAN ID, and MAC address for each connection. Use the **all** option to learn from both source and destination MAC addresses.

If you are installing Steelhead appliance on some type of shared L2 wan connection (local and remote in-path addresses in the same subnet, with or without VLANs):

```
in-path mac-except-locl (bug 16389)
```

If you are putting the Steelhead appliance on a simple non-VLAN trunk:

```
in-path simplified routing all
in-path peering auto <<enable the new discovery protocol>>
in-path simplified mac-def-gw-only
in-path mac-except-locl
```

If you are putting the Steelhead appliances on a VLAN trunk link:

```
in-path simplified routing all
```

```
in-path peering auto <<enable the new discovery protocol>>
in-path vlan-conn-based <<to keep LAN side traffic in its original VLAN; enabled by default>>
in-path simplified mac-def-gw-only
in-path mac-except-locl
in-path mac-match-vlan <<enabled by default>>
```

For details, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables simplified routing.

Example

```
amnesiac (config) # in-path simplified routing all
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path simplified routing"

in-path simplified mac-def-gw-only

Description

Configures VLAN IDs in simplified routing table look-ups.

Syntax

[no] in-path simplified mac-def-gw-only

Parameters

None

Usage

It might be necessary to override the information learned from the simplified routing entries. By default, simplified routing takes precedence over static routes. Use this command to change this behavior. This command instructs the Steelhead appliance to only use the simplified routing table if the packet is destined for the default gateway. If a matching static route is present, the static route entry will override the information learned from simplified routing.

The **no** command option disables the in-path feature.

Example

```
amnesiac (config) # in-path simplified mac-def-gw-only
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path macmap-tables"

Asymmetric Route Detection Commands

This section describes the asymmetric route detection commands.

in-path asym-route-tab flush

Description

Removes all entries in the asymmetric routing table.

Syntax

in-path asym-route-tab flush

Parameters

None

Usage

You can also access this command from enable mode.

Example

```
amnesiac (config) # in-path asym-route-tab flush
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path asym-route-tab"

in-path asym-route-tab remove

Description

Clears a specified single route from the asymmetric routing table.

Syntax

in-path asym-rout-tab remove <entry>

Parameters

<entry>	Specify the IP address of the asymmetric routing table entry to remove. To specify an address pair that exists in the table, use the format X.X.X.X-X.X.X.X. For example 1.1.1.1-2.2.2.2

Usage

Requires the specification of an address pair that exists in the table. For example 1.1.1.1-2.2.2.2.

You can also access this command from enable mode.

Example

```
amnesiac (config) # in-path asym-route-tab remove 1.1.1.1-2.2.2.2
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path asym-route-tab"

in-path asymmetric routing detection enable

Description

Enables asymmetric route detection. Asymmetric route detection automatically detects and reports asymmetric routing conditions and caches this information to avoid losing connectivity between a client and a server.

Syntax

[no] in-path asymmetric routing detection enable

Parameters

None

Usage

For details about asymmetric routing, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Types of asymmetry:

Complete Asymmetry - Packets traverse both Steelhead appliances going from client to server but bypass both Steelhead appliances on the return path.

- Asymmetric routing table entry: **bad RST**
- Log: `Sep 5 11:16:38 amnesiac kernel: [intercept.WARN] asymmetric routing between 10.11.111.19 and 10.11.25.23 detected (bad RST)`

Server-Side Asymmetry - Packets traverse both Steelhead appliances going from client to server but bypass the server-side Steelhead appliance on the return path.

- Asymmetric routing table entry: **bad SYN/ACK**
- Log: `Sep 7 16:17:25 amnesiac kernel: [intercept.WARN] asymmetric routing between 10.11.25.23:5001 and 10.11.111.19:33261 detected (bad SYN/ACK)`

Client-Side Asymmetry - Packets traverse both Steelhead appliances going from client to server but bypass the client-side Steelhead appliance on the return path.

- Asymmetric routing table entry: **no SYN/ACK**
- Log: `Sep 7 16:41:45 amnesiac kernel: [intercept.WARN] asymmetric routing between 10.11.111.19:33262 and 10.11.25.23:5001 detected (no SYN/ACK)`

Multi-SYN Retransmit- Probe-Filtered - Occurs when the client-side Steelhead appliance sends out multiple SYN+ frames and does not get a response.

- Asymmetric routing table entry: **probe-filtered(not-AR)**
- Log: `Sep 13 20:59:16 amnesiac kernel: [intercept.WARN] it appears as though probes from 10.11.111.19 to 10.11.25.23 are being filtered. Passing through connections between these two hosts.`

Multi-SYN Retransmit- SYN-Rexmit - Occurs when the client-side Steelhead appliance receives multiple SYN retransmits from a client and does not see a SYN/ACK packet from the destination server.

- Asymmetric routing table entry: **probe-filtered(not-AR)**
- Log: `Sep 13 20:59:16 amnesiac kernel: [intercept.WARN] it appears as though probes from 10.11.111.19 to 10.11.25.23 are being filtered. Passing through connections between these two hosts.`

You can use the following tools to detect and analyze asymmetric routes:

TCP Dump - Run a TCP dump on the client-side Steelhead appliance to verify the packet sequence that is causing the asymmetric route detection. You can take traces on the LAN and WAN ports of the Steelhead appliance and, based on the packet maps, look for the packet sequence that is expected for the type of warning message in the log. For example to obtain information on all packets on the WAN interface, sourced from or destined to 10.0.0.1, and with a source/destination TCP port of 80:

```
tcpdump -i wan0_0 host 10.0.0.1 port 80
```

You can use the following command to filter SYN, SYN/ACK, and reset packets. This command does not display the ACK packets but it can be useful if the link is saturated with traffic and the traces are filling quickly. The following command uses the **-i** parameter to specify the interface and the **-w** parameter to write to a file:

```
tcpdump -i wan1_0 'tcp[tcpflags] & (tcp-syn|tcp-fin|tcp-rst) = 0' -w lookingforasymwan
```

Trace Route - Run the trace route tool to discover what path a packet is taking from client to server and from server to client. Access the client and run the **traceroute** command with the IP address of the server, and then run the traceroute command from the server with the IP address of the client. For example for networking equipment:

```
#Client’s Address: 10.1.0.2 ..
#Server’s Address: 10.0.0.4
client# traceroute 10.0.0.4 Type escape sequence to abort.
Tracing the route to 10.0.0.4
1 10.1.0.1 4 msec 0 msec 4 msec
2 10.0.0.2 4 msec 4 msec 0 msec
3 10.0.0.3 4 msec 4 msec 0 msec
4 10.0.0.4 4 msec 4 msec 0 msec
```

```
server# traceroute 10.1.0.2 Type escape sequence to abort.
Tracing the route to 10.1.0.2
1 10.0.0.6 4 msec 0 msec 4 msec
2 10.0.0.5 4 msec 4 msec 0 msec
3 10.1.0.1 4 msec 4 msec 0 msec
4 10.1.0.2 4 msec 4 msec 0 msec
```

The **no** command option disables asymmetric route detection and caching.

Example

```
amnesiac (config) # in-path asymmetric routing detection enable
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path asym-route-tab"

in-path asymmetric routing pass-through enable

Description

Enables the pass-through feature for asymmetric routing. If disabled, asymmetrically routed TCP connections are still detected and a warning message is logged, but the connection is not passed-through and no alarm or email is sent.

Syntax

[no] in-path asymmetric routing pass-through enable

Parameters

None

Usage

Use this command to ensure connections are not passed-through the Steelhead appliances unoptimized. Logging occurs when asymmetric routes are detected.

If the system detects asymmetric routing, the pair of IP addresses, defined by the client and server addresses of the connection, is cached in the asymmetric routing cache on the Steelhead appliance. Further connections between these hosts are not optimized until that particular asymmetric routing cache entry times out.

The **no** command option disables asymmetric routing pass through.

Example

```
amnesiac (config) # no in-path asymmetric routing pass-through enable
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show in-path asym-route-tab"

in-path cdp allow-failure enable

Description

In PBR deployments with multiple in-path interfaces, this command enables Cisco Discovery Protocol (CDP) packets to be sent to the other routers when one of the routers goes down.

Syntax

[no] in-path cdp allow-failure enable

Parameters

None

Usage

With PBR, CDP is used by the Steelhead appliance to notify the router that the Steelhead appliance is still alive and that the router can still redirect packets to it.

In some cases, the you might want to disable this command so that if one router goes down, the Steelhead appliance stops sending CDP packets to all the routers it is attached to and connections are redirected and optimized by another Steelhead appliance.

This can be useful when the routers are configured to redirect to a Steelhead appliance when all routers are up but to another Steelhead appliance when one router goes down.

For details about how to configure a Steelhead appliance for PBR with CDP, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables CDP.

Example

```
amnesiac (config) # in-path cdp allow-failure enable
```

Product

Interceptor appliance, Steelhead appliance, Cloud Steelhead

Related Topics

"show in-path cdp"

in-path cdp enable

Description

Enables the asymmetric route caching and detection feature.

Syntax

[no] in-path cdp enable

Parameters

None

Usage

Enables Cisco Discovery Protocol (CDP) support in PBR deployments. Virtual in-path failover deployments require CDP on the Steelhead appliance to bypass the Steelhead appliance that is down.

CDP is a proprietary protocol used by Cisco routers and switches to obtain neighbor IP addresses, model information, IOS version, and so on. The protocol runs at the OSI layer 2 using the 802.3 Ethernet frame.

For details about how to configure a Steelhead appliance for PBR with CDP, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables CDP.

Example

```
amnesiac (config) # in-path cdp enable
```

Product

Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show in-path cdp"

in-path cdp holdtime

Description

Configures the hold-time for CDP. The hold-time period allows for a quick recovery in failover deployments with PBR and CDP.

Syntax

[no] in-path cdp holdtime <holdtime>

Parameters

<holdtime>	Specify the CDP hold-time in seconds. The default value is 5.

Usage

The **no** command option resets the CDP hold-time to the default value.

Example

```
amnesiac (config) # in-path cdp holdtime 10
```

Product

Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show in-path cdp"

in-path cdp interval

Description

Configures the refresh period for CDP. The refresh period allows for a quick recovery in failover deployments with PBR and CDP.

Syntax

[no] in-path cdp interval <seconds>

Parameters

<seconds>	Specify the CDP refresh interval in seconds. The default value is 1.

Usage

The **no** command option resets the CDP refresh period to the default value.

Example

```
amnesiac (config) # in-path cdp interval 10
```

Product

Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show in-path cdp"

Connection Forwarding

This section describes connection forwarding commands, typically used with the Interceptor appliance.

Note: To use connection forwarding with IPv6, both Steelhead appliances must be running RiOS v8.5 and you must enable multiple interface support. The control connection between neighbors is still IPv4 only.

steelhead communication ack-timer-cnt

Description

Sets the interval to wait for an acknowledgement (ACK).

Syntax

[no] steelhead communication ack-timer-cnt <integer>

Parameters

<integer>	Specify the number of intervals.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication ack-timer-cnt 5
```

Product

Steelhead appliance

Related Topics

"show in-path neighbor", "show steelhead communication"

steelhead communication ack-timer-intvl

Description

Sets the length of time to wait for an acknowledgement (ACK).

Syntax

[no] steelhead communication ack-timer-intvl <milliseconds>

Parameters

<milliseconds>	Specify the duration of the interval in milliseconds.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication ack-timer-intvl 5
```

Product

Steelhead appliance

Related Topics

"show in-path neighbor"

steelhead communication advertiseresync

Description

Re-synchronizes NAT entries if neighbor appliances go down and are restarted. If in-path0_0 went down, other in-path interfaces intercept and optimize connections, and traffic is optimized.

Syntax

[no] steelhead communication advertiseresync

Parameters

None

Usage

The Steelhead appliance allows neighbor connections from all in-path to all in-paths. When there are multiple neighbor connections from one Steelhead appliance to another, if one goes down the traffic is re-routed through the remaining in-path Steelhead appliance, and traffic continues on normally.

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication advertiseresync
```

Product

Steelhead appliance

Related Topics

"show in-path neighbor advertiseresync"

steelhead communication allow-failure

Description

Enables the Steelhead appliance to continue to optimize connections when one or more of the configured neighbors is unreachable.

Syntax

[no] steelhead communication allow-failure

Parameters

None

Usage

By default, if a Steelhead appliance loses connectivity to a connection forwarding neighbor, the Steelhead appliance stops attempting to optimize new connections. With the **steelhead communication allow-failure** command enabled the Steelhead appliance continues to optimize new connections, regardless of the state of its neighbors.

For virtual in-path deployments with multiple Steelhead appliances, including WCCP clusters, connection forwarding and the allow-failure feature must always be used. This is because certain events, such as network failures, and router or Steelhead appliance cluster changes, can cause routers to change the destination Steelhead appliance for TCP connection packets. When this happens, Steelhead appliances must be able to redirect traffic to each other to insure that optimization continues.

For parallel physical in-path deployments, where multiple paths to the WAN are covered by different Steelhead appliances, connection forwarding is needed because packets for a TCP connection might be routed asymmetrically; that is, the packets for a connection might sometimes go through one path, and other times go through another path. The Steelhead appliances on these paths must use connection forwarding to ensure that the traffic for a TCP connection is always sent to the Steelhead appliance that is performing optimization for that connection.

If the allow-failure feature is used in a parallel physical in-path deployment, Steelhead appliances only optimize those connections that are routed through the paths with operating Steelhead appliances. TCP connections that are routed across paths without Steelhead appliances (or with a failed Steelhead appliance) are detected by the asymmetric routing detection feature.

For physical in-path deployments, the allow-failure feature is commonly used with the fail-to-block feature (on supported hardware). When fail-to-block is enabled, a failed Steelhead appliance blocks traffic along its path, forcing traffic to be re-routed onto other paths (where the remaining Steelhead appliances are deployed). For details about configuring the allow-failure with the fail-to-block feature, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication allow failure
```

Product

Steelhead appliance

Related Topics

"show in-path neighbor"

steelhead communication enable

Description

Enables connection forwarding. With connection forwarding, the LAN interface forwards and receives connection forwarding packets.

Syntax

[no] steelhead communication enable

Parameters

None

Usage

You enable connection forwarding only in asymmetric networks; that is, in networks in which a client request traverses a different network path than the server response. The default port for connection forwarding is **7850**.

To optimize connections in asymmetric networks, packets traveling in both directions must pass through the same client-side and server-side Steelhead appliance. If you have one path from the client to the server and a different path from the server to the client, you need to enable in-path connection forwarding and configure the Steelhead appliances to communicate with each other. These Steelhead appliances are called neighbors and exchange connection information to redirect packets to each other. Neighbors can be placed in the same physical site or in different sites, but the latency between them should be small because the packets travelling between them are not optimized.

Important: When you define a neighbor, you specify the Steelhead appliance in-path IP address, not the primary IP address.

If there are more than two possible paths, additional Steelhead appliances must be installed on each path and configured as neighbors. Neighbors are notified in parallel so that the delay introduced at the connection set up is equal to the time it takes to get an acknowledgement from the furthest neighbor.

When you enable connection forwarding, multiple Steelhead appliances work together and share information about what connections are optimized by each Steelhead appliance. With connection forwarding, the LAN interface forwards and receives connection forwarding packets.

Steelhead appliances that are configured to use connection forwarding with each other are known as connection forwarding neighbors. If a Steelhead appliance sees a packet belonging to a connection that is optimized by a different Steelhead appliance, it forwards it to the correct Steelhead appliance. When a neighbor Steelhead appliance reaches its optimization capacity limit, that Steelhead appliance stops optimizing new connections, but continues to forward packets for TCP connections being optimized by its neighbors.

You can use connection forwarding both in physical in-path deployments and in virtual in-path deployments. In physical in-path deployments, it is used between Steelhead appliances that are deployed on separate parallel paths to the WAN. In virtual in-path deployments, it is used when the redirection mechanism does not guarantee that packets for a TCP connection are always sent to the same Steelhead appliance. This includes the WCCP protocol, a commonly used virtual in-path deployment method.

Typically, you want to configure physical in-path deployments that do not require connection forwarding. For example, if you have multiple paths to the WAN, you can use a Steelhead appliance model that supports multiple in-path interfaces, instead of using multiple Steelhead appliances with single in-path interfaces. In general, serial deployments are preferred over parallel deployments. For details about deployment best practices, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication enable
```

Product

Steelhead appliance

Related Topics

"show in-path neighbor"

steelhead communication fwd-vlan-mac

Description

Sets the VLAN and destination MAC address to be included when the packet is forwarded to a neighbor.

Syntax

[no] steelhead communication fwd-vlan-mac

Parameters

None

Usage

When you are configuring connection forwarding, this command causes the packet forwarding Steelhead appliance to include the VLAN and Ethernet header when it forwards packets to a neighbor. This feature is useful when you are using connection forwarding and VLAN transparency. For details, see the *Steelhead Appliance Deployment Guide*.

You can use this command to configure full address transparency for a VLAN when the following are true:

- you are using connection forwarding
- your Steelhead appliances are on the same Layer-2 network
- packets on your network use two different VLANs in the forward and reverse directions

You can also use this command if packets on your network use the same VLAN in the forward and reverse directions and you do not want to maintain network asymmetry.

The **no** command option disables VLAN and destination MAC address forwarding**.**

Example

```
amnesiac (config) # steelhead communication fwd-vlan-mac
```

Product

Steelhead appliance

Related Topics

"show in-path neighbor"

steelhead communication heartbeat enable

Description

Configures the Steelhead appliance communication heartbeat settings.

Syntax

[no] steelhead communication heartbeat enable

Parameters

None

Usage

When this command is enabled, the connection forwarding neighbors are sending heartbeat messages to each other periodically. A heartbeat message is a repeating signal from one appliance to another to indicate that the appliance is operating.

The **no** command option disables the heartbeat settings.

Example

```
amnesiac (config) # steelhead communication heartbeat enable
```

Product

Steelhead appliance

Related Topics

"show in-path neighbor"

steelhead communication keepalive count

Description

Sets the keep-alive messages before terminating connections with the neighbor Steelhead appliance for TCP connection forwarding.

Syntax

[no] steelhead communication keepalive count <count>

Parameters

<count>	Specify the number of keep-alive messages. The default value is 3.

Usage

The **no** command option resets the count to the default value.

Example

```
amnesiac (config) # steelhead communication keepalive count 10
```

Product

Steelhead appliance

Related Topics

"show in-path neighbor"

steelhead communication keepalive interval

Description

Sets the time interval between keep-alive messages with the neighbor Steelhead appliance for connection forwarding.

Syntax

[no] steelhead communication keepalive interval <seconds>

Parameters

<seconds>	Specify the number of seconds between keep-alive messages. The default value is 1.

Usage

The **no** command option resets the interval to the default.

Example

```
amnesiac (config) # steelhead communication keepalive interval 15
```

Product

Steelhead appliance

Related Topics

"show in-path neighbor"

steelhead communication multi-interface enable

Description

Enables multiple interface support. Typically, this feature is used with the Interceptor appliance.

Syntax

[no] steelhead communication multi-interface enable

Parameters

None

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication multi-interface enable
```

Product

Steelhead appliance

Related Topics

"show in-path neighbor"

steelhead communication port

Description

Sets the neighbor port for the Steelhead appliance in connection forwarding deployments.

Syntax

[no] steelhead communication port <port>

Parameters

<port>	Specify the connection forwarding port for the neighbor. The default value is 7850.

Usage

The **no** command option resets the port to the default.

Example

```
amnesiac (config) # steelhead communication port 2380
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path neighbor"

steelhead communication read-timeout

Description

Sets the response wait time.

Syntax

[no] steelhead communication read-timeout <milliseconds>

Parameters

<milliseconds>	Specify the length of the interval in milliseconds.

Usage

The **no** command option disables this option.

Example

```
amnesiac (config) # steelhead communication read-timeout 10
```

Product

Steelhead appliance

Related Topics

"show in-path neighbor"

steelhead communication recon-timeout

Description

Sets the reconnect response wait time.

Syntax

[no] steelhead communication recon-timeout <milliseconds>

Parameters

<milliseconds>	Specify the length of the interval in milliseconds.

Usage

The **no** command option disables this option.

Example

```
amnesiac (config) # steelhead communication recon-timeout 40
```

Product

Steelhead appliance

Related Topics

"show in-path neighbor"

steelhead name

Description

Configures connection forwarding neighbors.

Syntax

[no] steelhead name <name> {main-ip <ip-addr> [port <port>] | additional-ip <ip-addr>}

Parameters

<name>	Specify the hostname of the neighbor appliance.
main-ip <ip-addr>	Specify the main connection forwarding IP address of the neighbor.
port <port>	Optionally, specify the connection forwarding port of the neighbor.
additional-ip <ip-addr>	Specify an additional connection forwarding IP address for the neighbors.

Usage

For details about configuring connection forwarding, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables the neighbor.

Example

```
amnesiac (config) # steelhead name test main-ip 10.0.0.1 port 1234
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path neighbor"

in-path send-storeid enable

Description

Creates a table of data store IDs; typically used with the Interceptor appliance

Syntax

[no] in-path send-storeid enable

Parameters

None

Usage

Each time the Interceptor appliance receives a connection it forwards it to the appropriate Steelhead appliance.

The **no** command option disables this option.

Example

```
amnesiac (config) # in-path send-storeid enable
```

Product

Steelhead appliance, CSH

Related Topics

"show in-path neighbor"

Subnet-Side Rule Commands

This section describes the subnet-side rule commands. For details, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

subnet side add rule

Description

Adds a rule to the subnet map table.

Syntax

subnet side add rule index <rulenum> network <network prefix> is [lan | wan]

Parameters

index <rulenum>	Select **Start**, **End**, or a rule number. Steelhead appliances evaluate rules in numerical order starting with rule **1**. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule **2** is consulted. If rule **2** matches the conditions, it is applied, and no further rules are consulted. The type of a matching rule determines which action the Steelhead appliancee takes on the connection.
network <network prefix>	Specify the subnet. Use the format **<IP address>/<subnet mask>.**
lan | wan	Specify whether the addresses on the subnet are LAN or WAN. In virtual in-path configurations, all traffic is flowing in and out of one physical interface.

Usage

You configure subnet side rules to support RSP (VRSP) and Flow Export on a virtual in-path deployment.

Subnet side rules let you configure subnets as LAN-side subnets or WAN-side subnets for a virtual in-path Steelhead appliance. The subnet side rules determine whether traffic originated from the LAN or the WAN-side of the Steelhead appliance based on the source subnet. You must configure subnets on each Steelhead appliance in a virtual in-path configuration, as the subnets for each will likely be unique.

With subnet side rules in place, RiOS can send incoming packets to the correct RSP VNIs for VRSP, and a virtual in-path Steelhead can use flow export collectors such as NetFlow to analyze non-optimized or passed through traffic correctly. Otherwise, the Steelhead appliance cannot discern whether the traffic is traveling from the LAN to the WAN or in the opposite direction. This can result in over-reporting traffic in a particular direction or for a particular interface.

Before you use virtual RSP, you must disable simplified routing.

For details on virtual RSP, see "rsp enable" on page 640 and the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # subnet side add rule index 4 network 16 lan
```

Product

Steelhead appliance, CSH

Related Topics

"show subnet side rules"

subnet side delete rule

Description

Deletes a subnet-side rule.

Syntax

subnet side delete rule <rulenum>

Parameters

<rulenum>	Specify the rule number to delete.

Example

```
amnesiac (config) # subnet side delete rule 4
```

Product

Steelhead appliance, CSH

Related Topics

"show subnet side rules"

subnet side move rule

Description

Moves a subnet-side rule.

Syntax

subnet side move rule from <rulenum> to <rulenum>

Parameters

<rulenum>	Specify the rule number to move.

Usage

The subnet-side rules determine whether traffic originated from the LAN or the WAN side of the Steelhead appliance based on the source subnet. With subnet-side rules in place, RiOS can send incoming packets to the correct RSP VNIs, and data flow analyzers can analyze traffic correctly.

Example

```
amnesiac (config) # subnet side move rule from 4 to 3
```

Product

Steelhead appliance, CSH

Related Topics

"show subnet side rules"

Data Flow Support Commands

This section describes the data flow analyzer support commands.

ip flow-export destination

Description

Configures data flow support. Data flow support enables you to collect traffic flow data.

Syntax

[no] ip flow-export destination <collector ip> <collector port> [export-port {aux | primary}] | [filter ip <cr>] | [netmask <netmask> | port <port>] | [filter-enable] | [template refresh-rate <packets>] | [template-timeout-rate <minutes>] | [version <version>] |interface {<interface> | capture [all | optimized | passthrough] | lan-addrs [off | on]}

Parameters

<collector ip> <collector port>	Specify the export IP address and port the data flow collector is listening on. The default value is 2055.
export-port {**aux** | **primary**}	Specify the interface used to send data flow packets to the collector.
filter ip <ip-addr> <cr> | **netmask <netmask>** | **port <port>**	Specify the IP address for filter rules. Optionally, you can configure the netmask or port.
filter-enable	Specify to enable filters on the specified collector.
interface {**<interface>** | **capture all** | **optimized** | **passthrough**	Specify the interface used to capture packets. The data flow collector records sent from the Steelhead appliance appear to be sent from the IP address of the selected interface. Optionally, specify capture to configure the type of traffic to capture
capture [all | **optimized** | **passthrough]**	Specify the type of traffic to capture: Specify the traffic type to export to the flow collector. Select one of the following types from the drop-down list: • **all** - Exports both optimized and non-optimized traffic. • **optimized** - Exports optimized traffic. • **optimized** - Exports optimized LAN or WAN traffic when WCCP is enabled.
lan-addrs {**off** | **on**}	Specify whether the TCP IP addresses and ports reported for optimized flows should contain the original client and server IP addresses and not those of the Steelhead appliance: **off** displays the Steelhead appliance information; **on** displays the LAN address information. The default is to display the IP addresses of the original client and server without the IP address of the Steelhead appliances. **Note:** This option is not applicable to collector v9.
template refresh-rate <packets>	Specify the number of packets sent after which templates are resent. Applicable only to collector v9.
template-timeout-rate <minutes>	Specify the duration after which templates are resent. Applicable only to collector v9.
version <CascadeFlow | **Cascade-comp** | **Netflow-v5** | **Netflow-v9>**	Specify the data flow collector version: • **CascadeFlow** - Specifies Cascade v8.4 or later. • **Cascade-comp** - Specifies Cascade v8.34 or earlier. • **Netflow-v5** - Enables ingress flow records (Collector v5). • **Netflow-v9** - Enables ingress and egress flow records (Collector v9). The **CascadeFlow** and **CascadeFlow-comp** options are enhanced versions of flow export to Riverbed Cascade. These versions allow automatic discovery and interface grouping for Steelhead appliances in the Riverbed Cascade Profiler or Cascade Gateway and support WAN and optimization reports in Cascade. For details, see the *Cascade Profiler User Manual* and the *Cascade Gateway User Manual*.

Usage

Before you enable data flow support in your network, you should consider the following:

- Generating data-flow data can utilize large amounts of bandwidth, especially on low bandwidth links, thereby impacting Steelhead appliance performance.
- You can reduce the amount of data exported by data flow collectors if you export only optimized traffic.
- Data flow only tracks incoming packets (ingress). For collector v9 egress flows are also tracked always

To troubleshoot your flow export settings:

- Make sure the port configuration matches on the Steelhead appliance and the listening port of the collector.
- Ensure that you can reach the collector from the Steelhead appliance (for example, ping 1.1.1.1 where 1.1.1.1 is the NetFlow collector).
- Verify that your capture settings are on the correct interface and that traffic is flowing through it.

```
amnesiac (config) # ip flow-export enable
amnesiac (config) # ip flow-export destination 10.2.2.2 2055 interface wan0_0
capture optimized
amnesiac (config) # ip flow-export destination 10.2.2.2 2055 export-port
primary
amnesiac (config) # ip flow-export destination 10.2.2.2 2055 lan-addrs on
amnesiac (config) # show ip flow-export
```

Prior to Netflow v9, for virtual in-path deployments, because the traffic is arriving and leaving from the same WAN interface, when the Steelhead appliance exports data to a NetFlow collector, all traffic has the WAN interface index. This is the correct behavior because the input interface is the same as the output interface. For Netflow v9, LAN and WAN interfaces are reported for optimized flows.

For details, see the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # ip flow-export destination 10.2.2.2 2055 interface lan0_0
capture all
amnesiac (config) # ip flow-export destination 10.2.2.2 2055 export-port aux
amnesiac (config) # ip flow-export destination 10.2.2.2 2055 lan-addrs off
```

Product

Steelhead appliance, CSH

Related Topics

"show ip"

ip flow-export enable

Description

Enables data flow support.

Syntax

[no] ip flow-export enable

Parameters

None

Usage

Flow export enables you to export network statistics to external collectors that provide information about network data flows such as the top users, peak usage times, traffic accounting, security, and traffic routing. You can export pre-optimization and post-optimization data to an external collector. The Top Talkers feature enables a report that details the hosts, applications, and host and application pairs that are either sending or receiving the most data on the network. Top Talkers does not use a NetFlow Collector.

Steelhead appliances support NetFlow v5.0, CascadeFlow, NetFlow v9, and CascadeFlow-compatible. For details on NetFlow, including Riverbed-specific record flow fields for v9, see the *Steelhead Appliance Deployment Guide*.

Flow export requires the following components:

- **Exporter** - When you enable flow export support, the Steelhead appliance exports data about flows through the network.
- **Collector** - A server or appliance designed to aggregate data sent to it by the Steelhead appliance.

- **Analyzer** - A collection of tools used to analyze the data and provide relevant data summaries and graphs. NetFlow analyzers are available for free or from commercial sources. Analyzers are often provided in conjunction with the collectors.

Before you enable flow export in your network, consider the following:

- Flow data typically consumes less than 1% of link bandwidth. Care should be taken on low bandwidth links to ensure that flow export does not consume too much bandwidth and thereby impact application performance.
- You can reduce the amount of bandwidth consumption by applying filters that only export the most critical information needed for your reports.

For virtual in-path deployments such as WCCP or PBR, because the traffic is arriving and leaving from the same WAN interface, when the Steelhead appliance exports data to a flow export collector, all traffic has the WAN interface index. This is the correct behavior because the input interface is the same as the output interface.

Prior to Netflow v9, for virtual in-path deployments, because the traffic is arriving and leaving from the same WAN interface, when the Steelhead appliance exports data to a NetFlow collector, all traffic has the WAN interface index. This is the correct behavior because the input interface is the same as the output interface. For Netflow v9, LAN and WAN interfaces are reported for optimized flows.

The **no** command option disables data flow export support.

Example

```
amnesiac (config) # ip flow-export enable
```

Product

Steelhead appliance, CSH

Related Topics

"show ip"

ip flow-export qos-dpi enable

Description

Enables the Steelhead appliance to export QoS and application statistics about individual flows to a CascadeFlow Collector.

Syntax

[no] ip flow-export qos-dpi enable

Parameters

None

Usage

Cascade appliances provide central reporting capabilities. The Steelhead appliance sends the Cascade appliances an enhanced version of NetFlow called CascadeFlow. These Netflow records are exported from the Steelhead appliance to a CascadeFlow collector and contain DSCP marking information, the DPI application ID, and QoS class ID. CascadeFlow collectors can aggregate information about QoS configuration and other application statistics to send to a Cascade Enterprise Profiler appliance.

You must enable outbound QoS on the Steelhead appliance, add a CascadeFlow collector, and enable REST API access before sending QoS configuration statistics to an Enterprise Profiler.

For details, see the *Steelhead Appliance Management Console User's Guide* and the *Riverbed Cascade Appliances Deployment Guide*.

Example

```
amnesiac (config) # ip flow-export qos-dpi enable
```

Product

Steelhead appliance

Related Topics

"papi rest access_code generate," "papi rest access_code import," "show ip"

ip flow-setting active_to

Description

Sets length of time the collector retains a list of active flows.

Syntax

[no] ip flow-setting active_to <seconds>

Parameters

<seconds>	Specify the length of life for active flows. The default value is 1800 seconds. Enabling Top Talkers automatically sets the time-out period to 60 seconds and disables this option.

Usage

The **no** command option disables the interval.

Example

```
amnesiac (config) # ip flow-setting active_to 10
```

Product

Steelhead appliance, CSH

Related Topics

"show ip"

ip flow-setting inactive_to

Description

Sets length of time the collector retains a list of inactive flows.

Syntax

[no] ip flow-setting inactive to <seconds>

Parameters

<seconds>	Optionally, specify the amount of time, in seconds, the collector retains the list of inactive traffic flows. The default value is 15 seconds.

Usage

The **no** command option disables the interval.

Example

```
amnesiac (config) # ip flow-setting inactive_to 10
```

Product

Steelhead appliance, CSH

Related Topics

"show ip"

ip flow-setting max-pkt-size

Description

Sets the maximum packet size.

Syntax

[no] ip flow-setting max-pkt-size <rate>

Parameters

<rate>	Specify the maximum packet rate. The value must be between 1500 and 40000.

Usage

The **no** command option disables the interval.

Example

```
amnesiac (config) # ip flow-setting max-pkt-size 2000
```

Product

Steelhead appliance, CSH

Related Topics

"show ip"

Top Talkers Commands

This sections describes Top Talkers commands.

stats settings top-talkers enable

Description

Enables Top Talkers statistics for most active traffic flows. A traffic flow consists of data sent and received from a single source IP address and port number to a single destination IP address and port number over the same protocol.

Syntax

stats settings top-talkers enable

Parameters

None

Usage

A traffic flow consists of data sent and received from a single source IP address and port number to a single destination IP address and port number over the same protocol. The most active, heaviest users of WAN bandwidth are called the *Top Talkers*. A flow collector identifies the top consumers of the available WAN capacity (the top 50 by default) and displays them in the Top Talkers report. Collecting statistics on the Top Talkers provides visibility into WAN traffic without applying an in-path rule to enable a WAN visibility mode.

You can analyze the Top Talkers for accounting, security, troubleshooting, and capacity planning purposes. You can also export the complete list in CSV format.

The collector gathers statistics on the Top Talkers based on the proportion of WAN bandwidth consumed by the top hosts, applications, and host and application pair conversations. The statistics track pass-through or optimized traffic, or both. Data includes TCP or UDP traffic, or both (configurable on the Top Talkers report page).

You must enable Flow Export before you enable Top Talkers.

A NetFlow collector is not required for this feature.

Enabling Top Talkers automatically sets the Active Flow Timeout to 60 seconds.

You must enable Netflow Export ("ip flow-export enable") before you enable Top Talkers.

Enabling Top Talkers automatically sets the Active Flow Timeout ("ip flow-setting active_to") to 60 seconds.

The **no** command option disables this feature.

Example

```
amnesiac (config) # stats settings top-talkers enable
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show stats top-talkers"

stats settings top-talkers interval

Description

Enables Top Talkers collection period.

Syntax

stats settings top-talkers interval <interval>

Parameters

interval <hours>	Specify the interval: 24 or 48 hours.

Usage

Optionally, specify a time period to adjust the collection interval:

- **24-hour Report Period** - For a five-minute granularity (the default setting).
- **48-hour Report Period** - For a ten-minute granularity.

Example

```
amnesiac (config) # stats settings top-talkers interval 24
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show stats top-talkers"

Path Selection Commands

This section describes the path selection commands. Path selection refers to the ability to choose the best or most appropriate predefined WAN gateway for certain traffic flows in real-time, based on availability. A common use of path selection is to route voice and video over an expensive, high-quality MPLS link, while offloading less time-sensitive business traffic over a less expensive Internet VPN link. This solution provides the right performance levels for your applications and saves on bandwidth costs by optimizing the use of available bandwidth.

Path selection works independently of the Steelhead appliance optimization service and functions even if you pause the optimization service or if the optimization service becomes unavailable.

path-selection enable

Description

Enables the path selection feature.

Syntax

[no] path-selection enable

Parameters

None

Usage

Using the path selection feature, you can select a path for certain traffic flows based on the state of the links and your network configuration. At a high level, you can configure multiple paths for each connection by specifying rules based on various parameters. The Steelhead appliance monitors the state of the path and, based on this, selects the appropriate path for a packet. Selecting appropriate paths for packets provides more control over network link use.

Path selection interacts with QoS functionality to classify traffic and steer flows of specific applications over a path. You create or modify a QoS traffic rule with path information.

When a path fails, the Steelhead appliance directs traffic through another available path. When the original path comes back up, the Steelhead appliance redirects the traffic back to it.

Path selection is a transparent operation to the client, server, and any networking devices such as routers or switches. When path selection is enabled, it takes effect for new flows but not for pre-existing flows.

Path selection is disabled by default. Use the **no** version of the command to disable path selection if it has been enabled. Path selection does not require a service restart.

For details about the path selection feature, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # path-selection enable
```

Product

Steelhead appliance

Related Topics

"show path-selection settings"

path-selection path

Description

Configures settings for the path selection feature.

Syntax

[no] path-selection path <path-name> remote-ip <ipv4-address> [gateway-ip <ipv4-address>] interface <interface-name> [probe-dscp <dscp>] [probe-timeout <seconds>] [num-lost-probes <number>]

Parameters

path <path-name>	Specify the path name. The "*" character is not allowed in the path name. You can define up to three paths per traffic flow in priority order: a primary, a secondary, and a tertiary path.
remote-ip <ipv4-address>	Specify the IPv4 address of the remote endpoint to monitor with ICMP pings.
gateway-ip <ipv4-address>	Specify the next-hop gateway IPv4 address for the path.
interface <interface-name>	Specify the interface name over which the path is reached.
probe-dscp <dscp>	Specify the DSCP value (**0-63**) for the path monitoring probes.
probe-timeout <seconds>	Specify the time to wait for a probe response, in seconds, before a probe is considered lost. The default timeout value is 2 seconds.
probe-threshold <number>	Specify the number of timed-out probes before an up path is considered down or the number of received probes before a down path is considered up. The default is three probes.

Usage

When path selection is enabled, it takes effect for new flows but not for pre-existing flows.

You can configure a maximum of 1024 paths per Steelhead appliance.

You can define a path by the interface that the packet is sent out on, and you can enforce the next hop downstream router for that packet or a path based on the DSCP mark on the packet. For each application, you can also specify parameters to monitor path availability. If one path fails, the Steelhead appliance directs traffic through the next available path. When the original path comes back up, the Steelhead appliance redirects the traffic back to it.

Path selection uses ICMP pings to monitor the path state dynamically, on a regular schedule (the default is 2 seconds). If the ping responses do not make it back within the probe timeout, the probe is considered lost. If the system loses the number of probes defined by the probe threshold, it considers the path to be down and triggers an alarm, indicating that the path is unavailable.

You prioritize the path in basic or advanced outbound QoS. For basic outbound QoS, you can specify up to three paths in order of priority per application and a DSCP mark for each application. For advanced outbound QoS, apply the path selection settings to a QoS rule rather than an application. You can specify up to three paths per rule and three DSCP values.

For details about the path selection feature, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # path-selection path primary remote-ip 10.1.1.1 gateway-ip 10.2.1.1 interface
inpath0_0 probe-dscp 10 probe-timeout 8 probe-threshold 4
```

```
amnesiac (config) # path-selection path secondary remote-ip 10.1.1.1 gateway-ip 10.3.1.1 interface
inpath0_1  probe-dscp 11 probe-timeout 8 probe-threshold 4
```

Product

Steelhead appliance

Related Topics

"path-selection enable,""path-selection edit path,""qos basic classification global-app add," "qos basic classification global-app edit," "qos classification rule,""qos classification site add,""qos classification site edit,""show path-selection settings"

path-selection edit path

Description

Edits the configuration settings for the path selection feature.

Syntax

[no] path-selection edit path <path-name> [new-path-name <new-path-name>] [remote-ip <ipv4-address>] [gateway-ip <ipv4-address>] [interface <interface-name>] [probe-dscp <dscp>] [probe-timeout <seconds>] [probe-threshold <number>]

Parameters

path <path-name>	Specify the path name.
new-path <new-path-name>	Specify the new path name.
remote-ip <ipv4-address>	Specify the IPv4 address of the remote endpoint to monitor with ICMP pings.
gateway-ip <ipv4-address>	Specify the next hop gateway IPv4 address for the path.
interface <interface-name>	Specify the interface name over which the path is reached.
probe-dscp <dscp>	Specify the DSCP value for the probes.
probe-timeout <seconds>	Specify the time to wait for a probe response, in seconds, before a probe is considered lost. The default timeout value is 6 seconds.
probe-threshold <number>	Specify the number of timed-out probes before an up path is considered down or the number of received probes before a down path is considered up. The default is three probes.

Usage

When path selection is enabled, it takes effect for new flows but not for pre-existing flows.

For details about the path selection feature, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # path-selection edit path primary probe-timeout 2
```

Product

Steelhead appliance

Related Topics

"qos basic classification global-app add," "qos basic classification global-app edit," "qos classification rule," "path-selection path," "show path-selection settings"

path-selection settings bypass non-local-trpy enable

Description

Enables the bypass of non-local transparency mode packets.

Syntax

[no] path-selection settings bypass non-local-trpy enable

Parameters

None

Usage

If you are using the full transparency WAN visibility mode in a dual serial Steelhead appliance deployment, configure the **path-selection settings bypass non-local-trpy enable** command on the second Steelhead appliance referred to as the middle file engine (MFE). See the *Steelhead Appliance Deployment Guide* for more information.

This command is disabled by default.

Example

```
amnesiac (config) # path-selection settings bypass non-local-tryp enable
```

Product

Steelhead appliance

Related Topics

"path-selection enable,""path-selection path," "show path-selection settings"

path-selection settings path-reflect conn-setup enable

Description

Enables path reflection for an optimized connection set up.

Syntax

[no] path-selection settings path-reflect conn-setup enable

Parameters

None

Usage

This command enables the system to attempt to send connection setup packets back on the same path on which the last packet was received. This behavior is useful on the server-side Steelhead appliance because connection setup packets are sent before classification occurs.

This command is enabled by default.

Example

```
amnesiac (config) # path-selection settings path-reflect conn-setup enable
```

Product

Steelhead appliance

Related Topics

"qos basic classification global-app add," "qos basic classification global-app edit," "qos classification rule," "path-selection path," "show path-selection settings"

path-selection settings path-reflect probe enable

Description

Enables path reflection for probe responses.

Syntax

[no] path-selection settings path-reflect probe enable

Parameters

None

Usage

This command enables the system to attempt to send probe responses back on the same path on which the last probe was received. This behavior is useful on the server-side Steelhead appliance because probe responses are sent before classification occurs.

This command is enabled by default.

Example

```
amnesiac (config) # path-selection settings path-reflect probe enable
```

Product

Steelhead appliance

Related Topics

"qos classification rule," "path-selection path," "show path-selection settings"

path-selection settings probe ricochet

Description

Configures path monitoring settings to probe for ricochet behavior.

Syntax

[no] path-selection settings probe ricochet <learn>

Parameters

<learn>	• **on-any** - Specify to learn from all WAN egress probe requests on any in-path interface. • **first-on-any -** Specify to learn from the first WAN egress probe request on any in-path interface. • **first-on-cfg -** Specify to learn from the first WAN egress probe request on the configured in-path interface.

Usage

Path selection does not handle the ricochet of probe packets across relay interfaces.

Example

```
amnesiac (config) # path-selection settings probe ricochet on-any
```

Product

Steelhead appliance

Related Topics

"path-selection path," "show path-selection settings"

QoS Support Commands

This section describes the Quality of Service support commands. RiOS supports flat and hierarchical outbound QoS. There is no support for hierarchical QoS in inbound QoS.

For details about QoS features and limitations, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

- "QoS Platform Family Recommendations" on page 457
- "Basic and Advanced Outbound QoS Overview" on page 457
- "Inbound QoS Overview" on page 457
- "QoS Migration Commands" on page 457
- "Basic Outbound QoS Commands" on page 458
- "Advanced Outbound QoS Commands" on page 477
- "Inbound QoS Commands" on page 491
- "DSCP QoS Commands" on page 496

QoS Platform Family Recommendations

With the introduction of the Steelhead appliance CX *xx*55 and EX *xx*60 platform families, outbound QoS has maximum configurable bandwidth limits for root bandwidth. The QoS bandwidth limits are in place globally across all WAN interfaces.

Riverbed recommends the maximum classes, rules, and sites to use per Steelhead appliance model for optimal performance and to avoid delays while changing the QoS configuration. For details about these QoS configuration recommendations, see the *Steelhead Appliance Management Console User's Guide* for Steelhead CX and the *Steelhead EX Management Console User's Guide* for Steelhead EX.

Basic and Advanced Outbound QoS Overview

RiOS version 6.5 and later provides two types of QoS outbound configurations: basic and advanced. The QoS configuration you implement depends on how much classification and shaping your network traffic requires and whether you are migrating from a previous RiOS version or configuring QoS on a Steelhead appliance for the first time. Advanced outbound QoS supports different bandwidths for different interfaces. Basic outbound QoS does not support this capability, but you can specify the remote site absolute bandwidth.

A new Steelhead appliance or a Steelhead appliance with no QoS configuration upgraded to RiOS version 6.5 or later is configured with basic outbound QoS by default. If QoS was configured prior to upgrading to RiOS version 6.5 or later, the Steelhead appliance will be configured with advanced outbound QoS and existing QoS settings are preserved after the upgrade.

CLI commands for basic outbound QoS begin with *qos basic classification*; for example, **qos basic classification site add site-name**. CLI commands for advanced outbound QoS begin with *qos classification* or *qos shaping*; for example, **qos classification site edit site-name** or **qos shaping interface**.

Inbound QoS Overview

RiOS v7.0.1 introduces inbound QoS. In certain environments, running outbound QoS on a Steelhead appliance placed close to the traffic source is not sufficient to meet QoS requirements for optimal performance. Inbound QoS controls and prioritizes traffic flowing into the Steelhead appliance from the WAN network. Inbound QoS includes support to shape inbound application flows and provides the ability to slow down TCP traffic by application to allow critical traffic to get through.

CLI commands for inbound QoS begin with *qos inbound*. For example, **qos inbound class** or **qos inbound enable**.

QoS Migration Commands

To move from basic outbound QoS to advanced outbound QoS using the command-line interface, use the command, "qos migrate basic-to-adv". To move from advanced outbound QoS to basic outbound QoS, use, "qos migrate adv-to-basic".

If you move from advanced outbound QoS to basic outbound QoS all QoS settings are removed. If you move from basic outbound QoS to advanced outbound QoS your settings are preserved. If you return to basic outbound QoS, those settings are removed.

qos migrate basic-to-adv

Description

Configures advanced QoS mode on a Steelhead appliance currently in basic QoS mode.

Syntax

qos migrate basic-to-adv <confirm>

Parameters

<confirm>	Confirm migration from Basic to Advanced mode. All QoS settings will be deleted.

Usage

You must enter this command without the confirm option and then, within 10 seconds, enter the command again, with the confirm option.

All QoS settings are lost when migrating from one QoS mode to another.

Example

```
amnesiac (config) # qos migrate basic-to-adv
Proceeding with this action will result in a loss of *all* QoS settings. Please
re-run with the "confirm" keyword within 10 seconds to confirm this action.
amnesiac (config) # qos migrate basic-to-adv confirm
```

Product

Steelhead appliance

Related Topics

"show qos classification"

qos migrate adv-to-basic

Description

Configures basic QoS mode on a Steelhead appliance currently in advanced QoS mode.

Syntax

qos migrate adv-to-basic <confirm>}

Parameters

<confirm>	Confirm migration from Advanced to Basic mode. All QoS settings will be deleted.

Usage

You must enter this command without the confirm option and then, within 10 seconds, enter the command again, with the confirm option.

All QoS settings are lost when migrating from one QoS mode to another.

Example

```
amnesiac (config) # qos migrate adv-to-basic
Proceeding with this action will result in a loss of *all* QoS settings. Please
 re-run with the "confirm" keyword within 10 seconds to confirm this action.
amnesiac (config) # qos migrate adv-to-basic confirm
```

Product

Steelhead appliance

Related Topics

"show qos classification"

Basic Outbound QoS Commands

Use basic outbound QoS when you:

- currently do not have RiOS QoS configured.

- are currently using RiOS v6.1.x or earlier QoS but are willing to consolidate and reconfigure your existing rules. The existing configuration is lost when you switch from advanced to basic outbound QoS.
- do not need more granular control and can use the default settings.

qos basic classification global-app add

Description

Adds QoS classification rule for the specified global application. These site rules apply to every site.

Syntax

[no] qos basic classification global-app add global-app-name <name> class-name {realtime |interactive | business-critical |normal| low-priority |best-effort} [dscp <dscp level>] [protocol {all | gre | icmp |ipsec | tcp | udp}] [vlan <vlan>] [traffic-type {all |optimized |passthrough}] [srcnet {<subnet/mask> | <host_label>}] [srcport <port>] [dstnet {<subnet/mask> | <host_label>}] [dstport <port>] [l7protocol <protocol>] [domain-name <name>] [relative-path <path>] [out-dscp <out-dscp-value>] [path-1 <path-1-name>] [path-1-dscp <dscp>] [path-2 <path-2-name>] [path-2-dscp <dscp>] [path-3 <path-3-name>] [path-3-dscp <dscp>] [default-path {relay | drop}] [description <description>] [index <number>]

Parameters

global-app-name <name>	Specify the name of the global application. To view the predefined global application list, go to: http://www.riverbed.com/us/products/technology/riverbed_classification_qos_engine.php
class-name <class>	Specify the class that applies to the global application. If the rule matches, the specified rule sends the packet to this class. • **realtime**- Specify a real-time traffic class. Traffic that is your highest priority should be given this value, for example, VoIP, video conferencing. • **interactive** - Specify an interactive traffic class. For example, Citrix, RDP, telnet and ssh. • **business-critical** - Specify the business critical traffic class. For example, Thick Client Applications, ERPs, and CRMs • **normal** - Specify a normal priority traffic class. For example, Internet browsing, file sharing, and email. • **low-priority** - Specify a low priority traffic class. For example, FTP, backup, replication, other high-throughput data transfers, and recreational applications such as audio file sharing. • **best-effort** - Specify the lowest priority.
dscp <dscp level>	Optionally, specify a DSCP level (**0-63**). Use this option to configure a QoS rule matching a specific DSCP mark.
protocol {all | gre | icmp |ipsec | tcp | udp}	Optionally, specify the protocol for the rule. The default value is **all**.
vlan <vlan>	Optionally, specify the VLAN tag ID.
traffic-type {all | optimized | passthrough}	Specify the type of traffic. QoS rules are applied to optimized and pass-through (egress only) traffic.
srcnet <subnet/mask> |<host_label> | srcport <port>	Optionally, specify the source network subnet and mask, host label, or port. Use the format XXX.XXX.XXX.XXX/XX for subnet and mask. The default value for port is **all**. Host labels are names given to lists of hosts (IP addresses, IP subnets, and hostnames). You configure a host label using the **host-label** command.
dstnet <subnet/mask> |<host_label> | srcport <port>	Optionally, specify the destination network subnet and mask, host label, or port. Use the format XXX.XXX.XXX.XXX/XX for subnet and mask. The default value for port is **all**. Host labels are names given to lists of hosts (IP addresses, IP subnets, and hostnames). You configure a host label using the **host-label** command.
l7protocol <protocol>	Specify a protocol name Enable a protocol for classification rules. The application priority separates low-priority traffic (such as print jobs) from high-priority traffic (such as interactive screen updates). The upper bandwidth limit is defined at 100%, so that the lower priority classes can use the full bandwidth when it is available.
domain-name <name>	Specify a domain name. Only valid if you specify the **l7protocol HTTP** option.
relative-path <path>	Specify a relative path. For example, the relative path for `www.riverbed.com/appliance/commandline` would be `/appliance/commandline`. Only valid if you specify the **l7protocol** protocol **HTTP**. The relative path is the part of the URL that follows the domain name.

out-dscp <out-dscp-value>	Optionally, specify the QoS class outbound DSCP marking value. The outbound DSCP marking values are **0-63**, or **255** (reflect), or **254** (inherit from class). Reflect is the default setting for a service class. Reflect means that the DSCP level or IP ToS value found on pass-through traffic is unchanged when it passes through the Steelhead appliance.
path-1-path <path-1-name> | path-2-path <path-2-name> | path-3-path <path-3-name>	Specify the path name. Configure the available paths in the network using the **path-selection path** command.
path-1-dscp <dscp> | path-2-dscp <dscp> | path-3-dscp <dscp>	Optionally, specify the DSCP value associated with a path. The DSCP marking values are **0-63** and **253** (inherit from rule). Specifying a DSCP value for a path is used for Policy-Based Routing (PBR) use cases. For details about PBR and path selection, see the *Steelhead Appliance Deployment Guide* and *Steelhead Appliance Management Console User's Guide*. If you need to use the **255** (reflect) DSCP value for a path, specify it in the **out-dscp <out-dscp-value>** parameter and use **253** (inherit from rule) as the path DSCP value.
default-path {relay | drop}	Specify the default path-selection action for the rule if the rule is matched and all specified paths are down: • **relay** - Route packets normally using the default path. If not configured, the default behavior is relay without applying path selection. • **drop -** Drop the connection.
description <description>	Specify a description.
index <number>	Rank in QoS index.

Usage

Global applications are applications the Application Flow Engine can recognize and classify. Each global application is associated with a default QoS class. You can change the class with which a global application is associated using the **class-name** parameter.

You can display a complete list of supported global applications by using the **show qos basic classification global-app ?**. You can add additional global applications. For details, see the *Steelhead Appliance Deployment Guide*.

To view the predefined global application list, go to:

http://www.riverbed.com/us/products/technology/riverbed_classification_qos_engine.php

This command is only available in basic outbound QoS.

Example

```
amnesiac (config) # qos basic classification global-app add global-app-name MyGlobalApp class-name
Realtime vlan 1 traffic all srcport 123 srcnet 192.168.0.0/24 proto tcp dstport 456 dstnet
172.168.0.0/16 dscp 3

amnesiac (config) # qos basic classification global-app add global-app-name test_app class-name
business-critical dscp -1 protocol all vlan -1 traffic-type all srcnet 0.0.0.0/0 srcport test_label
dstnet 0.0.0.0/0 dstport test_label out-dscp 254 default-path relay path-1 4294967295 path-1-dscp
253 path-3 4294967295 path-3-dscp 253 path-2 4294967295 path-2-dscp 253 index 1
```

Product

Steelhead appliance

Related Topics

"host-label,""qos basic classification global-app move," "show qos basic classification," "Path Selection Commands"

qos basic classification global-app edit

Description

Edits QoS classification rules for the specified global application. These site rules apply to every site.

Syntax

[no] qos basic classification global-app edit global-app-name <name> [new-gapp-name <name>] [class-name {realtime |interactive | business-critical |normal| low-priority |best-effort}] [dscp <dscp level>] [protocol {all | gre | icmp |ipsec | tcp | udp}] [vlan <vlan>] [traffic-type {all |optimized |passthrough}] [srcnet <subnet/mask>] [srcport <port>] [dstnet <subnet/mask>] [dstport <port>] [l7protocol <protocol>] [domain-name <name>] [relative-path <path>] [path-1 <path-1-name>] [path-1-dscp <dscp>] [path-2 <path-2-name>] [path-2-dscp <dscp>] [path-3 <path-3-name>] [path-3-dscp <dscp>] [default-path {relay | drop}] [out-dscp <out-dscp-value>] [description]

Parameters

global-app-name <name>	Specify the name of the global application. To view the predefined global application list, go to: http://www.riverbed.com/us/products/technology/riverbed_classification_qos_engine.php
new-gapp-name <name>	Specify the name of a new global application.
class-name <class>	Specify the class that applies to the global application. If the rule matches, the specified rule sends the packet to this class. • **realtime**- Specify a real-time traffic class. Traffic that is your highest priority should be given this value: for example, VoIP, video conferencing. • **interactive** - Specify an interactive traffic class: for example, Citrix, RDP, telnet and ssh. • **business-critical** - Specify the business-critical traffic class: for example, Thick Client Applications, ERPs, and CRMs • **normal** - Specify a normal-priority traffic class: for example, Internet browsing, file sharing, and email. • **low-priority** - Specify a low-priority traffic class: for example, FTP, backup, replication, other high-throughput data transfers, and recreational applications such as audio file sharing. • **best-effort** - Specify the lowest priority.
dscp <dscp level>	Optionally, specify a DSCP level (**0-63**). Use this option to configure a QoS rule matching a specific DSCP mark.
protocol {all | gre | icmp |ipsec | tcp | udp}	Optionally, specify the protocol for the rule. The default value is **all**.
vlan <vlan>	Optionally, specify the VLAN tag ID.
traffic-type {all | optimized | passthrough}	Specify the type of traffic. QoS rules are applied to optimized and pass-through (egress only) traffic.
srcnet <subnet/mask> |<host_label< | srcport <port>	Optionally, specify the source network subnet and mask, host label, or port. Use the format XXX.XXX.XXX.XXX/XX for subnet and mask. The default value for port is **all**. Host labels are names given to lists of hosts (IP addresses, IP subnets, and hostnames). You configure a host label using the **host-label** command.
dstnet <subnet/mask> |<host_label> | dstport <port>}	Optionally, specify the destination network subnet and mask, host label, or port. Use the format XXX.XXX.XXX.XXX/XX for subnet and mask. The default value for port is **all**. Host labels are names given to lists of hosts (IP addresses, IP subnets, and hostnames). You configure a host label using the **host-label** command.
l7protocol <protocol>	Specify a protocol name Enable a protocol for classification rules. The application priority separates low-priority traffic (such as print jobs) from high-priority traffic (such as interactive screen updates). The upper bandwidth limit is defined at 100%, so that the lower priority classes can use the full bandwidth when it is available.
domain-name <name>	Specify a domain name. Only valid if you specify the **l7protocol HTTP** option.

relative-path <path>	Specify a relative path. For example, the relative path for `www.riverbed.com/appliance/commandline` would be `/appliance/commandline`. This option is only valid if you specify the **l7protocol** protocol **HTTP**. The relative path is the part of the URL that follows the domain name.
path-1-path <path-1-name> | path-2-path <path-2-name> | path-3-path <path-3-name>	Specify the path name. Configure the available paths in the network using the **path-selection path** command.
path-1-dscp <dscp> | path-2-dscp <dscp> | path-3-dscp <dscp>	Optionally, specify the DSCP value associated with a path. The DSCP marking values are **0-63** and **253** (inherit from rule). Specifying a DSCP value for a path is used for Policy-Based Routing (PBR) use cases. For details about PBR and path selection, see the *Steelhead Appliance Deployment Guide* and *Steelhead Appliance Management Console User's Guide*. If you need to use the **255** (reflect) DSCP value for a path, specify it in the **out-dscp <out-dscp-value>** parameter and use **253** (inherit from rule) as the path DSCP value.
default-path {relay | drop}	Specify the default path-selection action if the rule is matched and all specified paths are down: • **relay** - Route packets normally using the default path. If not configured, the default behavior is relay without applying path selection. • **drop -** Drop the connection.
out-dscp <out-dscp-value>	Optionally, specify the QoS class outbound DSCP marking value. The outbound DSCP marking values are **0-63**, or **255** (reflect), or **254** (inherit from class). Reflect is the default setting for a service class. Reflect means that the DSCP level or IP ToS value found on pass-through traffic is unchanged when it passes through the Steelhead appliance.
description <description>	Specify a description.

Usage

Global applications are applications the Application Flow Engine (AFE) can recognize and classify. With AFE, QoS can identify applications accurately, and differentiate applications that use the same port on the same server. The AFE is similar to deep packet inspection (DPI) because it identifies applications based on patterns.

Each global application is associated with a default QoS class. You can change the class with which a global application is associated using the **class-name** parameter.

You can display a complete list of supported global applications by using the **show qos basic classification global-app ?**. You can add additional global applications. For details, see the *Steelhead Appliance Deployment Guide*.

To view the predefined global application list, go to:

http://www.riverbed.com/us/products/technology/riverbed_classification_qos_engine.php

This command is only available in basic outbound QoS.

Example

```
amnesiac (config) # qos basic classification global-app add global-app-name MyGlobalApp class-name
Realtime vlan 1 traffic all srcport 123 srcnet 192.168.0.0/24 proto tcp dstport 456 dstnet
172.168.0.0/16 dscp 3
```

Product

Steelhead appliance

Related Topics

"qos basic classification global-app move,""show qos basic classification," "Path Selection Commands"

qos basic classification global-app move

Description

Moves an existing QoS rule in the rule index to the specified number, optionally on a particular site.

Syntax

qos basic classification global-app move from <index> to <index>

Parameters

from <index> to <index>	Move QoS global application position in index of QoS global application.

Usage

For a complete list of supported global applications use **show qos basic classification global-app ?** to print help information on the command line.

This command is available only in basic outbound QoS mode.

Example

```
amnesiac (config) # qos basic classification global-app move from 2 to 4
```

Product

Steelhead appliance

Related Topics

"qos basic classification global-app add," "qos classification rule", "show qos basic classification"

qos basic classification policy add

Description

Creates policies allocating bandwidth for the six classes used by a site in basic outbound QoS. You can use the default policies or you can optionally add a bandwidth policy to allocate a bandwidth percentage for any of the six predefined service classes.

Syntax

qos basic classification policy add policy-name <name> rt-min-bw-pct <rt-min-bw-pct> rt-max-bw-pct<rt-max-bw-pct> [rt-out-dscp <rt-out-dscp-value>] ia-min-bw-pct <ia-min-bw-pct> ia-max-bw-pct <ia-max-bw-pct> [ia-out-dscp <ia-out-dscp-value>] bc-min-bw-pct <bc-min-bw-pct> bc-max-bw-pct <bc-max-bw-pct> [bc-out-dscp <bc-out-dscp-value>] nm-min-bw-pct <nm-min-bw-pct> nm-max-bw-pct <nm-max-bw-pct> [nm-out-dscp <nm-out-dscp-value] lp-min-bw-pct <lp-min-bw-pct> lp-max-bw-pct <lp-max-bw-pct> [lp-out-dscp <lp-out-dscp-value>] be-min-bw-pct <be-min-bw-pct> be-max-bw-pct <be-max-bw-pct> [be-out-dscp <be-out-dscp-value>]

Parameters

policy-name <name>	Specify the name of the QoS service classification policy.
rt-min-bw-pct <rt-min-bw-pct>	Specify the minimum bandwidth for the real-time traffic class, in percentage. Traffic that is your highest priority should be given this value, for example, VoIP, video conferencing.
rt-max-bw-pct <rt-max-bw-pct> [rt-out-dscp <rt-out-dscp-value>]	Specify the maximum bandwidth maximum for the real-time traffic class, in percentage. Optionally, specify the QoS class outbound DSCP marking value for the real-time traffic class. The outbound DSCP values are **0-63** or **255** (reflect). Reflect is the default setting for a service class. Reflect means that the DSCP level or IP ToS value found on pass-through traffic is unchanged when it passes through the Steelhead appliance.
ia-min-bw-pct <rt-min-bw-pct>	Specify the minimum bandwidth for the interactive traffic class, in percentage. Examples of traffic for this class include Citrix, RDP, telnet, and SSH.
ia-max-bw-pct <ia-max-bw-pct> [ia-out-dscp <ia-out-dscp-value>]	Specify the maximum bandwidth maximum for the interactive traffic class, in percentage. Optionally, specify the QoS class outbound DSCP marking value for the interactive traffic class. The outbound DSCP values are **0-63** or **255** (reflect). Reflect is the default setting for a service class.
bc-min-bw-pct <bc-min-bw-pct>	Specify the minimum bandwidth for the business-critical traffic class, in percentage. Examples of traffic for this class include Thick Client Applications, ERPs, and CRMs.
bc-max-bw-pct <bc-max-bw-pct> [bc-out-dscp <bc-out-dscp-value>]	Specify the maximum bandwidth maximum for the business-critical traffic class, in percentage. Optionally, specify the QoS class outbound DSCP marking value for the business-critical traffic class. The outbound DSCP values are **0-63** or **255** (reflect). Reflect is the default setting for a service class.
nm-min-bw-pct <nm-min-bw-pct>	Specify the minimum bandwidth for the normal traffic class, in percentage. Examples of traffic for this class include Internet browsing, file sharing, and email.
nm-max-bw-pct <nm-max-bw-pct> [nm-out-dscp <nm-out-dscp-value>]	Specify the maximum bandwidth maximum for the normal traffic class, in percentage. Optionally, specify the QoS class outbound DSCP marking value for the normal traffic class. The outbound DSCP values are **0-63** or **255** (reflect). Reflect is the default setting for a service class.
lp-min-bw-pct <lp-min-bw-pct>	Specify the minimum bandwidth for the low-priority class, in percentage. Examples of traffic for this class include FTP, backup, replication, other high-throughput data transfers, and recreational applications such as audio file sharing.
lp-max-bw-pct <lp-max-bw-pct> [lp-out-dscp <lp-out-dscp-value>]	Specify the maximum bandwidth maximum for the low-priority traffic class, in percentage. Optionally, specify the QoS class outbound DSCP marking value for the low-priority traffic class. The outbound DSCP values are **0-63** or **255** (reflect). Reflect is the default setting for a service class.
be-min-bw-pct <be-min-bw-pct>	Specify the minimum bandwidth for the best-effort traffic class, in percentage.
be-max-bw-pct <be-max-bw-pct> [be-out-dscp <be-out-dscp-value>]	Specify the maximum bandwidth maximum for the best-effort traffic class, in percentage. Optionally, specify the QoS class outbound DSCP marking value for the best-effort traffic class. The outbound DSCP values are **0-63** or **255** (reflect). Reflect is the default setting for a service class.

Usage

A service policy contains the bandwidth allocation for six classes used at each site in basic QoS mode. Select a service policy when creating a new site or editing a site.

You must configure all six classes to create a complete service policy.

Bandwidth allocation, also known as traffic shaping, is a means of allocating the correct amount of bandwidth for each QoS traffic class. The amount you specify reserves a predetermined amount of bandwidth for each traffic class. Bandwidth allocation is important for ensuring that a given class of traffic cannot consume more bandwidth than it is allowed. It is also important to ensure that a given class of traffic has a minimum amount of bandwidth available for delivery of data through the network.

The minimum bandwidth is the percentage of the bandwidth that is guaranteed to be allocated to the application in the traffic class. A lower value indicates that the traffic in the class is more likely to be delayed.

The maximum bandwidth is the maximum percentage of the bandwidth that can be allocated to the application in the traffic class.

This command is available only in basic outbound QoS mode.

The **no qos basic classification policy add policy-name <name>** command deletes the policy configuration.

Example

```
amnesiac (config) # qos basic classification policy add policy-name test_policy rt-min-bw-pct 20
rt-max-bw-pct 100 rt-out-dscp 255 ia-min-bw-pct 10 ia-max-bw-pct 100 ia-out-dscp 255 bc-min-bw-pct 30
bc-max-bw-pct 100 bc-out-dscp 255 nm-min-bw-pct 30 nm-max-bw-pct 100 nm-out-dscp 255 lp-min-bw-pct 10
lp-max-bw-pct 30 lp-out-dscp 255 be-min-bw-pct 5 be-max-bw-pct 100 be-out-dscp 255Granite-Edge Id:
```

Product

Steelhead appliance

Related Topics

"qos basic classification policy edit,""show qos basic classification"

qos basic classification policy edit

Description

Edits a QoS classification service policy.

Syntax

qos basic classification policy edit policy-name <name> [rt-min-bw-pct <rt-min-bw-pct>] [rt-max-bw-pct <rt-max-bw-pct>] [rt-out-dscp <rt-out-dscp-value>] [ia-min-bw-pct <ia-min-bw-pct>] [ia-max-bw-pct <ia-max-bw-pct>] [ia-out-dscp <ia-out-dscp-value>] [bc-min-bw-pct <bc-min-bw-pct>] [bc-max-bw-pct <bc-max-bw-pct>] [bc-out-dscp <bc-out-dscp-value>] [nm-min-bw-pct <nm-min-bw-pct>] [nm-max-bw-pct <nm-max-bw-pct>] [nm-out-dscp <nm-out-dscp-value>] [lp-min-bw-pct <lp-min-bw-pct>] [lp-max-bw-pct <lt-max-bw-pct>] [lp-out-dscp <lp-out-dscp-value>] [be-min-bw-pct <be-min-bw-pct>] [be-max-bw-pct <be-max-bw-pct>] [be-out-dscp <be-out-dscp-value>]

Parameters

policy-name <name>	Specify the name of an existing service policy.
rt-min-bw-pct <rt-min-bw-pct>	Edit the minimum bandwidth for the real-time traffic class, in percentage.
rt-max-bw-pct <rt-max-bw-pct>]	Edit the maximum bandwidth for the real-time traffic class, in percentage.
rt-out-dscp <rt-out-dscp-value>	Edit the QoS class outbound DSCP marking value for the real-time traffic class.
ia-min-bw-pct <ia-min-bw-pct>]	Edit the minimum bandwidth for the interactive traffic class, in percentage.
ia-max-bw-pct <ia-max-bw-pct>	Edit the maximum bandwidth for the interactive class, in percentage.
ia-out-dscp <ia-out-dscp-value>	Edit the QoS class outbound DSCP marking value for the interactive traffic class.
bc-min-bw-pct <bc-min-bw-pct>	Edit the minimum bandwidth for the business-critical traffic class, in percentage.
bc-max-bw-pct <bc-max-bw-pct>	Edit the maximum bandwidth for the business-critical class, in percentage.
bc-out-dscp <bc-out-dscp-value>	Edit the QoS class outbound DSCP marking value for the business-critical traffic class.
nm-min-bw-pct <nm-min-bw-pct>	Edit the minimum bandwidth for the normal traffic class, in percentage.
nm-max-bw-pct <nm-max-bw-pct>	Edit the maximum bandwidth for the normal class, in percentage.
nm-out-dscp <nm-out-dscp-value>	Edit the QoS class outbound DSCP marking value for the normal traffic class.
lp-min-bw-pct <lp-min-bw-pct>	Edit the minimum bandwidth for the low-priority traffic class, in percentage.
lp-max-bw-pct <lp-max-bw-pct>	Edit the maximum bandwidth for the low-priority class, in percentage.
lp-out-dscp <lp-out-dscp-value>	Edit the QoS class outbound DSCP marking value for the low-priority traffic class.
be-min-bw-pct <be-min-bw-pct>	Edit the minimum bandwidth for the best-effort traffic class, in percentage.
be-max-bw-pct <be-max-bw-pct>	Edit the maximum bandwidth for the best-effort class, in percentage.
be-out-dscp <be-out-dscp-value>	Edit the QoS class outbound DSCP marking value for the best-effort traffic class.

Usage

A service policy contains the bandwidth allocation for each of the six service classes used at each site in basic QoS mode. You must configure all six classes to create a complete policy.

Bandwidth allocation, also known as traffic shaping, is a means of allocating the correct amount of bandwidth for each QoS traffic class. The amount you specify reserves a predetermined amount of bandwidth for each traffic class. Bandwidth allocation is important for ensuring that a given class of traffic cannot consume more bandwidth than it is allowed. It is also important to ensure that a given class of traffic has a minimum amount of bandwidth available for delivery of data through the network.

This command is available only in basic outbound QoS mode.

Example

```
amnesiac (config) # qos basic classification policy edit policy-name test_policy  bc-min-bw-pct 30
bc-max-bw-pct 50 bc-out-dscp 255
```

Product

Steelhead appliance

Related Topics

"qos basic classification policy add,""show qos basic classification"

qos basic classification site add

Description

Adds a site to a basic outbound QoS configuration, including WAN bandwidth and, optionally, index position.

Syntax

qos basic classification site add site-name <name> wan-bw <throughput> policy-name <name> [network {<IPv4 subnet>|all}] [default-class <def-class-for-site>] [index <number>] [def-out-dscp <dscp-value>] [path-1 <path-1-name>] [path-1-dscp <dscp>] [path-2 <path-2-name>] [path-2-dscp <dscp>] [path-3 <path-3-name>] [path-3-dscp <dscp>] [default-path {relay | drop}]

Parameters

site-name <name>	Specify the name of the site; for example, data center.
wan-bw <throughput>	Specify the maximum WAN bandwidth in Kbps.
policy-name <name>	Specify the name of a policy to associate with the site.
network <IPv4 subnet>	Specify the subnet of the site in the format XXX.XXX.XXX.XXX/XX.
all	Add all IPv4 addresses.
default-class <def-class-for-site>	Specify the default class for the site. Traffic classification options are: • **realtime**- Specify a real-time traffic class. Traffic that is your highest priority should be given this value: for example, VoIP, video conferencing. • **interactive** - Specify an interactive traffic class: for example, Citrix, RDP, telnet and ssh. • **business-critical** - Specify the business-critical traffic class: for example, Thick Client Applications, ERPs, and CRMs • **normal** - Specify a normal-priority traffic class: for example, Internet browsing, file sharing, and email. • **low-priority** - Specify a low-priority traffic class: for example, FTP, backup, replication, other high-throughput data transfers, and recreational applications such as audio file sharing. • **best-effort** - Specify the lowest priority.
index <number>	Optionally, specify the position in the index.
def-out-dscp <dscp-value>	Specify the DSCP mark for traffic matching the default rule in the site. The DSCP values are **0-63**, **255** (reflect), or **254** (inherit from service class). Reflect is the default setting. Reflect means that the DSCP level or IP ToS value found on pass-through traffic is unchanged when it passes through the Steelhead appliance.
path-1-path <path-1-name> | path-2-path <path-2-name> | path-3-path <path-3-name>	Specify the path name. Configure the available paths in the network using the **path-selection path** command.
path-1-dscp <dscp> | path-2-dscp <dscp> | path-3-dscp <dscp>	Optionally, specify the DSCP value associated with a path. The DSCP marking values are **0-63** and **253** (inherit from site). Specifying a DSCP value for a path is used for Policy-Based Routing (PBR) use cases. For details about PBR and path selection, see the *Steelhead Appliance Deployment Guide* and *Steelhead Appliance Management Console User's Guide*. If you need to use the **255** (reflect) DSCP value for a path, specify it in the **def-out-dscp <dscp-value>** parameter and use **253** (inherit from rule) as the path DSCP value.
default-path {relay | drop}	Specify the default path-selection action if the rule is matched and all specified paths are down: • **relay** - Route packets normally using the default path. If not configured, the default behavior is relay without applying path selection. • **drop -** Drop the connection.

Usage

For details about the recommended maximum number of sites see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Basic QoS supports the configuration of the path selection feature, a default class, and default DSCP values added to each site. These values are applied to a flow after it has started but before the DPI engine has enough information to assign it to a global application. Once assigned to a global application, the path-selection settings of the global application are used.

Example

```
amnesiac (config) # qos basic classification site add site-name MyTestSite network 192.12.12.10/32
wan-bw 5000 policy-name low-priority index 3
```

Product

Steelhead appliance

Related Topics

"qos basic classification site edit,""qos basic classification site edit add-network,""qos basic classification site move," "show qos basic classification," "Path Selection Commands"

qos basic classification site edit

Description

Edits QoS basic classification settings for the site.

Syntax

qos basic classification site edit site-name <name> [default-class <def-class-for-site>] [def-out-dscp <dscp-value>] [path-1 <path-1-name>] [path-1-dscp <dscp>] [path-2 <path-2-name>] [path-2-dscp <dscp>] [path-3 <path-3-name>] [path-3-dscp <dscp>] [default-path {relay | drop}]

Parameters

site-name <name>	Specify the name of the site.
default-class <def-class-for-site>	Specify the default class for the site. Traffic classification options are: • **realtime**- Specify a real-time traffic class. Traffic that is your highest priority should be given this value: for example, VoIP, video conferencing. • **interactive** - Specify an interactive traffic class: for example, Citrix, RDP, telnet and ssh. • **business-critical** - Specify the business-critical traffic class: for example, Thick Client Applications, ERPs, and CRMs • **normal** - Specify a normal-priority traffic class: for example, Internet browsing, file sharing, and email. • **low-priority** - Specify a low-priority traffic class: for example, FTP, backup, replication, other high-throughput data transfers, and recreational applications such as audio file sharing. • **best-effort** - Specify the lowest priority.
def-out-dscp <dscp-value>	Specify the DSCP mark for traffic matching the default rule in the site. The DSCP values are **0-63**, **255** (reflect), or **254** (inherit from service class). Reflect is the default setting. Reflect means that the DSCP level or IP ToS value found on pass-through traffic is unchanged when it passes through the Steelhead appliance.
path-1-path <path-1-name> | path-2-path <path-2-name> | path-3-path <path-3-name>	Specify the path name. Configure the available paths in the network using the **path-selection path** command.
path-1-dscp <dscp> | path-2-dscp <dscp> | path-3-dscp <dscp>	Specify the DSCP value associated with a path. The DSCP marking values are **0-63** and **253** (inherit from site). Specifying a DSCP value for a path is only used for Policy-Based Routing (PBR) use cases. For details about PBR and path selection, see the *Steelhead Appliance Deployment Guide* and *Steelhead Appliance Management Console User's Guide*. If you need to use the **255** (reflect) DSCP value for a path, specify it in the **def-out-dscp <dscp-value>** parameter and use **253** (inherit from rule) as the path DSCP value.
default-path {relay | drop}	Specify the default path-selection action if the rule is matched and all specified paths are down: • **relay** - Route packets normally using the default path. If not configured, the default behavior is relay without applying path selection. • **drop -** Drop the connection.

Usage

For details about the recommended maximum number of sites, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # qos basic classification site edit site-name MyTestSite policy-name low-priority
index 3 path-1 primary path-1-dscp 63 default-path relay
```

Product

Steelhead appliance

Related Topics

"qos basic classification site add," "qos basic classification site move," "show qos basic classification," "Path Selection Commands"

qos basic classification site edit add-network

Description

Adds a network to the site.

Syntax

qos basic classification site edit site-name <name> add-network network {<IPv4 subnet >| all}

Parameters

site-name <name>	Specify the name of an existing site.
network <IPv4 subnet>	Add the network to the site in the format XXX.XXX.XXX.XXX/XX.
network all	Add all IPv4 addresses.

Usage

For details about the recommended maximum number of sites, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # qos basic classification site edit site-name MyTestSite add-network network all
```

Product

Steelhead appliance

Related Topics

"qos basic classification site add," "qos basic classification site move," "show qos basic classification"

qos basic classification site edit policy-name

Description

Edits the service policy name of the site.

Syntax

qos basic classification site edit site-name <name> policy-name <service-policy-name>

Parameters

site-name <name>	Specify the name of the site.
<service-policy-name>	Specify the service policy name for the site: • **Large_Office** - Specify the large office service policy • **Larger_Office** - Specify the larger office service policy. • **Medium_Office** - Specify the medium office service policy. • **Small_Office** - Specify the small office service policy name. • **Smaller_Office** - Specify the smaller office service policy name.

Usage

For details about the recommended maximum number of sites, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # qos basic classification site edit site-name MyTestSite policy-name
Larger_Office
```

Product

Steelhead appliance

Related Topics

"qos basic classification site add," "qos basic classification site move," "show qos basic classification"

qos basic classification site edit wan-bw

Description

Edits the WAN throughput setting for the site.

Syntax

qos basic classification site edit wan-bw

Syntax

qos basic classification site edit site-name <name> wan-bw <throughput>

Parameters

site-name <name>	Specify the name of the site.
<throughput>	Specify the maximum WAN bandwidth in Kbps.

Usage

For details about the recommended maximum number of sites, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # qos basic classification site edit site-name MyTestSite wan-bw 5000
```

Product

Steelhead appliance

Related Topics

"qos basic classification site add," "qos basic classification site move," "show qos basic classification"

qos basic classification site move

Description

Moves the QoS site position in the order of application.

Syntax

qos basic classification site move from <position> to <position>

Parameters

from <position>	Specify the numeric position in the index.
to <position>	Specify the numeric position in the index.

Usage

Steelhead appliances evaluate rules in numerical order called an index, starting with rule 1. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.

The default site, which is tied to the Medium Office policy, cannot be removed and is always listed last. This command is available only in basic QoS mode.

Example

```
amnesiac (config) # qos basic classification site move from 4 to 1
```

Product

Steelhead appliance

Related Topics

"qos basic classification site edit add-network," "qos basic classification site add," "show qos basic classification"

qos basic shaping enable

Description

Enables basic QoS.

Syntax

[no] qos basic shaping enable

Parameters

None

Usage

The **no** version disables basic QoS. This command is available only in basic outbound QoS mode.

Example

```
amnesiac (config) # qos basic shaping enable
```

Product

Steelhead appliance

Related Topics

"qos basic shaping interface enable," "qos basic shaping interface rate", "show qos basic classification"

qos basic shaping interface enable

Description

Configures QoS shaping on the specified interface.

Syntax

[no] qos basic shaping interface <interface name> enable

Parameters

<interface name>	Specify an interface: **primary**, **wan0_0**.

Usage

This command enables QoS shaping on a specified interface. Traffic is not classified until at least one WAN interface is enabled.

Bandwidth allocation, also known as traffic shaping, is a means of allocating the correct amount of bandwidth for each QoS traffic class. The amount you specify reserves a pre-determined amount of bandwidth for each traffic class. Bandwidth allocation is important for ensuring that a given class of traffic cannot consume more bandwidth than it is allowed. It is also important to ensure that a given class of traffic has a minimum amount of bandwidth available for delivery of data through the network.

This command is available only in basic outbound QoS mode.

Example

```
amnesiac (config) # qos basic shaping interface wan0_0 enable
```

Product

Steelhead appliance

Related Topics

"qos basic shaping enable," "qos basic shaping interface rate," "show qos basic classification"

qos basic shaping interface rate

Description

Sets the absolute QoS rate limit applied individually to every interface that is performing QoS traffic shaping.

Syntax

[no] qos basic shaping interface rate <kbit rate>

Parameters

<kbit rate>	Specify an integer for the bandwidth of the interface.

Usage

The link rate is the bottleneck WAN bandwidth, not the interface speed out of the WAN interface into the router or switch. For example, if your Steelhead connects to a router with a 100 Mbps link, do not specify this value—specify the actual WAN bandwidth (for example, T1, T3).

Different WAN interfaces can have different WAN bandwidths; you must enter the bandwidth link rate correctly for QoS to function properly.

This command is available only in basic outbound QoS mode.

Example

```
amnesiac (config) # qos basic shaping interface rate 1000
```

Product

Steelhead appliance

Related Topics

"qos basic shaping enable", "qos basic shaping interface enable," "show qos basic classification"

qos basic shaping wan-oversub enable

Description

Enables bandwidth oversubscription support. Allows the sum of remote site bandwidths to exceed the WAN uplink speed.

Syntax

[no] qos basic shaping wan-oversub enable

Parameters

None

Usage

Riverbed recommends enabling this option when your network includes remote site bandwidths that collectively exceed the available bandwidth of the local WAN uplink interface speed when a subset of remote sites are active at once.

Bandwidth oversubscription shares the bandwidth fairly when the network includes remote site bandwidths that collectively exceed the available bandwidth of the local WAN uplink interface speed. The link sharing provides bandwidth guarantees when some of the sites are partially or fully inactive.

For example, your data center uplink might be 45Mbit/s with three remote office sites each with 20Mbit/s uplinks. When disabled, you can only allocate bandwidth for the remote sites such that the total bandwidth does not exceed the bandwidth of any of the interfaces on which QoS is enabled.

Enabling this option can degrade latency guarantees when the remote sites are fully active.

Example

```
amnesiac (config) # qos basic shaping wan-oversub enable
```

Product

Steelhead appliance

Related Topics

"qos basic shaping enable", "show qos basic classification"

Advanced Outbound QoS Commands

Use advanced outbound QoS when you:

- are currently using RiOS v6.1.x or earlier QoS and do not want to reconfigure your existing rules. The Steelhead preserves the configuration.
- need to use the MX-TCP queue. For details, see the *Steelhead Appliance Management Console User's Guide*.
- need to set application priorities for Citrix ICA traffic (this requires packet-order queue).
- need to set application priorities for PC-over-IP (PCoIP) traffic (choose either fifo, sfq, or packet-order for the queue).
- need to set application priorities for SnapMirror traffic (SnapMirror is not dependent on the queue type).
- have WAN links with different bandwidth (basic QoS assumes all links of the same size). For example, you might have a 2 Mbps MPLS link with a 1 Mbps ADSL backup.

qos classification class

Description

Adds or modifies a QoS class. Priorities and bandwidths are set by QoS class. You can create multiple classes.

Syntax

[no] qos classification class {add | modify} class-name <classname> priority {realtime | interactive | business | normal | low | best-effort} min-pct <min bw percent> <cr> | out-dscp <out-dscp-value> <cr> | parent <parent class name> | queue-length <length> <cr> | queue-type {fifo | sfq | mxtcp | packet-order} <cr> | [conn-limit <num> <cr>] | upper-limit-pct <upper-limit pct> <cr> | link-share <weight> <cr>

Parameters

add | modify	Specify whether to add or modify a new class.
class-name <classname>	Specify a name for the QoS class.
priority {**realtime | interactive | business| normal| low| best-effort**}	Specify a minimum guaranteed QoS priority level. The latency priority indicates how delay-sensitive a traffic class is to the QoS scheduler. Select the latency priority for the class (highest priority to lowest priority): • **realtime**- Specify a real-time traffic class. Traffic that is your highest priority should be given this value, for example, VoIP, video conferencing. • **interactive** - Specify an interactive traffic class: for example, Citrix, RDP, telnet and ssh. • **business** - Specify the business critical traffic class: for example, Thick Client Applications, ERPs, and CRMs • **normal** - Specify a normal priority traffic class: for example, Internet browsing, file sharing, and email. • **low** - Specify a low priority traffic class: for example, FTP, backup, replication, other high-throughput data transfers, and recreational applications such as audio file sharing. • **best-effort** - Specify the lowest priority.
min-pct <min bw percent>	Specify the minimum amount of bandwidth given to a flow when there is bandwidth contention (minimum bandwidth guarantee). Flows that do not use all of their allocated minimum bandwidth will share this excess bandwidth with other flows that exceed their minimum bandwidth allocation. All the classes combined cannot exceed 100%. During contention for bandwidth, the class is guaranteed at least to the amount of specified bandwidth. It will receive more if there is unused bandwidth remaining. The guaranteed bandwidth calculated based on this percentage should be no less than 1Kbps. For example, if the **wan0_0** throughput is 1000 Kbps, and a first-level class has its guaranteed bandwidth of 0.1%, this results in a bandwidth of 1000 * 0.1% = 1Kbps.
out-dscp <out-dscp-value>	Specify the QoS class outbound DSCP value. The DSCP values are **0-63** or **255** (reflect). Reflect is the default setting for a service class. Reflect means that the DSCP level or IP ToS value found on pass-through traffic is unchanged when it passes through the Steelhead appliance.
parent <parent class name>	Specify the parent for a child class to enable QoS hierarchy. The class will inherit the parent's definitions. For example, if the parent class has a business priority, and its child has a realtime priority, the child will inherit the business priority from its parent, and will use a realtime priority only with respect to its siblings. For details, see the *Steelhead Appliance Management Console User's Guide*.
queue-length <length>	Specify the QoS class queue length. By default, each class has a queue length of 100. Riverbed recommends that you consult with Riverbed Support or your sales engineer before you set this parameter.

queue-type {fifo | sfq | mxtcp | packet-order}

Optionally, select one of the following queue methods for the leaf class (the queue does not apply to the inner class):

- **fifo** - Transmits all flows in the order that they are received (first in, first out). Bursty sources can cause long delays in delivering time-sensitive application traffic and potentially to network control and signaling messages.
- **sfq** - Shared Fair Queueing (SFQ) is the default queue for all classes. Determines Steelhead appliance behavior when the number of packets in a QoS class outbound queue exceeds the configured queue length. When SFQ is used, packets are dropped from within the queue in a round-robin fashion, among the present traffic flows. SFQ ensures that each flow within the QoS class receives a fair share of output bandwidth relative to each other, preventing bursty flows from starving other flows within the QoS class.
- **mxtcp** - Maximum speed TCP queue has very different use cases than the other queue parameters. MX-TCP also has secondary effects that you need to understand before configuring:
  - – When optimized traffic is mapped into a QoS class with the MX-TCP queuing parameter, the TCP congestion control mechanism for that traffic is altered on the Steelhead appliance. The normal TCP behavior of reducing the outbound sending rate when detecting congestion or packet loss is disabled, and the outbound rate is made to match the minimum guaranteed bandwidth configured on the QoS class.
  - – You can use MX-TCP to achieve high-throughput rates even when the physical medium carrying the traffic has high loss rates. For example, MX-TCP is commonly used for ensuring high throughput on satellite connections where a lower-layer-loss recovery technique is not in use.
  - – Another use of MX-TCP is to achieve high throughput over high-bandwidth, high-latency links, especially when intermediate routers do not have properly tuned interface buffers. Improperly tuned router buffers cause TCP to perceive congestion in the network, resulting in unnecessarily dropped packets, even when the network can support high throughput rates.

You must ensure the following when you enable MX-TCP:

– The QoS rule for MX-TCP is at the top of QoS rules list.

– The rule does not use Application Flow Engine identification.

– You only use MX-TCP for optimized traffic. MX-TCP does not work for unoptimized traffic (pass-through traffic).

Use caution when specifying MX-TCP. The outbound rate for the optimized traffic in the configured QoS class immediately increases to the specified bandwidth, and does not decrease in the presence of network congestion. The Steelhead appliance always tries to transmit traffic at the specified rate. If no QoS mechanism (either parent classes on the Steelhead appliance, or another QoS mechanism in the WAN or WAN infrastructure) is in use to protect other traffic, that other traffic might be impacted by MX-TCP not backing off to fairly share bandwidth.

When MX-TCP is configured as the queue parameter for a QoS class, the following parameters for that class are also affected:

– **link-share** - The link share weight parameter has no effect on a QoS class configured with MX-TCP.

– **upper-limit-pct** - The upper limit parameter has no effect on a QoS class configured with MX-TCP.

- **packet-order** - Protects the TCP stream order by keeping track of flows that are currently inside the packet-shaping infrastructure. Packet-order protection allows only one packet from each flow into the HFSC traffic shaper at a time. The backlog for each flow stores the packets from the flow in order until the packet inside the HFSC infrastructure is dequeued for delivery to the network interface. The packet-order priority protection works for both TCP and UDP streams. For best performance, select this queue with Citrix real-time latency priority traffic.

conn-limit <optimized-connection-number>	Optionally, specify the connection limit. The connection limit is the maximum number of optimized connections for the class. When the limit is reached, all new connections are passed through unoptimized. In hierarchical mode, a parent class connection limit does not affect its child. Each child class optimized connection is limited by the connection limit specified for their class. For example, if B is a child of A, and the connection limit for A is set to 5, while the connection limit for B is set to 10, the connection limit for B is 10. Connection limit is supported only in in-path configurations. It is not supported in out-of-path or virtual-in-path configurations. Connection limit is supported only in in-path configurations. It is not supported in out-of-path or virtual-in-path configurations. Connection limit does not apply to the packet-order queue or Citrix ICA traffic. RiOS does not support a connection limit assigned to any QoS class that is associated with a QoS rule with an Application Flow Engine component. An Application Flow Engine component consists of a Layer-7 protocol specification. RiOS cannot honor the class connection limit because the QoS scheduler might subsequently reclassify the traffic flow after applying a more precise match using Application Flow Engine identification.
upper-limit-pct <upper-limit pct>	Specify the upper limit percent settings for the class. Specify the maximum allowed bandwidth (as a percentage) a class receives as a percentage of the parent class guaranteed bandwidth. The limit is applied even if there is excess bandwidth available. The upper limit parameter has no effect on a QoS class configured with MX-TCP. Starting with RiOS 8.x, there is maximum bandwidth setting for MX-TCP. This allows traffic in the MX class to burst to the maximum level if the bandwidth is available.

Usage

QoS classes set priorities and bandwidths. You can create multiple QoS classes. There is no requirement that QoS classes represent applications, traffic to remote sites, or any other particular aggregation.

The QoS classes that are always present in Advanced QoS on the Steelhead appliance are:

- **Root Class** - The root class is used to constrain the total outbound rate of traffic leaving the Steelhead appliance to the configured, per-link WAN bandwidth. This class is not configured directly, but is created when you enable QoS classification and enforcement on the Steelhead appliance.
- **Built-in Default Class** - The QoS scheduler applies the built-in default class constraints and parameters on traffic not otherwise placed in a class by the configured QoS rules.

QoS classes are configured in one of two different modes: *flat* or *hierarchical*. The difference between the two modes primarily consists of how QoS classes are created.

For details about QoS classes, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

The **no** command options deletes the QoS class.

Example

```
amnesiac (config) # qos classification class add class-name example out-dscp 10
```

Product

Steelhead appliance

Related Topics

"show qos classification"

qos classification mode hierarchy enable

Description

Enables advanced QoS classification in hierarchical mode.

Syntax

[no] qos classification mode hierarchy enable

Parameters

None

Usage

In hierarchical mode, you create QoS classes as children of QoS classes other than the root class. This allows you to create overall parameters for a certain traffic type, and specify parameters for subtypes of that traffic. There is no enforced limit to the number of QoS class levels you can create.

In hierarchical mode, the following relationships exist between QoS classes:

- **Sibling classes** - Classes that share the same parent class.
- **Leaf classes** - Classes at the bottom of the class hierarchy.
- **Inner classes** - Classes that are neither the root class nor leaf classes.

In hierarchical mode, QoS rules can only specify leaf classes as targets for traffic.

Riverbed QoS controls the traffic of hierarchical QoS classes in the following manner:

- QoS rules assign active traffic to leaf classes.
- The QoS scheduler:
  - applies active leaf class parameters to the traffic.
  - applies parameters to inner classes that have active leaf class children.

In flat mode, all of the QoS classes you create must have the root class as their parent. Thus all of the QoS classes you create are siblings.

The QoS scheduler treats QoS classes in flat mode the same way that it does in hierarchical mode. However, only a single class level is defined. QoS rules place active traffic into the leaf classes. Each active class has its own QoS rule parameters which the QoS scheduler applies to traffic.

For details about QoS and how to configure it, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

The appropriate QoS enforcement system to use depends on the location of WAN bottlenecks for traffic leaving the site.

Use the following guidelines when implementing advanced QoS:

- A site that acts as a data server for other locations, such as a data center or regional hub, typically uses hierarchical mode. The first level of classes represents remote sites, and those remote site classes have child classes that either represent application types, or are indirectly connected remote sites.
- A site that typically receives data from other locations, such as a branch site, typically uses flat mode. The classes represent different application types.

For example, suppose you have a network with ten locations, and you want to choose the correct mode for site 1. Traffic from site 1 normally goes to two other sites: sites 9 and 10. If the WAN links at sites 9 and 10 are at a higher bandwidth than the link at site 1, the WAN bottleneck rate for site 1 is always the link speed for site 1. In this case, you can use flat mode to enforce QoS at site 1, because the bottleneck that needs to be managed is the link at site 1. In flat mode, the parent class for all created classes is the root class that represents the WAN link at site 1.

In the same network, site 10 sends traffic to sites 1 through 8. Sites 1 through 8 have slower bandwidth links than site 10. Because the traffic from site 10 faces multiple WAN bottlenecks (one at each remote site), you configure hierarchical mode for site 10.

When configuring QoS classification for FTP, the QoS rules differ depending on whether the FTP data channel is using *active* or *passive* FTP. Active versus passive FTP determines whether the FTP client or the FTP server select the port connection for use with the data channel, which has implications for QoS classification. For details, see the *Riverbed Central Management Console User's Guide*

You can use the Central Management Console (CMC) to enable QoS and to configure and apply QoS policies centrally to Steelhead appliances. For details, see the *Riverbed Central Management Console User's Guide*.

You must enable QoS classification and set the bandwidth link rate for the WAN interface before you create a QoS class.

Example

```
amnesiac (config) # qos classification mode hierarchy enable
```

Product

Steelhead appliance

Related Topics

"show qos classification"

qos classification rule

Description

Adds or edits a QoS classification rule. QoS rules determine membership of traffic in a particular QoS class.

Syntax

[no] qos classification rule {add [rule-name <rule-name>] class-name <class>| edit [rule-name <rule-name>] [new-rule-name <rule-name>] [class-name <class>]} [dscp <dscp level>] [protocol {all | udp | tcp | gre | icmp | ipsec}] [vlan <vlan>] [traffic-type {all |optimized |passthrough}] [srcnet {<subnet/mask> |<host_label>] [srcport <port>] [dstnet {<subnet/mask> | <host_label>}] [dstport <port>] [out-dscp <out-dscp-value>] [l7protocol <protocol>] [domain-name <name>] | [relative-path <path>] [prio-0 <class-name>] [out-dscp-0 <out-dscp-0>] [prio-1 <class-name>] [out-dscp-1 <out-dscp-1>] [prio-2 <class-name>] [out-dscp-2 <out-dscp-2>] [prio-3 <class-name>] [out-dscp-3 <out-dscp-3>] [prio-4 <class-name>] [out-dscp-4] [path-1 <path-1-name>] [path-1-dscp <dscp>] [path-2 <path-2-name>] [path-2-dscp <dscp>] [path-3 <path-3-name>] [path-3-dscp <dscp>] [default-path {relay | drop}] [description <description>] [rulenum <priority>] site-num <number>

Parameters

add | edit	Adds or edits the QoS classification rule.
rule-name <rule-name>	Optionally, specify a rule name.
new-rule-name <rule-name>	Optionally, when editing a rule, specify a new rule name.
class-name <class>	Specify the class to which the rule applies. If the rule matches, the specified rule sends the packet to this class.
dscp <dscp level>	Optionally, specify a DSCP level (**0-63**). Use this option to configure a QoS rule matching a specific DSCP mark.
protocol {all | udp | tcp | gre | icmp | ipsec}	Optionally, specify the protocol for the rule. The default value is **all**.
vlan <vlan>	Optionally, specify the VLAN tag ID.
traffic-type {all | optimized | passthrough}	Specify the type of traffic. QoS rules are applied to optimized and pass-through (egress only) traffic.
srcnet <subnet/mask> |<host_label> | srcport <port>	Optionally, specify the source network subnet and mask, host label, or port. Use the format XXX.XXX.XXX.XXX/XX for subnet and mask. The default value for port is **all**. Host labels are names given to lists of hosts (IP addresses, IP subnets, and hostnames). You configure a host label using the **host-label** command.
dstnet <subnet/mask> |<host_label> | srcport <port>	Optionally, specify the destination network subnet and mask, host label, or port. Use the format XXX.XXX.XXX.XXX/XX for subnet and mask. The default value for port is **all**. Host labels are names given to lists of hosts (IP addresses, IP subnets, and hostnames). You configure a host label using the **host-label** command.
l7protocol <protocol>	Specify a Layer-7 protocol.
domain-name <name>	Specify a domain name; this parameter is valid only if you specify the **l7protocol** parameter **HTTP**.
relative-path <path>	Specify a relative path. For example, the relative path for `www.riverbed.com/appliance/commandline` would be `/appliance/commandline`; this is valid only if you specify the **l7protocol** parameter **HTTP**. The relative path is the part of the URL that follows the domain name.

prio-0 <class-name> | prio-1 <class-name>| prio-2 <class-name>| prio-3 <class-name> | prio-4 <class-name>	Optionally, specify to enable QoS classification priority rules for Citrix ICA, PCoIP, or SnapMirror traffic. **Citrix ICA** When configuring QoS classification for Citrix ICA traffic, you define four QoS classes, one class for each of the four application priorities and one default class. **prio-0** through **prio-3** are the priority 0 to 3 class names, which are only valid when the **l7protocol ICA** parameter is specified. The application priority separates low-priority traffic (such as print jobs) from high-priority traffic (such as interactive screen updates). The upper bandwidth limit is defined at 100%, so that the lower-priority classes can use the full bandwidth when it is available. For the best performance, select the **packet-order** queue for each Citrix QoS class to protect the TCP stream order. The packet-order queue protects the TCP stream order by keeping track of flows that are currently inside the packet-shaping infrastructure. You create your own classes for each site. For details see, “qos classification class” on page 477. Show classes with “show qos classification” on page 73. **PCoIP** PCoIP classification using a priority supports optimized and pass-through traffic. Select a priority for the PCoIP application to separate low-priority traffic from high-priority traffic. Choose either FIFO, SFQ, or packet-order for the queue (packet-order is not required for the queue). PCoIP has eight priority levels (0 – 7) that are mapped to four QoS classes (0 -3) defined by Riverbed as follows. • **prio - 0 <class-name>** - PCoIP traffic priority 6-7 (highest priority) • **prio-1 <class-name>** - PCoIP traffic priority 5 • **prio- 2 <class-name>** - PCoIP traffic priority 4 • **prio-3 <class-name> -** PCoIP traffic priority 0-3 (lowest priority) **SnapMirror** You can specify QoS classification and priority of SnapMirror flows based on filer and volume information. Using advanced QoS, you can assign a class ID and DSCP value to each volume priority. • **prio-0 <class-name>** - SnapMirror volume priority 0 (highest priority) • **prio-1 <class-name>** - SnapMirror volume priority 1 • **prio- 2 <class-name>** - SnapMirror volume priority 2 • **prio-3 <class-name> -** SnapMirror volume priority 3 • **prio-4 <class-name> -** SnapMirror volume priority 4 (lowest priority)

out-dscp <out-dscp-value> | out-dscp-0 <out-dscp-0> | out-dscp-1 <out-dscp-1> | out-dscp-2 <out-dscp-2> | out-dscp-3 <out-dscp-3> | out-dscp-4 <out-dscp-4>	Specify the QoS class outbound DSCP marking value based on the priority. Use this parameter in conjunction with the **prio-x** parameter, which specifies priority rules for Citrix ICA, PCoIP, and SnapMirror traffic. You must specify either the **l7protocol ICA**, **l7protocol pcoip,** or **l7protocol snapmirror** parameters when specifying the outbound DSCP marking value. The system ignores other Layer 7 protocol outbound DSCP marking configurations. • **out-dscp** - Specify an outbound DSCP value. The values are **0-63**, **255** (reflect), or **254** (inherit from service class). Inherit from the service class is the default setting for a classification rule. • **out-dscp-0** - Specify the DSCP Layer 7 mark for priority 0: **0-63**, **255** or **254**. • **out-dscp-1** - Specify the DSCP Layer 7 mark for priority 1: **0-63**, **255**, or **254**. • **out-dscp-2** - Specify the DSCP Layer 7 mark for priority 2. **0-63**, **255,** or **254**. • **out-dscp-3** - Specify the DSCP Layer 7 mark for priority 3. **0-63**, **255**, or **254**. • **out-dscp-4** - Specify the DSCP Layer 7 mark for priority 3. **0-63**, **255**, or **254**.
path-1-path <path-1-name> | path-2-path <path-2-name> | path-3-path <path-3-name>	Specify the path name. Configure the available paths in the network using the **path-selection path** command.
path-1-dscp <dscp> | path-2-dscp <dscp> | path-3-dscp <dscp>	Optionally, Specify the DSCP value associated with a path. The DSCP marking values are **0-63** and **253** (inherit from rule). Specifying a DSCP value for a path is used for Policy-Based Routing (PBR) use cases. For details about PBR and path selection, see the *Steelhead Appliance Deployment Guide* and *Steelhead Appliance Management Console User's Guide*.
default-path {relay | drop}	Specify the default path-selection behavior for the rule if all paths are down: • **relay** - Route packets normally using the default path. If not configured, the default behavior is relay without applying path selection. • **drop -** Drop the connection.
description <description>	Specify a rule description.
rulenum <priority>	Optionally, specify the order in which the rule is processed in the rules list. Steelhead appliances evaluate rules in numerical order, starting with rule 1. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.
site-num <number>	The site number for this site.

Usage

Each rule maps a type of network traffic to a QoS class. You can create more than one QoS rule for a class. When more than one QoS rule is created for a class, the rules are followed in the order in which they are shown in the command, **show qos classification rules,** and only the first matching rule is applied to the class.

Using path selection, you can configure a path for each packet based on the state of your links and your network configuration. At a high level, you can configure multiple paths for each connection by specifying QoS rules based on various parameters. The Steelhead appliance monitors the state of the path, and, based on this, selects the appropriate path for a packet. You can configure a maximum of three paths per rule.

A DSCP marking value specified in a rule takes precedence over a DSCP marking value specified in a class configuration.

In hierarchical QoS, only child classes can have rules.

If you delete or add new rules, existing connections are not affected. The changes only affect new connections.

The **no** command option disables the rule.

This command is only available in advanced outbound QoS mode.

For details about Steelhead appliance QoS rule, site, and port capabilities, see the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # qos classification rule add class-name Default-Site$$Business-Critical out-
dscp-0 50 out-dscp-1 60 out-dscp-2 255 out-dscp-3 58 traffic-type passthrough srcnet 192.12.12.1/
32 srcport 80 dstnet 192.168.4.0/24 dstport 80 l7protocol ICA prio-0 Default-Site$$Business-Critical
prio-1 Default-Site$$Business-Critical prio-2 Default-Site$$Business-Critical prio-3 Default-
Site$$Business-Critical dscp 2 vlan 2 rulenum 5 site-num 1
```

Product

Steelhead appliance

Related Topics

"host-label," "show qos classification," "Path Selection Commands"

qos classification rule move

Description

Moves an existing QoS rule in the rule index to the specified number, optionally on a particular site.

Syntax

qos classification rule move from <rule> to <rule> site-num <number>

Parameters

from <rule> to <rule>	Specify the number in the rules index, which determines the rule evaluation order.
site-num <number>	In multi-site configurations, assign a number to each site. For single site configurations, the site number is 1, but the option is not required.

Usage

Steelhead appliances evaluate rules in numerical order starting with rule 1. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.

This command is available only in advanced outbound QoS mode.

Example

```
amnesiac (config) # qos classification rule move from 2 to 4 site-num 1
```

Product

Steelhead appliance

Related Topics

"show qos classification", "qos classification rule"

qos classification site add

Description

Configures advanced QoS classification parameters for the named site.

Syntax

[no] qos classification site add site-name <name> network {<IPv4 address> | all} default-class <def-class-for-site> def-out-dscp <dscp-value> [path-1 <path-1-name>] [path-1-dscp <dscp>] [path-2 <path-2-name>] [path-2-dscp <dscp>] [path-3 <path-3-name>] [path-3-dscp <dscp>] [default-path {relay | drop}] [index <number>]

Parameters

site-name <name>	Specify the name of the site.
network {<IPv4 address> | all}	Specify the network IPv4 address for the site or **all** for all IPv4 addresses. For the network address, use the format XXX.XXX.XXX.XXX.
default-class <def-class-for-site>	Specify the default class for the site. Traffic classification options are: • **Default-Site$$Business-Critical** • **Default-Site$$Interactive** • **Default-Site$$Low-Priority** • **Default-Site$$Normal** • **Default-Site$$Realtime** • **Default-Site$$Best-effort** • **Default-Site$$parent_class**
def-out-dscp <dscp-value>	Specify the DSCP mark for traffic matching the default rule in the site. The DSCP values are **0-63** or **255** (reflect). Reflect is the default setting. Reflect means that the DSCP level or IP ToS value found on pass-through traffic is unchanged when it passes through the Steelhead appliance.
path-1-path <path-1-name> | path-2-path <path-2-name> | path-3-path <path-3-name>	Specify the path name. Configure the available paths in the network using the **path-selection path** command.
path-1-dscp <dscp> | path-2-dscp <dscp> | path-3-dscp <dscp>	Specify the DSCP value associated with a path. The DSCP values are **0-63** or **253** (inherit from rule). Specifying a DSCP value for a path is used for Policy-Based Routing (PBR) use cases. For details about PBR and path selection, see the *Steelhead Appliance Deployment Guide* and *Steelhead Appliance Management Console User's Guide*.
default-path {relay | drop}	Specify the default path behavior for the rule if all paths are down: • **relay** - Route packets normally using the default path (relay). • **drop -** Drop the connection (drop).
index <number>	Specify the position in the QoS index.

Usage

A site is a logical grouping of subnets. Sites represent the physical and logical topology of a site type. You can classify traffic for each site using network addresses. Site types are typically data center, small, medium and large branch office, and so on. Each site uses a bandwidth policy, and the sites have an order. Traffic is matched to the first matching site. For details on site rules and the number of recommended maximum sites, see the*Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

The default site is a catch-all site that has a subnet of 0.0.0.0/0. You do not need to add a remote site if you only have one remote site and the default site is suitable.

This command is available only in advanced outbound QoS mode.

Example

```
amnesiac (config) # qos classification site add site-name mySite network 192.168.4.0/24 default-
class Default-Site$$Best-effort
```

Product

Steelhead appliance

Related Topics

"show qos classification", "qos classification rule", "qos classification site edit", "qos classification site move"

qos classification site edit

Description

Modifies the site name, IP address, and class of a site.

Syntax

[no] qos classification site edit site-name <name> {add-network network {<IPv4 address> | all} | def-out-dscp <dscp-value>| default-class <class> | path-1 <path-1-name> [path-1-dscp <dscp>] [path-2 <path-2-name>] [path-2-dscp <dscp>] [path-3 <path-3-name>] [path-3-dscp <dscp>] [default-path {relay | drop}]}

Parameters

site-name <name>	Specify the name of the site.
add-network network {<IPv4 address> | all}	Specify the network IPv4 prefix for the site or **all** for all IPv4 addresses. For the network address, use the format XXX.XXX.XXX.XXX.
def-out-dscp <dscp-value>	Specify the DSCP mark for traffic matching the default rule in the site.
default-class <class>	Specify the default class for the site. Traffic classification options are: • **Default-Site$$Business-Critical** • **Default-Site$$Interactive** • **Default-Site$$Low-Priority** • **Default-Site$$Normal** • **Default-Site$$Realtime** • **Default-Site$$Best-effort** • **Default-Site$$parent_class**
path-1-path <path-1-name> | path-2-path <path-2-name> | path-3-path <path-3-name>	Specify the path name. Configure the available paths in the network using the **path-selection path** command.
path-1-dscp <dscp> | path-2-dscp <dscp> | path-3-dscp <dscp>	Specify the DSCP value associated with a path.
default-path {relay | drop}	Specify the default path behavior for the rule if all paths are down: • **relay**- Route packets normally using the default path (relay). • **drop -** Drop the connection (drop).

Usage

For details on site rules and the number of recommended maximum sites, see the*Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

This command is available only in advanced QoS mode.

Example

```
amnesiac (config) # qos classification site edit site-name MyTestSite add-network 2.2.0.0/16
amnesiac (config) # qos classification site edit site-name MyTestSite path-1 primary path-1-dscp 20
path-2 secondary path-2-dscp 255 default-path relay
```

Product

Steelhead appliance

Related Topics

"qos classification rule," "qos classification site add," "show qos classification"

qos classification site move

Description

Moves the QoS site position in the index.

Syntax

qos classification site move from <position> to <position>

Parameters

from <position>	Specify the numeric position in the index.
to <position>	Specify the numeric position in the index.

Usage

Steelhead appliances evaluate rules in numerical order called an index, starting with rule 1. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.

This command is available only in advanced outbound QoS mode.

Example

```
amnesiac (config) # qos classification site move from 4 to 1
```

Product

Steelhead appliance

Related Topics

"qos classification rule," "qos classification site edit," "show qos classification"

qos shaping enable

Description

Enables advanced QoS shaping configuration.

Syntax

[no] qos shaping enable

Parameters

None

Usage

QoS is a reservation system for network traffic in which you create QoS classes to distribute network resources. The classes are based on traffic importance, bandwidth needs, and delay-sensitivity. You allocate network resources to each of the classes. Traffic flows according to the network resources allocated to its class.

You can configure QoS on Steelhead appliances to control the prioritization of different types of network traffic and to ensure that Steelhead appliances give certain network traffic (for example, VoIP) higher priority over other network traffic.

QoS allows you to specify priorities for various classes of traffic and properly distribute excess bandwidth among classes. The QoS classification algorithm provides mechanisms for link sharing, real-time, and priority services while decoupling delay and bandwidth allocation.

QoS classes set priorities and bandwidths. You can create multiple QoS classes. There is no requirement that QoS classes represent applications, traffic to remote sites, or any other particular aggregation.

The QoS classes that are always present in Advanced QoS on the Steelhead appliance are:

- **Root Class** - The root class is used to constrain the total outbound rate of traffic leaving the Steelhead appliance to the configured, per-link WAN bandwidth. This class is not configured directly, but is created when you enable QoS classification and enforcement on the Steelhead appliance.
- **Built-in Default Class** - The QoS scheduler applies the built-in default class constraints and parameters on traffic not otherwise placed in a class by the configured QoS rules.

QoS classes are configured in one of two different modes: *flat* or *hierarchical*. The difference between the two modes primarily consists of how QoS classes are created.

Traffic is not classified until at least one WAN interface is enabled. QoS classification occurs during connection setup for optimized traffic, before optimization and compression. QoS shaping and enforcement occurs after optimization and compression. By design, QoS is applied to both pass-through and optimized traffic. QoS is implemented in the operating system; it is not a part of the optimization service. When the optimization service is disabled, all the traffic is passed through and is still shaped by QoS.

For details, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

The **no** command option disables advanced QoS. A service restart is required if you disable QoS.

Example

```
amnesiac (config) # qos shaping enable
```

Product

Steelhead appliance

Related Topics

"show qos classification"

qos shaping interface

Description

Enables and sets the bandwidth link-rate for the specified WAN interface.

Syntax

[no] qos shaping interface <interface> [enable] | [curve-burst <kbits>] | [rate <Kbps>]

Parameters

<interface>	Specify the interface for which to enable, set the link rate, or set the curve-burst. For example, **wan0_0**
enable	Optionally enable QoS classification on the interface.
curve-burst <kbits>	Optionally specify the QoS curve burst size. Sets bandwidth for traffic bursts greater than the upper bandwidth limit. This option is available in the CLI only.
rate <Kbps>	Optionally specify the link rate in Kbps.

Usage

You can set the rate for an interface before it is enabled. You must enable the interface to use QoS on that interface.

This rate is the *bottleneck* WAN bandwidth and not the interface speed out of the WAN interface into the router or switch. For example, if your Steelhead appliance connects to a router with a 100 Mbps link, do not specify this value—specify the actual WAN bandwidth (for example, T1, T3).

Different WAN interfaces can have different WAN bandwidths; this value must be correctly entered for QoS to function correctly.

The percentage of excess bandwidth given to a class is relative to the percentage of minimum bandwidth allocated to the class.

The **curve-burst** option sets the amount of burst allowed for real-time QoS classes at the link rate. During this burst, all other traffic is suppressed. The formula for the burst rate is:

```
    burst = 25% of (link-rate kb/sec * 1 sec)
```

Therefore, the burst rate changes as the link rate changes.

The **no** command option disables the specified command option.

Example

```
amnesiac (config) # qos shaping interface wan0_0 rate 1200
amnesiac (config) # qos shaping interface wan0_0 enable
```

Product

Steelhead appliance, CSH

Related Topics

"show qos classification"

Inbound QoS Commands

qos inbound class

Description

Adds or modifies the specified inbound QoS shaping class.

Syntax

qos inbound class {add | modify} class-name <classname> priority {realtime | interactive | business | normal | low | best-effort} min-pct <min bw percent> [upper-limit-pct <upper-limit pct>] [link-share <weight>]

Parameters

{add | modify}	Specify whether to add or modify a new inbound QoS class.
class-name <classname>	Specify a name for the QoS class. You can create up to 200 inbound QoS classes.
priority {realtime | interactive | business| normal| low| best-effort}	Specify a minimum guaranteed QoS priority level. The latency priority indicates how delay-sensitive a traffic class is to the QoS scheduler. Select the latency priority for the class (highest priority to lowest priority): • **realtime**- Specify a real-time traffic class. Traffic that is your highest priority should be given this value, for example, VoIP, video conferencing. • **interactive** - Specify an interactive traffic class: for example, Citrix, RDP, telnet and ssh. • **business** - Specify the business critical traffic class: for example, Thick Client Applications, ERPs, and CRMs • **normal** - Specify a normal priority traffic class: for example, Internet browsing, file sharing, and email. • **low** - Specify a low priority traffic class: for example, FTP, backup, replication, other high-throughput data transfers, and recreational applications such as audio file sharing. • **best-effort** - Specify the lowest priority.
min-pct <min bw percent>	Specify the minimum amount of bandwidth given to a flow when there is bandwidth contention (minimum bandwidth guarantee). Flows that do not use all of their allocated minimum bandwidth will share this excess bandwidth with other flows that exceed their minimum bandwidth allocation. All the classes combined cannot exceed 100%. During contention for bandwidth, the class is guaranteed at least to the amount of specified bandwidth. It will receive more if there is unused bandwidth remaining. The guaranteed bandwidth calculated based on this percentage should be no less than 1Kbps. For example, if the **wan0_0** throughput is 1000 Kbps, and a first-level class has its guaranteed bandwidth of 0.1%, this results in a bandwidth of 1000 * 0.1% = 1Kbps.
upper-limit-pct <upper-limit pct>	Specify the upper limit percent settings for the class. Specify the maximum allowed bandwidth (as a percentage) a class receives as a percentage of the parent class guaranteed bandwidth. The limit is applied even if there is excess bandwidth available.
link-share <weight>	Specify the weight for the class. This parameter applies to flat mode only. The link share weight determines how the excess bandwidth is allocated among sibling classes. Link share does not depend on the minimum guaranteed bandwidth. By default, all the link shares are equal. Classes with a larger weight are allocated more of the excess bandwidth than classes with a lower link share weight.

Usage

QoS inbound classification controls the prioritization of different types of inbound network traffic to ensure that the Steelhead gives certain network traffic (for example, Voice Over IP) higher priority than other network traffic. Traffic is not classified until at least one WAN interface is enabled. Inbound QoS does not support hierarchical class configuration.

The **no qos inbound class class-name <name>** command option deletes an existing QoS inbound class.

For details about QoS classes, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # qos inbound class add class-name Business_Apps priority normal min-pct 30 upper-
limit-pct 100

amnesiac (config) # qos inbound class modify class-name Business_Apps min-pct 45 upper-limit-pct 50
priority business
```

Product

Steelhead appliance

Related Topics

"show qos inbound classes"

qos inbound enable

Description

Enables inbound QoS shaping.

Syntax

[no] qos inbound enable

Parameters

None

Usage

By default, inbound QoS is disabled. The **no** version of the command disables QoS inbound enforcement if it has been enabled.

Example

```
amnesiac (config) # qos inbound enable
```

Product

Steelhead appliance

Related Topics

"show qos inbound"

qos inbound interface enable

Description

Enables inbound QoS on the specified interface.

Syntax

[no] qos inbound interface <interface-name> enable

Parameters

<interface-name>	Specify an interface name.

Usage

Inbound QoS supports in-path interfaces only; it does not support primary or auxiliary interfaces.

Example

```
amnesiac (config) # qos inbound interface wan0_0 enable
```

Product

Steelhead appliance

Related Topics

"show qos inbound"

qos inbound interface rate

Description

Configures the inbound WAN bandwidth rate for the specified interface.

Syntax

qos inbound interface <name> rate <rate>

Parameters

<name>	Specify an interface name.
<rate>	Specify the inbound QoS shaping rate in Kbps.

Usage

Inbound QoS supports in-path interfaces only; it does not support primary or auxiliary interfaces.

Example

```
amnesiac (config) # qos inbound interface wan0_0 rate 1500
```

Product

Steelhead appliance

Related Topics

"show qos inbound"

qos inbound rule

Description

Creates or modifies an inbound QoS traffic classification rule.

Syntax

[no] qos inbound rule {add class-name <class-name> [rulenum <rulenum>] | modify rulenum <rulenum>} [rule-name <rule-name>] [description <description>] [traffic-type {all | optimized |passthrough}] [vlan <vlan-id>] [dscp <dscp-value>] [protocol <protocol>] [srcnet {<src-network> | <host_label>}] [srcport <src-port>] [dstnet {<dst-network> | <host-label>}] [dstport <dst-port] [l7protocol <dpi-protocol>] [domain-name <http-domain-name>] [relative-path <http-relative-path>]

Parameters

<class-name>	Specify the class to which the rule applies. If the rule matches, the specified rule sends the packet to this class.
rulenum <rulenum>	Specify the order in which the rule is processed in the rules list. Steelhead appliances evaluate rules in numerical order, starting with rule 1. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.
rule-name <name>	Specify a rule name.
description <description	Specify a description of the rule.
traffic-type {all | optimized |passthrough}	Specify the type of traffic. The default value is **all**.
vlan <vlan-id>	Optionally, specify the VLAN tag ID.
dscp <dscp-value>	Optionally, specify a DSCP level (**0-63**). Use this option to configure a QoS rule matching a specific DSCP mark.
protocol {all | udp | tcp | gre | icmp | ipsec}	Specify the protocol for the rule.
srcnet <subnet/mask> |<host_label>	Specify the subnet and mask or host label for the source network. Use the format XXX.XXX.XXX.XXX/XX for subnet and mask. Host labels are names given to lists of hosts (IP addresses, IP subnets, and hostnames). You configure a host label using the **host-label** command.
srcport <src-port>	Specify the remote port settings. The default value for port is **all**.
dstnet <subnet/mask> |<host_label>	Specify the subnet and mask or host label for the local subnet. Use the format XXX.XXX.XXX.XXX/XX for subnet and mask. Host labels are names given to lists of hosts (IP addresses, IP subnets, and hostnames). You configure a host label using the **host-label** command.
dstport <dst-port	Specify the local port settings. The default value for port is **all**.
l7protocol <dpi-protocol>	Specify a layer-7 protocol name.
domain-name <http-domain-name>	Specify a domain name. This option is only valid if you specify the **l7protocol HTTP** option.
relative-path <http-relative-path>	Specify a relative path. For example, the relative path for `www.riverbed.com/appliance/commandline` would be `/appliance/commandline`. Only valid if you specify the **l7protocol** protocol **HTTP**. The relative path is the part of the URL that follows the domain name

Usage

Each rule maps a type of network traffic to a QoS class. You can create more than one QoS rule for a class. When more than one QoS rule is created for a class, the rules are followed in the order in which they are shown in the command, **show qos inbound rules,** and only the first matching rule is applied to the class. Steelhead appliances support up to 500 inbound QoS rules.

For details on Steelhead appliance QoS rule, site, and port capabilities, see the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # qos inbound rule add class-name Business_Apps rule-name Wiki description
```

```
"Internal Wiki Server" l7protocol HTTP domain-name wikiserver.riverbed.com

amnesiac (config) # qos inbound rule modify rulenum 2 class-name Wiki_Apps srcnet 10.1.1.0/24
```

Product

Steelhead appliance

Related Topics

"show qos inbound rules"

qos inbound rule move

Description

Moves the rule to a new position.

Syntax

qos inbound rule move from <rulenum> to <rulenum>

Parameters

from <rulenum>	Specify the numeric position in the index.
to <rulenum>	Specify the numeric position in the index.

Usage

Steelhead appliances evaluate rules in numerical order called an index, starting with rule 1. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.

Example

```
amnesiac (config) # qos inbound rule move from 3 to 4
```

Product

Steelhead appliance

Related Topics

"show qos inbound rules"

DSCP QoS Commands

By default, Steelhead appliances reflect the differentiated services code point (DSCP) or IP ToS value found on pass-through traffic and optimized connections. This means that the DSCP or IP ToS value on pass-through traffic is unchanged when it passes through the Steelhead appliance.

After you map a source-destination-port pattern and a DSCP level, every packet corresponding to the connection with that destination port has the DSCP field set to that value in the forward and backward direction. On the WAN side of the Steelhead appliance, you configure a network router or a traffic shaper to prioritize packets according to the value in the DSCP field before they are sent across the WAN. Enabling these features is optional.

In RiOS v5.5 and earlier, the DSCP parameter of a QoS classification rule matches the DSCP value before DSCP marking rules are applied. In RiOS 6.0.x and v6.1.x, the DSCP field in a QoS classification rule matches the DSCP value after DSCP marking rules are applied; that is, it matches the post-marking DSCP value.

In RiOS v6.5, the DSCP field in a QoS classification rule for pass-through traffic matches the DSCP value before DSCP marking rules are applied. The DSCP field in a QoS classification rule for optimized traffic matches the DSCP value after DSCP marking rules are applied; that is, it matches the post-marking DSCP value.

In RiOS v7.0, the DSCP field in a QoS classification rule for pass-through traffic matches the DSCP value after DSCP marking rules are applied. The DSCP field in a QoS classification rule for optimized traffic matches the DSCP value before DSCP marking rules are applied; that is, it matches the pre-marking DSCP value.

In RiOS v7.0, the DSCP or IP TOS marking only has local significance. This means that you can set the DSCP or IP TOS values on the server-side Steelhead appliance to values different to those set on the client-side Steelhead appliance.

qos control-packets

Description

Configures WAN control packet settings.

Syntax

[no] qos control-packets dscp <dscp>

Parameters

dscp <dscp>	Specify the DSCP marking for control packets. The DSCP values are **0-64** or **255** (reflect).

Usage

The **qos control-packets** command defines the global DSCP marking.

Example

```
amnesiac (config) # qos control-packets dscp 4
```

Product

Steelhead appliance

Related Topics

"show qos control-packets dscp"

qos basic dscp-marking enable

Description

Enables DSCP marking in QoS basic mode.

Syntax

[no] qos basic dscp-marking enable

Parameters

None

Usage

In RiOS v7.0, the DSCP or IP TOS marking only has local significance. This means you can set the DSCP or IP TOS values on the server-side Steelhead appliance to values different to those set on the client-side Steelhead appliance.

In RiOS v7.0, if you have not configured either basic or advanced outbound Qos in the previous version of RiOS:

- The system migrates to advanced outbound QoS mode, sets the default class to DSCP reflect and the QoS configuration to use the default QoS rule.

- Because the server-side Steelhead appliance in RiOS v7.0 and later uses its local rules table for QoS marking instead of relying on the rules configured on the client-side Steelhead appliance, both the client-side and server-side Steelhead appliances must be running 7.0 or later.

The **no** version of the command disables DSCP marking.

Example

```
amnesiac (config) # qos basic dscp-marking enable
```

Product

Steelhead appliance

Related Topics

"show qos classification"

---

qos dscp-marking enable

Description

Enables DSCP marking in QoS advanced mode.

Syntax

[no] qos dscp-marking enable

Parameters

None

Usage

In RiOS v7.0, the DSCP or IP TOS marking only has local significance. This means you can set the DSCP or IP TOS values on the server-side Steelhead appliance to values different to those set on the client-side Steelhead appliance.

In RiOS v7.0, if you have not configured either basic or advanced outbound Qos in the previous version of RiOS:

- The system migrates to advanced outbound QoS mode, sets the default class to DSCP reflect and the QoS configuration to use the default QoS rule.
- Because the server-side Steelhead appliance in RiOS v7.0 and later uses its local rules table for QoS marking instead of relying on the rules configured on the client-side Steelhead appliance, both the client-side and server-side Steelhead appliances must be running 7.0 or later.

The **no** version of the command disables DSCP marking.

Example

```
amnesiac (config) # qos dscp-marking enable
```

Product

Steelhead appliance

Related Topics

"show qos classification"

Host Label Commands

This section describes the host label commands.

---

host-label

Description

Configures host label settings.

Syntax

[no] host-label <name> {hostname <hostname> [subnet X.X.X.X/XX] | subnet X.X.X.X/XX [hostname <hostname>]}

Parameters

<name>	Specify the name of the host label. • Host labels are case sensitive and can be any string consisting of letters, the underscore (_), or the hyphen (-). There cannot be spaces in host labels. There is no limit on the number of host labels you can configure. • To avoid confusion, do not use a number for a host label. • Host labels that are used in QoS rules cannot be deleted. • Host label changes (that is, adding and removing hostnames inside a label) are applied immediately by the rules that use the host labels that you have modified.
hostname <hostname, . . .>	Specify a hostname or a comma-separated list of hostnames. • Hostnames are case insensitive. • You can configure a maximum of 100 unique hostnames across all host labels. • A maximum of 64 subnets and hostnames per host label is allowed.
subnet <X.X.X.X/ XX>, . . .	Specify an IPv4 subnet for the specified host label or a comma-separated list of IPv4 subnets. Use the format X.X.X.X/XX.

Usage

Host labels are names given to lists of hosts (IP addresses, IP subnets, and hostnames) that you can specify to match the source and destination network when configuring QoS rules. For example, you can specify host labels to define a set of hosts for which QoS classification and QoS marking rules apply. You can configure a mixture of subnets and hostnames for each label. A maximum of 64 subnets and hostnames per host label is allowed. You can configure a maximum of 100 unique hostnames across all host labels.

Hostnames referenced in a host label are automatically resolved through a DNS. The system resolves them immediately after you add a new host label or after you edit an existing host label. The system also automatically re-resolves hostnames once daily. If you want to resolve a hostname immediately, use the **resolve host-labels** command.

Example

```
amnesiac (config) # host-label test hostname riverbed.com,example.com subnet 192.168.0.1/32,
192.168.0.2/32,10.0.0.0/8
```

```
amnesiac (config) # qos basic classification global-app add global-app-name MyGlobalApp class-name
Realtime vlan 1 traffic all srcport 123 srcnet test
```

Product

CMC, Steelhead appliance

Related Topics

"QoS Support Commands," "resolve host-labels," "show host-label"

resolve host-labels

Description

Forces the system to resolve host labels immediately.

Syntax

resolve host-labels

Parameters

None

Usage

You can use the **resolve host-labels** command to force a resolve operation instead of waiting for the daily automatic resolve instance. Every time this command is executed, the next automatic resolve instance is reset to occur 24 hours later.

Example

```
amnesiac # resolve host-labels
```

Product

CMC, Steelhead appliance

Related Topics

"host-label," "show host-label"

Port Label Commands

This section describes the port label commands.

port-label

Description

Configures port label settings. Port labels are names given to sets of ports. When you configure rules for feature implementation, you can specify port labels instead of port numbers to reduce the number of in-path rules.

Syntax

[no] port-label <name> port <port>

Parameters

<name>	Specify the name of the port label. Port labels are not case sensitive and can be any string consisting of letters, numbers, underscore (_), or a hyphen (-).
<port>	Specify a comma-separated list of ports and ranges of ports. For example: 22,443,990-995,3077-3078

Usage

The Riverbed system includes the following default port labels:

Secure - Contains ports that belong to the system label for secure ports. The Steelhead appliance automatically passes through traffic on commonly secure ports (for example, ssh, https, and smtps). For a list of secure ports, see Appendix A, "Riverbed Ports."

Interactive - Contains ports that belong to the system label for interactive ports. The Steelhead appliance automatically passes through traffic on interactive ports (for example, Telnet, TCP ECHO, remote logging, and shell). For a list of interactive ports, see Appendix A, "Riverbed Ports."

- **RBT-Proto** - Contains ports that belong to the label for system processes: 7744 (data store synchronization), 7800-7801 (in-path), 7810 (out-of-path), 7820 (failover), 7850 (connection forwarding), 7860 (Interceptor appliance), 7570 (Steelhead Mobile Controller).
- **All** - Contains all ports that have been discovered by the system. This label cannot be modified.
- **Unknown** - Contains ports that have been discovered by the system that do not belong to another port label (besides **All**). Riverbed appliances automatically discover active ports. Activity for the discovered port is included in the Traffic Summary report. If a port label contains the discovered port, the report reflects this. If a label does not exist, the port activity is labeled **unknown**. You can create an appropriately descriptive port label for activity on such ports. All statistics for this new port label are preserved from the time the port was discovered.

You can use the **port-label FOO port <port>** command to add or modify ports in a port label. For example you define port label FOO by issuing following the command.

```
    (config)# port-label FOO port 2-9,14
```

If you want to add ports to the FOO port label:

```
   (config)# port-label FOO port 10-20
```

If you run the **show port-label FOO** command, you will see the new range of ports from 2 to 20.
The **no** command option removes the port label for the specified port label.

Example

```
amnesiac (config) # port-label foo port 22,443,990-995,3077-3078
amnesiac (config) # show port-label foo
Port Label: foo
22,443,990-995,3077-3078
```

Product

Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show port-label"

FTP Support Commands

This section describes the FTP support commands.

protocol ftp port

Description

Configures FTP port settings.

Syntax

[no] protocol ftp port <port>

Parameters

port <port>	Specify the FTP port.

Usage

The **no** command option disables the FTP port.

Example

```
amnesiac (config) # protocol ftp port 2243
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ftp"

protocol ftp port enable

Description

Enables FTP port settings.

Syntax

[no] protocol ftp port <port> enable

Parameters

port <port>	Specify the FTP port.

Usage

The **no** command option disables the FTP port.

Example

```
amnesiac (config) # protocol ftp port 2243 enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ftp"

Domain and Workgroup Commands

This section describes the Domain and Workgroup commands. The domain commands apply to the following features:

- SMB signing delegation trust for CIFS optimizations and SMB2 signing. For SMB, SMB2, and SMB3 signing commands, see "CIFS, SMB, SMB2, and SMB3 Support Commands" on page 518.
- MAPI 2007 encrypted traffic optimization authentication. For details, see "MAPI Support Commands" on page 560.
- PFS. For details, see "PFS Support Commands" on page 613 or the *Riverbed Central Management Console User's Guide*.

domain cancel-event

Description

Cancels domain action.

Syntax

domain cancel-event

Parameters

None

Example

```
amnesiac (config) # domain cancel-event
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show domain"

domain check

Description

Configures the system to require a domain check upon startup.

Syntax

[no] domain check

Parameters

None

Example

```
amnesiac (config) # domain check
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show domain"

domain join

Description

Configures a Windows domain.

Syntax

domain join domain-name <name> login <login> password <password> [dc-list <dc-list>] [org-unit <name>] [join-type {workstation | win2k8-mode | win2k3-mode}] [short-name <name>] [netbios-name <name>]

Parameters

domain-name <name>	Specify the domain of which to make the Steelhead appliance a member of. Typically, this is your company domain name. RiOS supports Windows 2000 or later domains.
login <login>	Specify the login for the domain. The login and password are not stored. This account must have domain-join privileges; it does not need to be a domain administrator account.
password <password>	Specify the password for the domain. The login and password are not stored.
dc-list <dc-list>	Optionally, specify the domain controllers (hosts) that provide user login service in the domain. (Typically, with Windows 2000 Active Directory Service domains, given a domain name, the system automatically retrieves the DC name.) **Note:** Specifying the domain controller name in high-latency situations reduces the time to join the domain significantly. **Note:** The **dc-list** parameter is required when the join type is **win2k8-mode**. The DC list should contain only the names or IP addresses of Windows 2008 and later domain controllers.
org-unit <name>	Specify the organization name (for example, the company name).
join-type {workstation | win2k8-mode | win2k3-mode}	Optionally, specify the join account type in which the server-side Steelhead appliance can join the domain in one of the following roles: • **workstation** - Joins the server-side Steelhead appliance to the domain with workstation privilege. You can join the domain to this account type using any ordinary user account that has the permission to join a machine to the domain. • **win2k8-mode** - Active Directory integrated mode for Windows 2008 and later • **win2k3-mode** - Active Directory integrated mode for Windows 2003 If you do not specify a join type, the system uses the default, which is the workstation join type. The **dc-list** parameter is required when the join type is **win2k8-mode**. The DC list should contain only the names or IP addresses of Windows 2008 and higher domain controllers.
short-name <name>	Optionally, specify a short domain name. Typically, the short domain name is a substring of the realm. In rare situations, this is not the case, and you must explicitly specify the short domain name. Case matters; NBTTECH is not the same as nbttech. The short domain name is required if the NetBIOS domain name does not match the first portion of the Active Directory domain name.
netbios-name <name>	Specify a NetBIOS name. The short domain name is required if the NetBIOS domain name does not match the first portion of the Active Directory domain name.

Usage

A server-side Steelhead appliance can join a Windows domain or local workgroup. You configure the Steelhead appliance to join a Windows domain (typically, the domain of your company) for PFS, SMB signing, and MAPI encrypted traffic optimization authentication.

When you configure the Steelhead appliance to join a Windows domain, you do not have to manage local accounts in the branch office, as you do in local workgroup mode. Domain mode allows a domain controller (DC) to authenticate users.

If the server-side Steelhead appliance is running a version of RiOS between v6.1 and v6.5, it can only join the domain to appear as a *Workstation*. In RiOS v7.0 and later, the Steelhead appliance can join the domain in one of three different roles: Workstation, Active Directory Integrated (Windows 2003) or Active Directory Integrated (Windows 2008). Domain users are allowed to use the Kerberos delegation trust facility and/or NTLM environments for encrypted MAPI or SMB signing based on the access permission settings provided for each user.

When the Steelhead appliance joins as one of the Active Directory integrated roles, it has very limited functionality. Even though the Steelhead appliance is integrated with Active Directory, it does not provide any Windows domain controller functionality to any other machines in the domain.

When the Steelhead appliance is joined to the domain as part of a proxy file server (PFS) deployment, data volumes at the data center are configured explicitly on the proxy-file server and are served locally by the Steelhead appliance. As part of the configuration, the data volume and ACLs from the origin-file server are copied to the Steelhead appliance.

Before enabling domain mode, make sure that you:

- configure the DNS server correctly. The configured DNS server must be the same DNS server to which all the Windows client computers point. To use SMB signing, the server-side Steelhead appliance must be in the DNS.
- have a fully qualified domain name. This domain name must be the domain name for which all the Windows desktop computers are configured.
- set the owner of all files and folders in all remote paths to a domain account and not a local account.

Note: PFS supports only domain accounts on the origin-file server; PFS does not support local accounts on the origin-file server. During an initial copy from the origin-file server to the PFS Steelhead appliance, if PFS encounters a file or folder with permissions for both domain and local accounts, only the domain account permissions are preserved on the Steelhead appliance.

For details about domains and PFS, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # domain join domain-name signing.test login admin password mypassword dc-list
mytestdc1
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"domain rejoin,""show domain"

domain rejoin

Description

Rejoins a domain.

Syntax

domain rejoin login <login> password <password> [dc-list <dc-list>] [join-type {workstation | win2k8-mode | win2k3-mode}] [short-name <name>] [netbios-name <name>]

Parameters

login <login>	Specify the login for the domain. The login and password are not stored. **Note:** This account must have domain-join privileges; it does not need to be a domain administrator account.
password <password>	Specify the domain password. The password is not stored.
dc-list <dc-list>	Specify a list of domain controller names, separated by commas. The **dc-list** parameter is required when the join type is **win2k8-mode**. The DC list should contain only the names or IP addresses of Windows 2008 and later domain controllers.
join-type {workstation | win2k8-mode | win2k3-mode}	Optionally, specify the join account type in which the server-side Steelhead appliance can join the domain in one of the following roles: • **workstation** - Workstation • **win2k8-mode** - Active Directory integrated (Windows 2008 and later) • **win2k3-mode** - Active Directory integrated (Windows 2003) If you do not specify a join type, the Steelhead appliance uses the default behavior and joins the domain as a workstation join type. The **dc-list** parameter is required when the join type is **win2k8-mode**. The DC list should only contain the names or IP addresses of Windows 2008 and higher domain controllers.
short-name <name>	Optionally, specify a short domain name. Typically, the short domain name is a substring of the realm. In rare situations, this is not the case, and you must explicitly specify the short domain name. Case matters; NBTTECH is not the same as nbttech. The short domain name is required if the NetBIOS domain name does not match the first portion of the Active Directory domain name.
netbios-name <name>	Specify a NetBIOS name. The short domain name is required if the NetBIOS domain name does not match the first portion of the Active Directory domain name.

Usage

The Steelhead appliance rejoins the same domain as specified by the **domain join** command.

Example

```
amnesiac (config) # domain rejoin login admin password mypassword
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"domain join,""show domain"

domain leave

Description

Enables the system to leave a domain.

Syntax

domain leave

Parameters

None

Example

```
amnesiac (config) # domain leave
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show domain"

domain require

Description

Configures the system to require a domain.

Syntax

[no] domain require

Parameters

None

Example

```
amnesiac (config) # domain require
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show domain"

workgroup account add

Description

Adds a local user to the local workgroup.

Syntax

workgroup account add username <local user> password <password>

Parameters

username <local user>	Specify a local user name for the Local Workgroup.
password <password>	Specify a local password for the Local Workgroup.

Example

```
amnesiac (config) # workgroup account add username myuser password mypass
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show workgroup account," "show workgroup configuration," "show workgroup status"

workgroup account modify

Description

Modifies a local user settings for the local workgroup.

Syntax

workgroup account modify username <local user> password <password>

Parameters

username <local user>	Specify a local user name for the Local Workgroup.
password <password>	Specify a local password for the Local Workgroup.

Example

```
amnesiac (config) # workgroup account modify username myuser password userpass
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show workgroup account," "show workgroup configuration," "show workgroup status"

workgroup account remove

Description

Removes a local user from the local workgroup.

Syntax

workgroup account remove username <local user> password <password>

Parameters

username <local user>	Specify a local user name for the domain.
password <password>	Specify a local password for the domain.

Example

```
amnesiac (config) # workgroup account remove username myuser password userpass
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show workgroup account," "show workgroup configuration," "show workgroup status"

workgroup join

Description

Configures the system to join a Windows local workgroup.

Syntax

workgroup join <workgroup>

Parameters

<workgroup>	Specify the name of the Local Workgroup you want to join. If you configure in Local Workgroup mode the Steelhead appliance does not need to join a domain. Local Workgroup accounts are used by clients when they connect to the Steelhead appliance. **Note:** PFS, MAPI 2007, SMB signing, or SMB2 signing must be enabled and Local Workgroup Settings must be selected before you can set the Workgroup Name. After you have set a Workgroup Name, click Join.

Usage

In Local Workgroup mode, you define a workgroup and add individual users that have access to the Steelhead appliance. The Steelhead appliance does not join a Windows domain.

Use Local Workgroup mode in environments where you do not want the Steelhead appliance to be a part of a Windows domain. Creating a workgroup eliminates the need to join a Windows domain and simplifies the configuration process.

Note: If you use Local Workgroup mode you must manage the accounts and permissions for the branch office on the Steelhead appliance. The Local Workgroup account permissions might not match the permissions on the origin-file server.

Example

```
amnesiac (config) # workgroup join myworkgroup
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show workgroup account," "show workgroup configuration," "show workgroup status"

workgroup leave

Description

Configures the system to leave a Windows workgroup.

Syntax

workgroup leave

Parameters

None

Example

```
amnesiac (config) # workgroup leave
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show workgroup account," "show workgroup configuration," "show workgroup status"

Windows Domain Health Check Commands

Windows Domain Health Check commands identify, diagnose, and report possible problems with a Steelhead appliance within a Windows domain environment. These commands also automatically configure a delegation or replication account with the privileges needed for constrained delegation or Kerberos replication. The Windows domain health check on the Steelhead appliance does not create the delegate or replication user; the Windows domain administrator must create the account in advance.

protocol domain-auth auto-conf delegation adminuser

Description

Automatically configures constrained delegation settings. This command adds or deletes CIFS, SMB2/3, or Exchange servers to or from the delegation user's msDS-AllowedToDelegateTo list.

Syntax

protocol domain-auth auto-conf delegation {add-server | delete-server} adminuser <name> adminpass <password> domain <name> dc <dcname> service { cifs | exchangeMDB} serverlist <serverlist>

Parameters

{add-server | delete-server}	Adds or deletes servers to and from the msDS-Allowed-ToDelegateTo Active Directory attribute.
adminuser <name>	Specify the user name of the domain administrator.
adminpass <password>	Specify the password of the domain administrator.
domain <name>	Specify the domain name of the delegation domain.
dc <dcname>	Specify the name of the domain controller.
service {cifs | exchangeMDB}	Specify a service: • **cifs** - CIFS service • **exchangeMDB** - Exchange service
serverlist <serverlist>	Specify a list of delegation server names, by commas.

Usage

Use the **protocol domain-auth auto-conf delegation adminuser** command to add or delete CIFS, SMB2/3, or Exchange servers to or from the delegation user's msDS-AllowedToDelegateTo Active Directory attribute. After they are in the list, the servers are eligible for optimization as specified by the **service** parameter.

The delegation user must have administrator-level privileges to use this command. If the delegation user has autodelegation privileges, no administrator-level privileges are needed.

Example

```
amnesiac (config) # protocol domain-auth auto-conf delegation add-server adminuser Administrator
adminpass password domain company.exchange.com dc exchange-dc service exchangeMDB serverlist
exch1,exch2,exch2
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth auto-conf delegation"

protocol domain-auth auto-conf delegation domain

Description

Automatically configures constrained delegation settings. This command adds or deletes CIFS, SMB2/3, or Exchange servers to or from the delegation user's msDS-AllowedToDelegateTo list.

Syntax

protocol domain-auth auto-conf delegation {add-server | delete-server} domain <name> dc <dcname> service {cifs | exchangeMDB} serverlist <serverlist>

Parameters

{add-server | delete-server}	Adds or deletes servers to and from the msDS-Allowed-ToDelegateTo Active Directory attribute.
domain <name>	Specify the name of the delegation domain.
dc <dcname>	Specify the name of the domain controller.
service {cifs | exchangeMDB}	Specify a service: • **cifs** - CIFS service • **exchangeMDB** - Exchange service
serverlist <serverlist>	Specify a list of delegation server names, by commas.

Usage

Use the **protocol domain-auth auto-conf delegation domain** command to add or delete CIFS, SMB2/3, or Exchange servers to or from the delegation user's msDS-AllowedToDelegateTo Active Directory attribute. After they are in the list, the servers are eligible for optimization as specified by the **service** parameter.

If the delegation user has autodelegation privileges, no administrator-level privileges are required.

This command is identical to the **protocol domain-auth auto-conf delegation adminuser** command except that administrator-level privileges are not required.

Example

```
amnesiac (config) # protocol domain-auth auto-conf delegation add-server domain
company.exchange.com dc exchange-dc service exchangeMDB serverlist exch1,exch2,exch2
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth auto-conf delegation"

protocol domain-auth auto-conf delegation setup-user

Description

Automatically configures a precreated account with constrained delegation privileges in the Active Directory.

Syntax

protocol domain-auth auto-conf delegation setup-user adminuser <name > adminpass <password> domain <name> dc <dcname>

Parameters

adminuser <name>	Specify the user name of the domain administrator.
adminpass <password>	Specify the password of the domain administrator.
domain <name>	Specify the delegation domain in which you want to give the user delegation privileges, as in the following example: `DELEGATION.TEST`
dc <dcname>	Specify the name of the domain controller.

Usage

The **protocol domain-auth auto-conf delegation setup-user** command reads the configuration of the delegation user on the Steelhead appliance and configures the backend domain controller in Active Directory with the same settings.

This command adds privileges per the configuration on the Steelhead appliance. For example, if autodelegation is configured on the Steelhead appliance, the **protocol domain-auth auto-conf delegation setup-user** command attempts to configure autodelegation in Active Directory.

Example

```
amnesiac (config) # protocol domain-auth auto-conf delegation setup-user adminuser Administrator
adminpass password domain delegation.test dc delegation-dc1
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth auto-conf delegation"

protocol domain-auth auto-conf easy-auth

Description

Enables an automated domain authentication configuration process for the server-side Steelhead appliance.

Syntax

protocol domain-auth auto-conf easy-auth conf-type <conf-type> adminuser <name> adminpass < adminpass > join-domain <domain> dc <dc-name> [join-type {win2k8-mode | win2k3-mode}] [short-name <name>]

Parameters

conf-type <conf-type>	Specify a configuration type or a comma-separated list for the automated configuration: • **emapi** - Encrypted MAPI • **smbsigning** - SMB signing • **smb2signing** - SMB2 signing • **smb3signing** - SMB3 signing • **all** - Encrypted MAPI, SMB signing, SMB2 signing, and SMB3 signing
adminuser <name>	Specify the user name of the domain administrator.
adminpass <password>	Specify the password of the domain administrator. The password is case sensitive.
join-domain <name>	Specify the fully qualified domain name of the Active Directory domain in which to make the Steelhead appliance a member.
dc <dc-name> [join-type {win2k8-mode | win2k3-mode}]	Specify the name of the domain controller to contact. Optionally, specify the join account type by which the server-side Steelhead appliance can join the Windows domain in one of the following roles: • **win2k8-mode** - Active Directory integrated mode (Windows 2008 and later) • **win2k3-mode** - Active Directory integrated mode (Windows 2003). This is the default setting.
short-name <name>	Optionally, specify a short domain name. Typically, the short domain name is a substring of the realm. In rare situations, this is not the case, and you must explicitly specify the short domain name. Case matters; NBTTECH is not the same as nbttech. The short domain name is required if the NetBIOS domain name does not match the first portion of the Active Directory domain name.

Usage

The **protocol domain-auth auto-conf easy-auth** command simplifies the server-side Steelhead appliance configuration for domain authentication. By entering only one command, you can perform these steps:

- Test the DNS configuration.

- Join the server-side Steelhead appliance to the domain in AD integrated Windows 2008 (and later) mode or AD integrated Windows 2003 mode.
- Enable secure protocol optimization such as SMB signing.
- Optionally, configure a deployed replication user in Active Directory with the necessary privileges.

To integrate the server-side Steelhead appliance into Active Directory, you must configure the mode when you join the Steelhead appliance to the Windows domain. The **protocol domain-auth auto-conf easy-auth** command configures the server-side Steelhead appliance in Active Directory integrated mode for Windows 2003 or Windows 2008 to enable secure protocol optimization for CIFS SMB1, SMB2/3, and encrypted MAPI for all clients and servers.

When you configure the server-side Steelhead appliance in integrated Active Directory mode, the server-side Steelhead appliance does not provide any Windows domain controller functionality to any other machines in the domain and does not advertise itself as a domain controller or register any service records. In addition, the Steelhead appliance does not perform any replication nor hold any AD objects. When integrated with the Active Directory, the server-side Steelhead appliance has just enough privileges so that it can have a legitimate conversation with the domain controller and then use transparent mode for NTLM authentication.

Use the **show protocol domain-auth auto-conf easy-auth** command to verify if the domain authentication configuration is successful.

For details, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide - Protocols*.

Example

```
amnesiac (config) # protocol domain-auth auto-conf easy-auth conf-type all adminuser chiefadmin
adminpass chief327 join-domain central.company.com dc exchange-dc join-type win2k8-mode
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth auto-conf easy-auth"

protocol domain-auth auto-conf replication

Description

Automatically configures a precreated account in Active Directory with replication privileges over the entire domain.

Syntax

[no] protocol domain-auth auto-conf replication adminuser <name> adminpass <password> domain <domain> dc <dc-name>

Parameters

adminuser <name>	Specify the administrator user name.
adminpass <password>	Specify the domain administrator password.
domain <domain>	Specify the replication domain in which you want to give the user replication privileges, as in the following example: `REPLICATION.TEST`
dc <dc-name>	Specify a domain controller.

Usage

The **protocol domain-auth auto-conf replication** command reads the configuration of the replication user on the Steelhead appliance and configures the backend domain controller(s) in Active Directory with the same settings.

You must have domain administrator privileges to use this command.

Example

```
amnesiac (config) # protocol domain-auth replication adminuser Administrator adminpass password
domain replication.test dc replication-dc1
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth auto-conf replication"

protocol domain-auth test authentication

Description

Attempts to authenticate the user to the joined domain controller.

Syntax

protocol domain-auth test authentication username <username> password <password>

Parameters

username <username>	Specify the delegate username. The maximum length is 20 characters. The username cannot contain any of the following characters: / \ [ ] : ; | = , + * ? < > @ " **Note:** The system translates the user name into uppercase to match the registered server realm information.
password <password>	Specify a password.

Usage

The **protocol domain-auth test authentication** command tests whether transparent mode NTLM (used by SMB signing, SMB2/3 signing, and encrypted MAPI) is working as expected.

Example

```
amnesiac (config) # protocol domain-auth test authentication
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth test authentication"

protocol domain-auth test delegation server-privs

Description

Tests the delegation privileges for a server.

Syntax

protocol domain-auth test delegation server-privs domain <domain> server <server> server-ip <server-ip> service {cifs | exchangeMDB} [enduser <enduser>]

Parameters

domain <domain>	Specify the delegation domain in which you want to make the delegate user a trusted member, as in the following example: `SIGNING.TEST`
server <server>	Specify a delegate server hostname.
server-ip <server-ip>	Specify the delegate server IP address.
service {cifs | exchangeMDB}	Specify a service: • **cifs** - CIFS service • **exchangeMDB** - Exchange service
enduser <enduser>	Specify the end user name used on the client. The default end user is the delegate user.

Usage

Within SMB signing, SMB2/3 signing, and encrypted MAPI in delegation mode, the Steelhead appliance and the AD environment must have correct privileges to obtain Kerberos tickets for the CIFS or exchange server and perform the subsequent authentication.

The **protocol domain-auth test delegation server-privs** command tests whether correct privileges are set to perform constrained delegation.

Example

```
amnesiac (config) # protocol domain-auth test delegation server-privs domain delegation.test server
exchange01 server-ip 10.2.3.4 service exchangeMDB
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth test delegation server-privs"

protocol domain-auth test delegation setup

Description

Tests the delegation user authentication setup.

Syntax

protocol domain-auth test delegation setup domain <domain> dc <dc-name>

Parameters

domain <domain>	Specify the delegation domain in which you want to make the delegate user a trusted member, as in the following example: `SIGNING.TEST`
dc <dc-name>	Specify a domain controller.
auto <true | false>	Tests for autodelegation privileges.

Usage

Thes **protocol domain-auth test delegation setup** command checks whether an account has the necessary privileges for delegation and autodelegation.

Example

```
amnesiac (config) # protocol domain-auth test delegation setup domain delegation-test dc delegation-
dc1
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth test delegation setup"

protocol domain-auth test dns

Description

Tests Steelhead appliance DNS settings.

Syntax

protocol domain-auth test dns join-domain <domain>

Parameters

None

Parameters

join-domain <domain>	Specify the FQDN of the join domain: `JOIN.TEST`

Usage

The **protocol domain-auth test dns** command tests whether the DNS domain join configuration is correctly configured for Windows domain authentication, SMB signing, SMB2 signing, SMB3 signing, and encrypted MAPI optimizations.

Example

```
amnesiac (config) # protocol domain-auth test dns join-domain join.test
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth test dns"

protocol domain-auth test join

Description

Checks to determine whether the Steelhead appliance is joined to the domain.

Syntax

protocol domain-auth test join

Parameters

None

Usage

The **protocol domain-auth test join** command tests whether the domain join configuration of the Steelhead appliance is valid on the backend domain controller(s) in Active Directory.

Example

```
amnesiac (config) # protocol domain-auth test join
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth test join"

protocol domain-auth test replication prp

Description

Tests the password replication policy (PRP) of the domain.

Syntax

protocol domain-auth test replication prp domain <domain> dc <dcname> rserver <rserver>

Parameters

domain <domain>	Specify the replication domain: `REPLICATION.TEST`
dc <dcname>	Specify the name of the domain controller.
rserver <rserver>	Specify the server account to replicate.

Usage

The **protocol domain-auth test replication prp** command determines whether the server account can be replicated as specified by the PRP on the domain controller.

Example

```
amnesiac (config) # protocol domain-auth test replication prp domain replication.test dc
replication-dc1 rserver server1
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth test replication prp"

protocol domain-auth test replication try-repl

Description

Tests the ability to replicate the server account.

Syntax

protocol domain-auth test replication try-repl domain <domain> shortdom <shortdom> rserver <rserver>

Parameters

domain <domain>	Specify the replication domain in which you want to make the replication user a trusted member, as in the following example: `REPLICATION.TEST`
shortdom <shortdom>	Specify the short domain name.
rserver <rserver>	Specify the server account to replicate.

Usage

The **protocol domain-auth test replication try-repl** command attempts to replicate a server account using the replication user for the domain.

Example

```
amnesiac (config) # protocol domain-auth test replication try-repl domain replication.test shortdom
rep.test rserver server1
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth test replication try-repl"

CIFS, SMB, SMB2, and SMB3 Support Commands

This section describes the CIFS/SMB and SMB2/SMB3 support commands. For detailed information about SMB signing, including steps for configuring Windows, see the *Steelhead Appliance Management Console User's Guide* and "CIFS Prepopulation Support Commands".

ip fqdn override

Description

Sets the fully qualified domain name.

Syntax

[no] ip fqdn override <domain name>

Parameters

<domain name>	Specify a fully qualified domain name.

Usage

For SMB signing, specify the delegation domain in which you want to make the delegate user a trusted member; for example: **SIGNING.TEST**.

Example

```
amnesiac (config) # ip fqdn override SIGNING.TEST
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, CSH

Related Topics

"show domain"

protocol cifs applock enable

Description

Enables CIFS application lock mechanism. RiOS v5.5.x or higher optimizes Microsoft Office, Excel, and CIFS traffic with SMB signing enabled.

Syntax

[no] protocol cifs applock enable

Parameters

None

Usage

Enables CIFS latency optimizations to improve read and write performance for Microsoft Word and Excel documents when multiple users have the file open. By default, this setting is enabled in RiOS v6.0 and later.

This feature enhances the Enable Overlapping Open Optimization feature by identifying and obtaining locks on read write access at the application level. The overlapping open optimization feature handles locks at the file level.

Enable the **applock** optimization feature on the client-side Steelhead appliance. The client-side Steelhead appliance must be running RiOS v5.5 or later.

Example

```
amnesiac (config) # protocol cifs applock enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs applock"

protocol cifs clear-read-resp enable

Description

Clears read response CIFS data when poor performance occurs.

Syntax

[no] protocol cifs clear-read-resp enable

Parameters

None

Usage

Increases performance for deployments with high bandwidth, low-latency links.

Example

```
amnesiac (config) # protocol cifs clear-read-resp enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs"

protocol cifs disable write optimization

Description

Disables CIFS write optimization.

Syntax

[no] protocol cifs disable write optimization

Parameters

None

Usage

Disable write optimization only if you have applications that assume and require write-through in the network. If you disable write optimization, the Steelhead appliance still provides optimization for CIFS reads and for other protocols, but you might experience a slight decrease in overall optimization.

Most applications operate safely with write optimization because CIFS allows you to explicitly specify write-through on each write operation. However, if you have an application that does not support explicit write-through operations, you must disable it in the Steelhead appliance.

If you do not disable write-through, the Steelhead appliance acknowledges writes before they are fully committed to disk, to speed up the write operation. The Steelhead appliance does not acknowledge the file close until the file is safely written.

The **no** command option enables CIFS write optimization.

Example

```
amnesiac (config) # protocol cifs disable write optimization
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs"

protocol cifs dw-throttling enable

Description

Enables CIFS dynamic throttling mechanism.

Syntax

[no] protocol cifs dw-throttling enable

Parameters

None

Usage

Enables CIFS dynamic throttling mechanism which replaces the current static buffer scheme. If you enable CIFS dynamic throttling, it is activated only when there are sub-optimal conditions on the server-side causing a back-log of write messages; it does not have a negative effect under normal network conditions.

The **no** command option disables the dynamic throttling mechanism.

Example

```
amnesiac (config) # protocol cifs dw-throttling enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs"

protocol cifs enable

Description

Enables CIFS optimization. CIFS optimization is enabled by default.

Syntax

[no] protocol cifs enable

Parameters

None

Usage

RiOS v5.5x and later includes settings to optimize Microsoft Office and CIFS traffic with SMB signing enabled.

RiOS v6.0 and later supports CIFS latency optimization and SMB Signing settings for Mac OSX 10.5.x and later clients.

Mac OSX support includes two CLI commands. You can alter a response for Query Path Info request issued with info-level QUERY_FILE_ALL_INFO and also edit the list of names that are queried by Mac clients immediately following a tree connect request.

CIFS latency optimization does not require a separate license and is enabled by default.

Typically, you disable CIFS optimizations only to troubleshoot the system.

The **no** command option disables CIFS optimization for testing purposes. Typically, you disable latency optimization to troubleshoot problems with the system.

Important: Latency optimization must be enabled (or disabled) on both Steelhead appliances.

Example

```
amnesiac (config) # protocol cifs enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs"

protocol cifs ext-dir-cache enable

Description

Enables extended directory caching.

Syntax

[no] protocol cifs ext-dir-cache enable

Parameters

None

Usage

Extended directory caching enhances directory browsing over the WAN.

The **no** command option disables extended directory caching.

Example

```
amnesiac (config) # protocol cifs ext-dir-cache enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs ext-dir-cache," "protocol cifs enable"

protocol cifs mac oplock enable

Description

Enables enables opportunist lock (oplock) support for Mac clients.

Syntax

[no] protocol cifs mac oplock enable

Parameters

None

Usage

A lock requested by a client on a file that resides on a remote server. To prevent any compromise to data integrity, the Steelhead appliance only optimizes data where exclusive access is available (in other words, when locks are granted). When an oplock is not available, the Steelhead appliance does not perform application-level latency optimizations but still performs Scalable

Data Referencing and compression on the data as well as TCP optimizations. Therefore, even without the benefits of latency optimization, Steelhead appliances still increase WAN performance, but not as effectively as when application optimizations are available.

The **no** command option disables CIFS MAC oplock support.

Example

```
amnesiac (config) # protocol cifs mac oplock enable
```

Product

Steelhead appliance, CSH

Related Topics

"show prepop"

protocol cifs nosupport

Description

Sets a specified OS as unsupported for optimization.

Syntax

protocol cifs nosupport client | server {add | remove} <os name>

Parameters

client | server	Specify the location to disable OS support.
add | remove	Adds or removes a OS support from the specified location.
<os name>	Specify the OS type: **longhorn, vista, win2k3, winxp, win2k, win98. wnt4, wnt3, winunk. emc. mac, linux, novell, samba, snap, unix, bsd**

Example

```
amnesiac (config) # protocol cifs nosupport client add win2k
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs nosupport client," "show protocol cifs nosupport server"

protocol cifs oopen enable

Description

Enables CIFS overlapping opens.

Syntax

[no] protocol cifs oopen enable

Parameters

None

Usage

Enable overlapping opens to obtain better performance with applications that perform multiple opens on the same file (for example, CAD applications). By default, this setting is disabled.

With overlapping opens enabled the Steelhead appliance optimizes data where exclusive access is available (in other words, when opportunist locks are granted). When an opportunist lock (oplock) is not available, the Steelhead appliance does not perform application-level latency optimizations but still performs SDR and compression on the data as well as TCP optimizations. Therefore, even without the benefits of latency optimization,Steelhead appliances still increase WAN performance, but not as effectively as when application optimizations are available.

If a remote user opens a file that is optimized using the overlapping opens feature and a second user opens the same file, they might receive an error if the file fails to go through a v3.x.x or later Steelhead appliance or if it does not go through a Steelhead appliance (for example, certain applications that are sent over the LAN). If this occurs, you should disable overlapping opens for those applications.

You can configure an include list or exclude list of file types subject to overlapping opens optimization with the "protocol cifs oopen extension" on page 523.

The **no** command option disables CIFS overlapping opens.

Example

```
amnesiac (config) # protocol cifs oopen enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs oopen"

protocol cifs oopen extension

Description

Configures file extensions to include or exclude from overlapping open optimization.

Syntax

protocol cifs oopen extension {[add <ext> <cr> | setting-always <policy>] | [modify <ext> setting <policy> <cr>] | remove <ext> <cr>}

Parameters

add <ext> <cr>	Specify a list of file extensions to include in overlapping opens optimization.
setting-always <policy>	Specify the policy to force on the specified file extension: • **allow** - Allows overlapping opens to enable better performance. • **deny** - Denies overlapping opens on the specified file extension.
[modify <ext> setting <policy> <cr>]	Modifies the policy setting for the specified file extension: • **allow** - Allows overlapping opens to enable better performance. • **deny** - Denies overlapping opens on the specified file extension.
remove <ext> <cr>	Removes a file extension from the special case list (that is, do not optimize the specified file extension).

Usage

Enable overlapping opens to obtain better performance with applications that perform multiple opens on the same file. With overlapping opens enabled, the Steelhead appliance optimizes data to which exclusive access is available (in other words, when locks are granted). When an oplock is not available, the Steelhead appliance does not perform application-level latency optimization but still performs SDR and compression on the data, as well as TCP optimizations. If you do not enable this feature, the Steelhead appliance still increases WAN performance, but not as effectively.

Enabling this feature on applications that perform multiple opens on the same file to complete an operation (for example, CAD applications) results in a performance improvement.

You specify a list of extensions you want to optimize using overlapping opens. You can also use this command to specify a list of extensions you do not want to optimize using overlapping opens.

If a remote user opens a file which is optimized using the overlapping opens feature and a second user opens the same file, the second user might receive an error if the file fails to go through a v3.x Steelhead appliance or if it does not go through a Steelhead appliance at all (for example, certain applications that are sent over the LAN). If this occurs, you should disable overlapping opens for those applications.

Example

```
amnesiac (config) # protocol cifs oopen extension modify pdf setting allow
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs oopen"

protocol cifs oopen policy

Description

Changes the default CIFS overlapping open policy.

Syntax

[no] protocol cifs oopen policy allow | deny

Parameters

<allow | deny>	Specify the policy: **allow** or **deny**

Usage

The default policy is to deny overlapping open optimization.

Example

```
amnesiac (config) # protocol cifs oopen policy allow
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs oopen"

protocol cifs secure-sig-opt enable

Description

Enables Security Signature negotiations between Windows client and the server.

Syntax

[no] protocol cifs secure-sig-opt enable

Parameters

None

Usage

The Secure-CIFS feature automatically stops Windows SMB signing. SMB signing prevents the appliance from applying full optimization on CIFS connections and significantly reduces the performance gain from a Steelhead deployment. Because many enterprises already take additional security precautions (such as firewalls, internal-only reachable servers, and so on), SMB signing adds little additional security, at a significant performance cost (even without Steelhead appliances).

Before you enable Secure-CIFS, you must consider the following factors:

- If the client-side machine has **Required** signing, enabling Secure-CIFS prevents the client from connecting to the server.
- If the server-side machine has **Required** signing, the client and the server connect but you cannot perform full latency optimization with the Steelhead appliance. domain controllers default to **Required**.

If your deployment requires SMB signing, see the *Steelhead Appliance Management Console User's Guide* for detailed procedures, including procedures for Windows.

The **no** command option enables Security Signature negotiations.

Example

```
amnesiac (config) # protocol cifs secure-sig-opt enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs"

protocol cifs smb signing enable

Description

Enables SMB signing. By default, RiOS SMB signing is disabled.

Syntax

[no] protocol cifs smb signing enable

Parameters

None

Usage

When sharing files, Windows provides the ability to sign CIFS messages to prevent man-in-the-middle attacks. Each CIFS message has a unique signature which prevents the message from being tampered. This security feature is called SMB signing. Prior to the v5.5 release, RiOS did not provide latency optimization for signed traffic. For detailed information about configuring SMB signing, including the necessary steps for Windows, see the *Steelhead Appliance Management Console User's Guide*.

You can enable the RiOS SMB signing feature on a server-side Steelhead appliance to alleviate latency in file access with CIFS acceleration while maintaining message security signatures. With SMB signing on, the Steelhead appliance optimizes CIFS traffic by providing bandwidth optimizations (SDR and LZ), TCP optimizations, and CIFS latency optimizations—even when the CIFS messages are signed.

By default, RiOS SMB signing is disabled.

The RiOS SMB signing feature works with Windows 2003 and later domain security and is fully-compliant with the Microsoft SMB signing v1 protocol. The server-side Steelhead appliance in the path of the signed CIFS traffic becomes part of the Windows trust domain. The Windows domain is either the same as the domain of the user or has a trust relationship with the domain of the user. The trust relationship can be either a parent-child relationship or an unrelated trust relationship.

Important: This feature works with Windows 2003 native mode domains and later, when in delegation mode. In transparent mode the domain restrictions do not apply. SMB signing transparent mode is not currently supported in Windows 7.

RiOS v6.0 and later optimizes signed CIFS traffic even when the logged-in user or client machine and the target server belong to different domains, provided these domains have a trust relationship with the domain the Steelhead appliance has joined. RiOS v6.1 and later supports delegation for users that are in domains trusted by the server's domain.

The RiOS SMB-signing feature uses Kerberos between the server-side Steelhead appliance and any configured servers participating in the signed session. The client-side Steelhead appliance uses NTLM and will negotiate down to NTLM from Kerberos if supported. The client-side Steelhead appliance does not use Kerberos.

Prerequisites

- With RiOS SMB signing enabled, Steelhead appliances sign the traffic between the client and the client-side Steelhead appliance and between the server and the server-side Steelhead appliance. The traffic is not signed between the Steelhead appliances, but the Steelheads implement their own integrity mechanisms. For maximum security, Riverbed recommends that you use IPsec encryption to secure the traffic between the Steelhead appliances.
- RiOS SMB signing requires joining a Windows domain. Setting the correct time zone is vital for joining a domain. The most common reason for failing to join a domain is a significant difference in the system time on the Windows domain controller and the Steelhead appliance.

Basic Steps

1. Verify that the Windows domain functionality is at the Windows 2003 level or later. For detailed information about configuring SMB signing, including the necessary steps for Windows, see the *Steelhead Appliance Management Console User's Guide*.
2. Identify the full domain name, which must be the same as DNS. You need to specify this name when you join the server-side Steelhead appliance to the domain.
3. Identify the short (NetBIOS) domain name (press Ctrl+Alt+Del on any member server). You need to specify the short name when the Steelhead appliance joins the domain if it does not match the left-most portion of the fully-qualified domain name.
4. Make sure that the primary or auxiliary interface for the server-side Steelhead appliance is routed to the DNS and the domain controller.
5. Verify the DNS settings:

- You must be able to ping the server-side Steelhead appliance, by name, from a CIFS server joined to the same domain that the server-side Steelhead appliance will join. If you cannot, create an entry in the DNS server for the server-side Steelhead appliance.
- You must be able to ping the domain controller, by name, whose domain the server-side Steelhead appliance will join. To verify your domain run the "show domain," and "show dns settings".

6. Join the Windows domain running in native mode. In delegation mode, RiOS SMB-signing does not support Windows NT and Windows 2000. For detailed information about joining domains, see "domain rejoin" on page 505.
7. If you configured SMB signing in delegation mode, set up the domain controller and SPN. For detailed information, see the *Steelhead Appliance Management Console User's Guide*.
8. If you configured SMB signing in delegation mode, grant the user access to delegate CIFS service in Windows. You must perform the following procedure for every server on which you want to enable RiOS SMB signing. For detailed information, see the *Steelhead Appliance Management Console User's Guide*.
9. If you configured SMB signing in delegation mode, add delegate users on the Steelhead appliance.
10. Enable SMB signing on the server-side Steelhead appliances.

For detailed procedures, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # protocol cifs smb signing enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs smb signing status"

protocol cifs smb signing mode-type

Description

Configures SMB signing mode as either transparent or delegation.

Syntax

[no] protocol cifs smb signing mode-type <mode>

Parameters

<mode>	Specify one of the following modes: • **transparent** - Enables SMB signed packets with transparent authentication. Transparent mode uses the secure inner channel to authenticate and secure traffic, eliminating the need to define delegation trust. This is the default setting in RiOS v6.0 and later; however, if you enabled SMB signing in RiOS v5.5 and upgraded to v6.0 or later, delegation mode is enabled by default. The advantage transparent mode offers over the delegation mode is that it simplifies the amount of configuration required. Delegate users do not have to be configured for this mode. Transparent mode uses NTLM end-to-end between the client and server-side Steelhead appliance and the server-side Steelhead and the server. If you have Windows 7 clients, you will need to use delegation mode. • **delegation** - Enables SMB signed packets with delegate user authentication. Select this mode if you have previously enabled SMB signing with RiOS v5.5.x or higher. Use delegation mode if you want to optimize connections with Windows 7 clients. Using this mode requires setting up delegate users. Delegation mode uses NTLM between the client and server-side Steelhead appliance and Kerberos between the server-side Steelhead and the server. **Note:** If you switch between transparent and delegation modes you must restart the optimization service.

Example

```
amnesiac (config) # protocol cifs smb signing mode-type delegation
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"show protocol cifs smb signing status", "Windows Domain Authentication Delegation Commands"

protocol cifs smb signing native-krb enable

Description

Enables end-to-end Kerberos authentication support for SMB signing.

Syntax

[no] protocol cifs smb signing native-krb enable

Parameters

None

Usage

The **no** command option disables end-to-end Kerberos authentication support for SMB signing.

Example

```
amnesiac (config) # protocol cifs smb signing native-krb enable
```

Product

Steelhead appliance

Related Topics

"show protocol cifs smb signing status", "Windows Domain Authentication Delegation Commands"

protocol cifs smbv1-mode enable

Description

Enables SMBv1 backward compatibility mode, which allows a Steelhead appliance to perform CIFS latency optimization and SDR on SMB traffic in Windows Vista environments.

Syntax

[no] protocol cifs smbv1-mode enable

Parameters

None

Usage

Improves SMB optimization for Windows Vista users. Select to perform latency and SDR optimizations on SMB traffic on the client-side Steelhead appliance. Without this feature, Steelhead appliances perform only SDR optimization without improving CIFS latency. This feature enables SMBv1 for Vista-to-Vista CIFS connections instead of SMBv2 (similar to Vista to pre-Vista CIFS connections). While the Steelhead appliances are fully compatible with the SMBv2 included in Vista, they deliver the best performance using SMBv1.

Important: You must restart the client Steelhead service after enabling the SMBv1 Backward Compatibility Mode.

To enable SDR and CIFS latency optimization on SMB traffic in a Windows Vista environment, perform the following steps on the client-side Steelhead appliance:

1. Run the following command:

   ```
   # protocol cifs smbv1-mode enable
   ```

2. Restart the Steelhead service.

   ```
   # restart
   ```

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol cifs smbv1-mode enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs"

protocol cifs spoolss enable

Description

Enables CIFS print-spool subsystem optimization.

Syntax

[no] protocol cifs spoolss enable

Parameters

None

Usage

Improves centralized print traffic performance. For example, when the print server is located in the data center and the printer is located in the branch office, enabling this option speeds the transfer of a print job spooled across the WAN to the server and back again to the printer. By default, this setting is disabled.

Enabling this option requires an optimization service restart.

Windows XP and Vista are supported as clients, and Windows 2003 and Windows 2008 as servers.

Note: Both the client and server-side Steelhead appliance must be running RiOS v6.0 and later.

Example

```
amnesiac (config) # protocol cifs spoolss enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol cifs spoolss"

protocol smb2 signing native-krb enable

Description

Enables end-to-end Kerberos authentication support for SMB2 signing.

Syntax

[no] protocol smb2 signing native-krb enable

Parameters

None

Usage

The **no** command option disables end-to-end Kerberos authentication support for SMB2 signing.

Example

```
amnesiac (config) # protocol smb2 signing native-krb enable
```

Product

Steelhead appliance

Related Topics

"show protocol smb2"

protocol smb2 enable

Description

Enables optimization of SMB2 traffic for native SMB2 clients and servers. SMB2 allows for access across disparate networks. It is the default mode of communication between Windows Vista and Windows 7 clients and Windows Server 2008 and Windows Server 2008r2 servers.

Syntax

[no] protocol smb2 enable

Usage

You must restart the optimization service after running this command. For details on SMB2, see the *Steelhead Appliance Management Console User's Guide* and "protocol cifs smb signing enable" on page 525.

Example

```
amnesiac (config) # protocol smb2 enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol smb2"

protocol smb2 signing enable

Description

Enables the optimization of SMB2 signed traffic.

Syntax

[no] protocol smb2 signing enable

Usage

You must enable SMB2 and join a domain before enabling SMB2 signing. For details on SMB2, see the *Steelhead Appliance Management Console User's Guide* and "protocol cifs smb signing enable" on page 525.

When upgrading from RiOS v6.1 to v6.5 or later, you might already have a delegate user and be joined to a domain. If so, enabling SMB2 signing works when enabled with no additional configuration.

Example

```
amnesiac (config) # protocol smb2 enable
amnesiac (config) # protocol smb2 signing enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"protocol cifs smb signing enable", "protocol cifs smbv1-mode enable," "show protocol smb2"

protocol smb2 signing mode-type

Description

Configures the RiOS SMB2 signing mode. By default, RiOS SMB2 signing is disabled.

Syntax

[no] protocol smb2 signing mode-type <mode type>

Parameters

<mode type>	Specify one of the following modes: • **transparent** - Enables SMB signed packets with transparent authentication. Transparent mode uses the secure inner channel to authenticate and secure traffic, eliminating the need to define delegation trust. This is the default setting in RiOS v6.0 and later; however, if you enabled SMB signing in RiOS v5.5 and upgraded to v6.0 or later, delegation mode is enabled by default. The advantage transparent mode offers over the delegation mode is that it simplifies the amount of configuration required. Delegate users do not have to be configured for this mode. Transparent mode uses NTLM end-to-end between the client and server-side Steelhead appliance and the server-side Steelhead and the server. Note: If you have Windows 7 clients, you will need to use delegation mode. • **delegation** - Enables SMB signed packets with delegate user authentication. Select this mode if you have previously enabled SMB signing with RiOS v5.5.x or higher. Use delegation mode if you want to optimize connections with Windows 7 clients. Using this mode requires setting up delegate users. Delegation mode uses NTLM between the client and server-side Steelhead appliance and Kerberos between the server-side Steelhead and the server. **Note:** If you switch between transparent and delegation modes you must restart the optimization service.

Usage

You can enable the RiOS SMB2 signing feature on a server-side Steelhead appliance to alleviate latency in file access with CIFS acceleration while maintaining message security signatures.When sharing files, Windows provides the ability to sign CIFS messages to prevent man-in-the-middle attacks. Each CIFS message has a unique signature which prevents the message from being tampered with.

You must restart the optimization service after running this command. You must enable SMB2 before enabling SMB2 signing. For more information on SMB2, see the *Steelhead Appliance Management Console User's Guide*

Example

```
amnesiac (config) # protocol smb2 signing mode-type transparent
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"show protocol cifs smb signing status", "protocol domain-auth delegation auto-mode enable," "Windows Domain Authentication Delegation Commands"

protocol smb2 strip-8dot3

Description

Enables the removal of short names from the find data.

Syntax

[no] protocol smb2 strip-8dot3

Parameters

None

Usage

Use the **protocol smb2 strip-8dot3** command to remove the short names from the find data. You can also disable short names directly on the server, which eliminates the need for the Steelhead appliance to remove the short names from the find data.

You must enable SMB2 before using this command.

For details on SMB2, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # protocol smb2 enable
amnesiac (config) # protocol smb2 strip-8dot3
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol smb2"

---

protocol smb2 smb3-support enable

Description

Enables optimization of SMB3 traffic.

Syntax

[no] protocol smb2 smb3-support enable

Usage

RiOS v8.5 includes support for optimizing SMB3-signed traffic for native SMB3 clients and servers. You must enable SMB3 signing if the client or server use any of these settings:

- SMB2/SMB3 signing is set to required. SMB3 signing is enabled by default.
- SMB3 secure dialect negotiation (enabled by default on the Windows 8 client)
- SMB3 encryption

You must first enable SMB2 and then restart the optimization service after running this command. For details on SMB3, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # protocol smb2 enable
amnesiac (config) # protocol smb2 smb3-support enable
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"show protocol smb2"

CIFS Prepopulation Support Commands

This section describes the CIFS prepopulation support commands. See also the related section, "CIFS, SMB, SMB2, and SMB3 Support Commands".

prepop enable

Description

Enables CIFS prepopulation.

Syntax

[no] prepop enable

Parameters

None

Usage

The prepopulation operation effectively performs the first Steelhead appliance read of the data on the prepopulation share. Subsequently, the Steelhead appliance handles read and write requests as effectively as with a warm data transfer. With warm transfers, only new or modified data is sent, dramatically increasing the rate of data transfer over the WAN.

The **no** command option disables the prepopulation feature.

Example

```
amnesiac (config) # prepop enable
```

Product

Steelhead appliance, CSH

Related Topics

"show prepop"

prepop share cancel-event

Description

Cancels CIFS prepopulation synchronization and verification for a share.

Syntax

prepop share cancel-event {remote-path <remote-path>}

Parameters

remote-path <remote-path>	Cancels synchronization and verification processes for a remote share. Use the format `'\\server\share'`.

Usage

Use this command to cancel CIFS prepopulation and verification processes for a remote share.

Example

```
amnesiac (config) # prepop share cancel-event remote-path '\\10.11.61.66\backup'
```

Product

Steelhead appliance, CSH

Related Topics

"show prepop"

prepop share configure

Description

Configures CIFS prepopulation settings for a share.

Syntax

prepop share configure {remote-path <remote-path> server-account <login> server-password <password> interval <number of seconds>} [comment <"text comment"> start-time <date and time>]

Parameters

remote-path <remote-path>	Specify the remote path of the share to be synchronized. Use the format `'\\server\share'`.
server-account <login>	Specify the login, if any, required to access the share.
server-password <password>	Specify the corresponding password, if any, to access the share.
interval <number of seconds>	Specify the number of seconds for the synchronization interval.
comment <"text comment">	Type a string to describe the share, for administrative purposes.
start-time <date and time>	Specify a start time for synchronization. Use the format 'YYYY/MM/DD HH:MM:SS'.

Usage

Use this command to configure CIFS settings for a share.

Example

```
amnesiac (config) # prepop share configure remote-path '\\server\share' server-account mylogin
server-password XyyXX interval 68 comment "test" start-time '2011/09/09 00:00:00'
```

Product

Steelhead appliance, CSH

Related Topics

"show prepop"

prepop share dry-run

Description

Enables a dry run of a share synchronization.

Syntax

prepop share dry-run remote-path <remote-path>

Parameters

remote-path <remote-path>	Specify the remote path of the share. Use the format `'\\server\share'`.

Usage

The **prepop share dry-run** command allows an administrator to view details about share synchronization and the amount of data expected to be transferred. No actual data is transferred.

Example

```
amnesiac (config) # prepop share dry-run share-name '\\10.11.61.66\backup'
```

Product

Steelhead appliance

Related Topics

"show prepop log dry-run"

prepop share manual-sync

Description

Performs manual synchronization for a remote share.

Syntax

prepop share manual-sync remote-path <remote-path>

Parameters

remote-path <remote-path>	Specify the remote path of the share to be synchronized. Use the format: `'\\server\share'`.

Usage

Use this command to perform manual synchronization for a remote share.

Example

```
amnesiac (config) # prepop share manual-sync remote-path '\\10.11.61.66\backup'
```

Product

Steelhead appliance, CSH

Related Topics

"show prepop"

prepop share modify

Description

Modifies prepopulation settings for a share.

Syntax

prepop share modify {remote-path <remote-path> server-account <login> server-password <password> interval <number of seconds> comment <"text comment"> | start-time <date and time> | max-duration <seconds> | max-sync-size <bytes> | syncing <true | false>}

Parameters

remote-path <remote-path>	Specify the remote path of the share to be synchronized. Use the format `'\\server\share'`.
server-account <login>	Specify the login, if any, required to access the share.
server-password <password>	Specify the corresponding password, if any, to access the share.
interval <number of seconds>	Specify the interval, in seconds, for subsequent synchronizations.
comment <"text comment">	Type a string to describe the share, for administrative purposes.
start-time <date and time>	Specify a start time for synchronization in the format 'YYYY/MM/DD HH:MM:SS'.
max-duration <seconds>	Specify the maximum duration, in seconds, for the synchronization to occur.
max-sync-size <bytes>	Specify the maximum data size, in bytes, for data synchronized in a prepopulation operation. This is a data-size limit on the LAN side.
syncing <true | false>	Disable or enable synchronization of a share.

Usage

The **prepop share modify** command allows you to modify various setting for a share.

Example

```
amnesiac (config) # prepop share modify remote-path '\\10.11.61.66\backup' interval 68 start-time
'2011/09/09 00:00:00'
```

Product

Steelhead appliance, CSH

Related Topics

"show prepop"

no prepop share policy rule

Description

Removes a rule within a policy.

Syntax

no prepop share policy remote-path <remote-path> policy-name <policy-name> [rule <rule>]

Parameters

remote-path <remote-path>	Specify the remote path of the share. Use the format `'\\server\share'`.
policy-name <policy-name>	Specify the policy name.
<rule>	Specify the policy rule index.

Usage

Use the **show prepop share policy** command to obtain the value for the <rule> argument.

Example

```
amnesiac (config) # no prepop share policy remote-path '\\10.11.61.66\backup' policy-name
```

```
localpolicy rule 5
```

Product

Steelhead appliance

Related Topics

"show prepop"

prepop share policy

Description

Creates a policy with the specified name.

Syntax

[no] prepop share policy remote-path <remote-path> policy-name <policy-name>

Parameters

remote-path <remote-path>	Specify the remote path of the share. Use the format `'\\server\share'`.
policy-name <policy-name>	Specify the policy name.

Usage

The **no** command option removes the policy.

Example

```
amnesiac (config) # prepop share policy remote-path '\\10.11.61.66\backup' policy-name
centralregion
```

Product

Steelhead appliance

Related Topics

"show prepop share policy"

prepop share policy access-time

Description

Adds an access time synchronization rule to the policy.

Syntax

prepop share policy remote-path <remote-path> policy-name <policy-name> access-time {sync-relative <time> | time <time> compare-op {before | after}}

Parameters

remote-path <remote-path>	Specify the remote path of the share. Use the format `'\\server\share'`.
policy-name <policy-name>	Specify a policy name.
sync-relative <time>	Specify the time relative to synchronization, in the following format: 'HH:MM:SS'
time <time>	Specify the reference time in the following format: 'YYYY/MM/DD HH:MM:SS'
compare-op {before | after}	Specify the compare operator: • **before** - Before the specified time • **after** - After the specified time

Usage

The **prepop share policy access-time** command performs prepopulation synchronization based on the time that a file was accessed.

Example

```
amnesiac (config) # prepop share policy remote-path '\\10.11.61.66\backup' policy-name prepoppolicy
access-time sync-relative '03:05:11'
```

Product

Steelhead appliance

Related Topics

"show prepop share policy"

prepop share policy create-time

Description

Adds a create time synchronization rule to the policy.

Syntax

prepop share policy remote-path <remote-path> policy-name <policy-name> create-time {sync-relative <time> | time <time> compare-op {before | after}}

Parameters

remote-path <remote-path>	Specify the remote path of the share. Use the format `'\\server\share'`.
policy-name <policy-name>	Specify a policy name.
sync-relative <time>	Specify the time relative to synchronization, in the following format: 'HH:MM:SS'
time <time>	Specify reference time in the following format: 'YYYY/MM/DD HH:MM:SS'
compare-op {before | after}	Specify the compare operator: • **before** - Before the specified time • **after** - After the specified time

Usage

The **prepop share policy create-time** command performs prepopulation synchronization based on the time that a file was created.

Example

The following example shows a policy with a rule that synchronizes files created after August 1, 2012, but before August 5, 2012:

```
amnesiac (config) # prepop share policy share-name '\\10.11.61.66\example_prepop' policy-name
policy1 create-time time '2012/08/01 00:00:00' compare-op after

amnesiac (config) # prepop share policy share-name '\\10.11.61.66\example_prepop' policy-name
policy1 create-time time '2012/08/05 00:00:00' compare-op before
```

Product

Steelhead appliance

Related Topics

"show prepop share policy"

prepop share policy file-name

Description

Adds a file name rule to the policy.

Syntax

prepop share policy remote-path <remote-path> policy-name <policy-name> file-name <file-name> compare-op {matches | not-matches}

Parameters

remote-path <remote-path>	Specify the remote path of the share. Use the format `'\\server\share'`.
policy-name <policy-name>	Specify a policy name.
<file-name>	Specify a file name or a list of file names separated by semicolons. The file name can contain a wildcard character: for example, *001.doc; *pdf.
compare-op {matches | not-matches}	Specify the compare operator: • **matches** - Matches the file name. • **not-matches** - Does not match the file name.

Usage

The **prepop share policy file-name** command performs prepopulation synchronization based on files matching a regular expression.

Example

The following example shows a policy with a rule that synchronizes all files matching a*.doc and a*.pdf file names:

```
amnesiac (config) # prepop share policy share-name '\\10.11.61.66\backup' policy-name prepoppolicy
file-name 'a*.doc;a*.pdf' compare-op matches
```

Product

Steelhead appliance

Related Topics

"show prepop share policy"

prepop share policy file-size

Description

Adds a file size rule to the policy.

Syntax

prepop share policy remote-path <remote-path> policy-name <policy-name> file-size <file-size> compare-op {less |greater}

Parameters

remote-path <remote-path>	Specify the remote path of the share. Use the format `'\\server\share'`.
policy-name <policy-name>	Specify a policy name.
<file-size>	Specify a file size.
compare-op {less | greater}	Specify the compare operator: • **less** - Less than or equal to the file size • **greater** - Greater than or equal to the file size

Usage

The **prepop share policy file-size** command performs prepopulation synchronization based on file sizes.

Example

The following example shows a policy with a rule that synchronizes all files between 5 MB and 10 MB:

```
amnesiac (config) # prepop share policy remote-path '\\10.11.61.66\example_prepop' policy-name
```

```
policy2 file-size 10M compare-op less

amnesiac (config) # prepop share policy remote-path '\\10.11.61.66\example_prepop' policy-name
policy2 file-size 5M compare-op greater
```

Product

Steelhead appliance

Related Topics

"show prepop"

prepop share policy write-time

Description

Adds a write time synchronization rule to the policy.

Syntax

prepop share policy remote-path <remote-path> policy-name <policy-name> write-time {sync-relative <time> | time <time> compare-op {before | after}}

Parameters

remote-path <remote-path>	Specify the remote path of the share. Use the format: `'\\server\share'`.
policy-name <policy-name>	Specify a policy name.
sync-relative <time>	Specify the time relative to synchronization, in the following format: 'HH:MM:SS'
time <time>	Specify the reference time in the following format: 'YYYY/MM/DD HH:MM:SS'
compare-op {before | after}	Specify the compare operator: • **before** - Before the specified time • **after** - After the specified time

Usage

The **prepop share policy write-time** command performs prepopulation synchronization based on the time a file was modified.

Example

The following example shows a policy with a rule that synchronizes files modified in the last 48 hours:

```
amnesiac (config) # prepop share policy remote-path '\\10.11.61.66\example_prepop' policy-name
policy1 write-time sync-relative '48:00:00'
```

Product

Steelhead appliance

Related Topics

"show prepop share policy"

prepop share snapshot

Description

Enables or disables synchronization from the latest snapshot of the share needing prepopulation.

Syntax

prepop share snapshot remote-path <remote-path> status {<true | false>}

Parameters

remote-path <remote-path>	Specify the remote path of the share. Use the format `'\\server\share'`.
status <true | false>	Specify **true** to enable synchronization from the latest share snapshot. Specify **false** to disable synchronization from the latest share snapshot.

Usage

The **prepop share snapshot** command enables or disables synchronization from the latest snapshot of the share needing prepopulation when shadow copy is enabled on the CIFs server.

Example

```
amnesiac (config) # prepop share snapshot remote-path '\\10.11.61.66\example_snapshot' status true
```

Product

Steelhead appliance

Related Topics

"show prepop"

protocol cifs prepop enable

Description

Enables CIFS transparent prepopulation.

Syntax

[no] protocol cifs prepop enable

Parameters

None

Usage

The **no** command option disables CIFS transparent prepopulation.

Example

```
amnesiac (config) # protocol cifs prepop enable
```

Product

Steelhead appliance, CSH

Related Topics

"show prepop"

HTTP Support Commands

This section describes the HTTP support commands.

protocol http auto-config clear-stats

Description

Clears the hostname autoconfiguration statistics.

Syntax

protocol http auto-config clear-stats {all | hostname <hostname>}

Parameters

all	Clears statistics for all hostnames.
hostname <hostname>	Clears statistics for the specified hostname.

Usage

If you clear the statistics using the **protocol http auto-config clear-stats** command, the autoconfiguration process starts again.

Example

```
amnesiac (config) # protocol http auto-config clear-stats hostname localcompany.com
```

Product

Steelhead appliance

Related Topics

"show protocol http"

protocol http auto-config enable

Description

Configures an optimal HTTP automatic configuration scheme per host.

Syntax

[no] protocol http auto-config enable

Parameters

None

Usage

RiOS v7.0 introduces HTTP automatic configuration, which creates an optimal HTTP optimization scheme based on a collection of comprehensive HTTP traffic statistics gathered for a host.

Automatic configuration defines the optimal combination of all visible HTTP features.

By default, RiOS HTTP automatic configuration is enabled.

Example

```
amnesiac (config) # protocol http auto-config enable
```

Product

Steelhead appliance

Related Topics

"show protocol http"

protocol http auto-config selection

Description

Configures the per-host autoconfiguration selection settings.

Syntax

[no] protocol http auto-config selection {obj-pref-table | parse-prefetch |url-learning | reuse-auth|strip-auth-hdr | gratuitous-401| force-nego-ntlm| strip-compress |insert-cookie | insrt-keep-aliv|FPSE | WebDAV| FSSHTTP}

Parameters

obj-pref-table	Specify to enable the Object Prefetch Table, which stores HTTP object prefetches from HTTP GET requests for cascading style sheets, static images, and Java scripts in the Object Prefetch Table. When the browser performs If-Modified-Since (IMS) checks for stored content or sends regular HTTP requests, the client-side Steelhead appliance responds to these IMS checks and HTTP requests, reducing round trips across the WAN.
parse-prefetch	Specify to enable Parse and Prefetch, which parses the base HTML page received from the server and prefetches any embedded objects to the client-side Steelhead appliance. This option complements URL Learning by handling dynamically generated pages and URLs that include state information. When the browser requests an embedded object, the Steelhead appliance serves the request from the prefetched results, eliminating the round-trip delay to the server. The prefetched objects contained in the base HTML page can be images, style sheets, or any Java scripts associated with the base page and located on the same host as the base URL. Parse and Prefetch requires cookies. If the application does not use cookies, you can insert one using the **insert-cookie** option.
url-learning	Specify to enable URL Learning, which learns associations between a base URL request and a follow-on request. Stores information about which URLs have been requested and which URLs have generated a 200 OK response from the server. This option fetches the URLs embedded in style sheets or any JavaScript associated with the base page and located on the same host as the base URL. URL Learning works best with content that is not dynamic and does not contain session-specific information. URL Learning is enabled by default. Your system must support cookies and persistent connections to benefit from URL Learning. If your system has cookies turned off and depends on URL rewriting for HTTP state management, or is using HTTP v1.0 (with no keep-alives), you can force the use of cookies by using the Add Cookie option and force the use of persistent connections using the Insert Keep Alive option.
reuse-auth	Specify to allow an unauthenticated connection to serve prefetched objects, as long as the connection belongs to a session whose base connection is already authenticated. This option is most effective when the Web server is configured to use per-connection NTLM or Kerberos authentication.
strip-auth-hdr	Specify to remove all credentials from the request on an already authenticated connection. This works around Internet Explorer behavior that reauthorizes connections that have been previously authorized. This option is most effective when the Web server is configured to use per-connection NTLM authentication. **Important:** If the Web server is configured to use per-request NTLM authentication, enabling this option might cause authentication failure.
gratuitous-401	Specify to prevent a WAN round trip by issuing the first 401 containing the realm choices from the client-side Steelhead appliance. Riverbed recommends enabling **strip-auth-hdr** along with this option. This option is most effective when the Web server is configured to use per-connection NTLM authentication or per-request Kerberos authentication. **Important:** If the Web server is configured to use per-connection Kerberos authentication, enabling this option might cause additional delay.

force-nego-ntlm	In the case of negotiated Kerberos and NTLM authentication, specify to force NTLM. Kerberos is less efficient over the WAN because the client must contact the domain controller to answer the server authentication challenge and tends to be employed on a per-request basis. Riverbed recommends enabling **strip-auth-hdr** with this option. This setting is disabled by default.
strip-compress	Specify **yes** to enable this feature; specify **no** to disable it. Removes the accept-encoding lines from the HTTP compression header. An accept-encoding directive compresses content rather than using raw HTML. Enabling this option improves the performance of the Steelhead appliance data-reduction algorithms. This setting is enabled by default.
insert-cookie	Specify to add a cookie to HTTP applications that do not already have one. HTTP applications frequently use cookies to monitor sessions. The Steelhead appliance uses cookies to distinguish one user session from another. If an HTTP application does not use cookies, the client Steelhead appliance inserts one so that it can track requests from the same client. By default, this setting is disabled.
insrt-keep-aliv	Specify to use the same TCP connection to send and receive multiple HTTP requests and responses, as opposed to opening new ones for every single request and response. Enable this option when using the URL Learning or Parse and Prefetch features with HTTP v1.0 or HTTP v1.1 applications using the Connection Close method. This setting is disabled by default.
FPSE	Specify to enable or disable Sharepoint Front Page Server Extensions Protocol (FPSE) on a subnet or hostname. RiOS v8.5 caches and responds locally to all FPSE requests to save at least five round trips per request, resulting in performance improvements. SSL connections and files smaller than 5 MB can experience significant performance improvements. This setting is disabled by default.
WebDAV	Specify to enable or disable Sharepoint Web-based Distributed Authoring and Versioning (WebDAV) on a subnet or hostname. WebDAV is an open-standard extension to the HTTP 1.1 protocol that enables file management on remote Web servers. WebDAV is used by the WebDAV redirector, Web Folders, SMS/SCCM, and many other Microsoft components. SharePoint clients typically issue a Depth 0 request, then subsequently issue a Depth 1 request. RiOS fetches the Depth 1 response in place of the Depth 0 response and then serves subsequent Depth 1 and Depth 0 requests on collection/internal members locally. Serving requests locally saves multiple round trips and makes browsing the SharePoint file repository more responsive. This setting is disabled by default.
FSSHTTP	Specify to enable or disable Sharepoint File Synchronization via SOAP over HTTP (FSSHTTP) on a subnet or hostname. This setting is disabled by default.

Usage

Use the **no** version of the command to ignore the specified option in the selection.

Example

```
amnesiac (config) # protocol http auto-config WebDAV
```

Product

Steelhead appliance

Related Topics

"show protocol http auto-config selection"

protocol http enable

Description

Enables HTTP acceleration, which prefetches and caches objects embedded in Web pages to improve HTTP traffic performance. Enabling HTTP module support optimizes traffic to or from port 80. HTTP optimization works for most HTTP and HTTPS applications, including SAP, Customer Relationship Management, Enterprise Resource Planning, Financials, Document Management, and Intranet portals.

Syntax

[no] protocol http enable

Parameters

None

Usage

A typical Web page is not a single file that is downloaded all at once. Instead, Web pages are composed of dozens of separate objects—including .jpg and .gif images, JavaScript code, and cascading style sheets—each of which must be requested and retrieved separately, one after the other. Given the presence of latency, this behavior is highly detrimental to the performance of Web-based applications over the WAN. The higher the latency, the longer it takes to fetch each individual object and, ultimately, to display the entire page.

- **URL Learning** - The Steelhead appliance learns associations between a base request and a follow-on request. This feature is most effective for Web applications with large amounts of static content: for example, images, style sheets, and so on. Instead of saving each object transaction, the Steelhead appliance saves only the request URL of object transactions in a Knowledge Base and then generates related transactions from the list. This feature uses the Referer header field to generate relationships between object requests and the base HTML page that referenced them and to group embedded objects. This information is stored in an internal HTTP database. The following objects are retrieved by default: .gif, .jpg, .css, .js, .png. You can add additional object types to be retrieved.

- **Parse and Prefetch** - The Steelhead appliance includes a specialized algorithm that determines which objects are going to be requested for a given Web page and prefetches them so that they are readily available when the client makes its requests. This feature complements the URL Learning feature by handling dynamically generated pages and URLs that include state information. Parse and Prefetch essentially reads a page, finds HTML tags that it recognizes as containing a prefetchable object, and sends out prefetch requests for those objects. Typically, a client would need to request the base page, parse it, and then send out requests for each of these objects. This still occurs, but with Parse and Prefetch the Steelhead appliance has quietly perused the page before the client receives it and has already sent out the requests. This allows it to serve the objects as soon as the client requests them, rather than forcing the client to wait on a slow WAN link. For example, when an HTML page contains the tag **<img src=my_picture.gif>**, the Steelhead appliance prefetches the image **my_picture.gif** because it parses an **img** tag with an attribute of **src** by default. The HTML tags that are prefetched by default are **base/href**, **body/background**, **img/src**, **link/href**, and **script/src**. You can add additional object types to be prefetched.

- **Removal of Unfetchable Objects** - The Steelhead appliance removes unfetchable objects from the URL Learning Knowledge Base.

- **Object Prefetch Table** - The Steelhead appliance stores object prefetches from HTTP GET requests for cascading style sheets, static images, and Java scripts. This helps the client-side Steelhead appliance respond to If-Modified-Since (IMS) requests and regular requests from the client, thus cutting back on round trips across the WAN. This feature is useful for applications that use a lot of cacheable content.

- **Persistent Connections** - The Steelhead appliance uses an existing TCP connection between a client and a server to prefetch objects from the Web server that it determines are about to be requested by the client. Many Web browsers open multiple TCP connections to the Web server when requesting embedded objects. Typically, each of these TCP connections go through a lengthy authentication dialog before the browser can request and receive objects from the Web server on that connection. NTLM is a Microsoft authentication protocol which employs a challenge-response mechanism for authentication, in which clients are required to prove their identities without sending a password to a server. NTLM requires the transmission of three messages between the client (wanting to authenticate) and the server (requesting authentication).

For detailed information, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

The **no** command option disables HTTP module support.

Example

```
amnesiac (config) # protocol http enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol http"

protocol http metadata-resp extension

Description

Specify the object extensions to add. By default, the Steelhead appliance prefetches .css, .gif, .jpg, .js, and .png.

Syntax

[no] protocol http metadata-resp extension <extension>

Parameters

<extension>	Specify the type of extension.

Usage

Use only when the browser or application performs IMS checks and recognizes the control headers.

The **no** command option removes the specified extension type.

Example

```
amnesiac (config) # no protocol http metadata-resp extension css
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol http"

protocol http metadata-resp max-time

Description

Sets the maximum number of seconds that HTTP optimization stores the object information.

Syntax

[no] protocol http metadata-resp max-time <seconds>

Parameters

<seconds>	Specify the maximum time to store the objects. The default value is 86,400 seconds.

Usage

This setting specifies the maximum lifetime of the stored object. During this lifetime, any qualified If-Modified-Since (IMS) request from the client receives an HTTP 304 response, indicating that the resource for the requested object has not changed since it was stored.

The **no** command option resets the value.

Example

```
amnesiac (config) # protocol http metadata-resp max-time 60000
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol http"

protocol http metadata-resp min-time

Description

Sets the minimum number of seconds that HTTP optimization stores the object information.

Syntax

[no] protocol http metadata-resp min-time <number of seconds>

Parameters

<number of seconds>	Specify the number of seconds for the cache to store objects. The default value is 60 seconds.

Usage

This setting specifies the minimum lifetime of the stored object. During this lifetime, any qualified If-Modified-Since (IMS) request from the client receives an HTTP 304 response, indicating that the resource for the requested object has not changed since it was stored.

The **no** command option resets the cache minimum time.

Example

```
amnesiac (config) # protocol http metadata-resp min-time 10
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol http"

protocol http metadata-resp mode

Description

Configures the object caching mode for the HTTP optimization cache.

Syntax

[no] protocol http metadata-resp mode {all | use-list | none}

Parameters

all	Cache all allowable objects.
use-list	Cache objects matching the extension list.
none	Do not cache any object.

Usage

The **no** command option resets the HTTP optimization caching mode to the default mode.

Example

```
amnesiac (config) # protocol http metadata-resp mode all
```

Product

Steelhead appliance

Related Topics

"show protocol http"

protocol http native-krb enable

Description

Enables end-to-end Kerberos authentication support for HTTP.

Syntax

[no] protocol http native-krb enable

Parameters

None

Usage

The **no** command option disables end-to-end Kerberos authentication support for HTTP.

Example

```
amnesiac (config) # protocol http native-krb enable
```

Product

Steelhead appliance

Related Topics

"show protocol http"

protocol http prefetch

Description

Specify file extensions or the tag you want to prefetch for HTTP optimization.

Syntax

[no] protocol http prefetch {extension <ext> | tag <tag> attribute <tag attribute>}

Parameters

extension <ext>	Specify a file extension to add to the list of file types to prefetch.
tag <tag> attribute <attribute>	Specify the tag and the attributes to add or modify.

Usage

Use this command if your application uses custom tags for an object.

By default, the Steelhead appliance prefetches .jpg, .gif, .js, .png, and .css object extensions.

The **no** command option removes the extension.

Example

```
amnesiac (config) # no protocol http prefetch extension css
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol http"

protocol http prepop list

Description

Adds or deletes an HTTP prepopulation list.

Syntax

[no] protocol http prepop list <list-name>

Parameters

<list-name>	Specify the list name.

Usage

To configure HTTP prepopulation, you create a list composed of URLs that contain the data that you want optimized.

You can specify up to 100 lists and an unlimited number of URLs within each list. These lists can be prepopulated simultaneously.

For example, you can combine URL links to multiple Human Resource training videos in one list called HRlist.

The **no** command option deletes the specified list.

Example

```
amnesiac (config) # protocol http prepop list HRlist
```

Product

Steelhead appliance

Related Topics

"show protocol http prepop list," "show protocol http prepop status"

protocol http prepop list url

Description

Adds or deletes a URL from the HTTP prepopulation list.

Syntax

[no] protocol http prepop list <list-name> url <url>

Parameters

<list-name>	Specify the list name.
<url>	Specify the URL. URLs to HTML files, Apple video manifest, Adobe manifest, and Silverlight manifest files are accepted.

Usage

HTTP prepopulation is an enhanced HTTP-based data delivery method. HTTP prepopulation delivers data to the remote site by using the HTTP protocol to prewarm the RiOS data store. For example, you can prepopulate video at branch office locations during off-peak periods and then retrieve them for later viewing.

HTTP prepopulation supports Silverlight video, Silverlight streaming, Apple HLS, and Adobe flash video formats. Silverlight manifest files are files that video players parse to determine the different video (and audio) qualities that the server is advertising. Contact the network administrator to obtain the URL to the manifest file.

The **no** command option deletes the URL from the list.

The **protocol http prepop list silverlight-url** command is deprecated in RiOS v8.5 and is replaced by the **protocol http prepop list url** command.

You can view the prepopulation status using the **show protocol http prepop status** command. For more information on HTTP prepopulation, see the *Steelhead Appliance Deployment Guide - Protocols*.

Example

The following example points to a video file on a company intranet:

```
amnesiac (config) # protocol http prepop list trainingvideos url http://intranet/video.mov
```

The following example points to an HTML page with embedded videos:

```
amnesiac (config) # protocol http prepop list my-prepop-list url http://gen-vcs4/iisstart.htm
```

The following example points to a manifest file:

```
amnesiac (config) # protocol http prepop list my-prepop-list url http://gen-vcs4/ExampleManifest/
examplexyz.ism/manifest
```

Product

Steelhead appliance

Related Topics

"show protocol http prepop list," "show protocol http prepop status"

protocol http prepop list start

Description

Starts a prepopulation operation on the URLs in the specified list.

Syntax

protocol http prepop list <list-name> start

Parameters

<list-name>	Specify list name.

Usage

You can delete a list at any time. However, if the prepopulation operation on the list has started, the operation completes and the URLs are prepopulated. You can cancel the prepopulation operation on the list by specifying the **protocol http prepop list cancel** command.

Example

```
amnesiac (config) # protocol http prepop list site3 start
```

Product

Steelhead appliance

Related Topics

"protocol http prepop list cancel," "show protocol http prepop list," "show protocol http prepop status"

protocol http prepop list cancel

Description

Cancels a prepopulation operation on the specified list.

Syntax

protocol http prepop list <list-name> cancel

Parameters

<list-name>	Specify the list name.

Usage

The **protocol http prepop list cancel** command cancels a prepopulation operation that is currently running. When a prepopulation operation on a list has started, you cannot delete the list until the prepopulation operation completes or is cancelled.

You can start the prepopulation operation on the list again by specifying the **protocol http prepop list start** command.

Example

```
amnesiac (config) # protocol http prepop list site3 cancel
```

Product

Steelhead appliance

Related Topics

"protocol http prepop list start," "show protocol http prepop list," "show protocol http prepop status"

protocol http stream-split live enable

Description

Enables stream-splitting optimization for live streaming video.

Syntax

[no] protocol http stream-split live enable

Parameters

None

Usage

The **protocol http stream-split live enable** command enables the client-side Steelhead appliance to split Silverlight smooth streaming video, Adobe Flash HTTP dynamic streaming streams, and Apple HTTP Live Streaming (HLS) video.

This feature includes support for Microsoft Silverlight video and Silverlight extensions support on Information Internet Server (IIS) version 7.5 installed on Windows Server 2008 R2.

To split Adobe Flash streams, you must set up the video origin server before enabling this feature for Flash. For details, see the *Steelhead Appliance Deployment Guide - Protocols.*

Apple HLS is an HTTP-based video delivery protocol for iOS and OSX that streams video to iPads, iPhones, and Macs. HLS is part of an upgrade to QuickTime. RiOS splits both live and on-demand video streams.

RiOS uses stream-splitting technology to enable many users to watch a live video presentation, while transferring it over the WAN only once, enabling video scalability and freeing network bandwidth. Without stream-splitting, all requests for the same content traverse the network (or go across the WAN or to the server). For widely viewed live presentations, the same video clip might be transported over the network thousands of times.

When you enable HTTP stream splitting on the client-side Steelhead, it identifies live streaming video URL fragment requests and holds any request for a video fragment that has already been requested until the response is available, at which time it delivers that response to all clients that have requested it. The Steelhead appliance delivers only one request and response pair for a video fragment transfer over the WAN.

The **no** command option disables support for video stream-splitting optimization video.

Example

```
amnesiac (config) # protocol http stream-split live enable
```

Product

Steelhead appliance

Related Topics

"show protocol http stream-split"

protocol http prepop verify-svr-cert enable

Description

Enables server certificate verification during a prepopulation operation.

Syntax

[no] protocol http prepop verify-svr-cert enable

Parameters

None

Usage

The **no** command option disables the server certificate verification settings. The secure vault must be unlocked to allow the server certification verification. The CA certificates are saved in the secure vault.

Example

```
amnesiac (config) # protocol http prepop verify-svr-cert enable
```

Product

Steelhead appliance

Related Topics

"show protocol http prepop verify-svr-cert"

protocol http servers flush

Description

Flushes all HTTP server entries.

Syntax

[no] protocol http servers flush

Parameters

None

Usage

The **no** command option removes all server entries.

Example

```
amnesiac (config) # protocol http servers flush
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show protocol http"

protocol http server-table

Description

Specify the server table settings on which to accelerate HTTP traffic.

Syntax

[no] protocol http server-table {default | subnet {<IPv4 network> | IPv6 network |all-ipv4 | all-ipv6} | hostname {<name> | all} [obj-pref-table <yes | no>] [parse-prefetch <yes | no>] [url-learning <yes | no>] [reuse-auth <yes | no>] [strip-auth-hdr <yes | no>] [gratuitous-401 <yes | no>] [force-nego-ntlm <yes | no>] [strip-compress <yes | no>] [insert-cookie <yes | no>] [insrt-keep-aliv <yes | no>] [fpse <yes | no>] [webdav <yes | no>] [fsshttp <yes | no>]

Parameters

default	Changes the default value of the server table. This option is used for all traffic if no specific match is found.
subnet <network>	Specify one of the following for the HTTP server subnet: • **<IPv4 network>** - Specify an IPv4 network. Use the format X.X.X.X/<0-32>. • **<IPv6 network> -** Specify an IPv6 network. Use the format X:X:X: :X/<0-128>. • **all-ipv4 -** Specify an all IPv4 network. • **all-ipv6 -** Specify an all IPv6 network.
hostname {<name> | all}	Specify the hostname or all hostnames.
obj-pref-table <yes | no>	Specify to enable the Object Prefetch Table, which stores HTTP object prefetches from HTTP GET requests for cascading style sheets, static images, and Java scripts in the Object Prefetch Table. When the browser performs If-Modified-Since (IMS) checks for stored content or sends regular HTTP requests, the client-side Steelhead appliance responds to these IMS checks and HTTP requests, reducing round trips across the WAN.
parse-prefetch <yes | no>	Specify to enable Parse and Prefetch, which parses the base HTML page received from the server and prefetches any embedded objects to the client-side Steelhead appliance. This option complements URL Learning by handling dynamically generated pages and URLs that include state information. When the browser requests an embedded object, the Steelhead appliance serves the request from the prefetched results, eliminating the round-trip delay to the server. The prefetched objects contained in the base HTML page can be images, style sheets, or any Java scripts associated with the base page and located on the same host as the base URL. Parse and Prefetch requires cookies. If the application does not use cookies, you can insert one using the **insert-cookie** option.
url-learning <yes | no>	Specify to enable URL Learning, which learns associations between a base URL request and a follow-on request. Stores information about which URLs have been requested and which URLs have generated a 200 OK response from the server. This option fetches the URLs embedded in style sheets or any JavaScript associated with the base page and located on the same host as the base URL. URL Learning works best with content that is not dynamic and does not contain session-specific information. URL Learning is enabled by default. Your system must support cookies and persistent connections to benefit from URL Learning. If your system has cookies turned off and depends on URL rewriting for HTTP state management, or is using HTTP v1.0 (with no keep-alives), you can force the use of cookies by using the Add Cookie option and force the use of persistent connections using the Insert Keep Alive option.
reuse-auth <yes | no>	Specify to allow an unauthenticated connection to serve prefetched objects, as long as the connection belongs to a session whose base connection is already authenticated. This option is most effective when the Web server is configured to use per-connection NTLM or Kerberos authentication.
strip-auth-hdr <yes | no>	Specify to remove all credentials from the request on an already authenticated connection. This works around Internet Explorer behavior that re-authorizes connections that have been previously authorized. This option is most effective when the Web server is configured to use per-connection NTLM authentication. **Important:** If the Web server is configured to use per-request NTLM authentication, enabling this option might cause authentication failure.

gratuitous-401 <yes | no>	Specify to prevent a WAN round trip by issuing the first 401 containing the realm choices from the client-side Steelhead appliance. Riverbed recommends enabling **strip-auth-hdr** along with this option. This option is most effective when the Web server is configured to use per-connection NTLM authentication or per-request Kerberos authentication. **Important:** If the Web server is configured to use per-connection Kerberos authentication, enabling this option might cause additional delay.
force-nego-ntlm <yes | no>	In the case of negotiated Kerberos and NTLM authentication, specify to force NTLM. Kerberos is less efficient over the WAN because the client must contact the domain controller to answer the server authentication challenge and tends to be employed on a per-request basis. Riverbed recommends enabling **strip-auth-hdr** with this option. This setting is disabled by default.
strip-compress <yes | no>	Specify **yes** to enable this feature; specify **no** to disable it. Removes the accept-encoding lines from the HTTP compression header. An accept-encoding directive compresses content rather than using raw HTML. Enabling this option improves the performance of the Steelhead appliance data-reduction algorithms. This setting is enabled by default.
insert-cookie <yes | no>	Specify to add a cookie to HTTP applications that do not already have one. HTTP applications frequently use cookies to monitor sessions. The Steelhead appliance uses cookies to distinguish one user session from another. If an HTTP application does not use cookies, the client Steelhead appliance inserts one so that it can track requests from the same client. By default, this setting is disabled. This setting is disabled by default.
insrt-keep-aliv <yes | no>	Specify to use the same TCP connection to send and receive multiple HTTP requests and responses, as opposed to opening new ones for every single request and response. Enable this option when using the URL Learning or Parse and Prefetch features with HTTP v1.0 or HTTP v1.1 applications using the Connection Close method. This setting is disabled by default.
fpse <yes | no>	Specify to enable or disable Sharepoint Front Page Server Extensions Protocol (FPSE) on a subnet or hostname. RiOS v8.5 caches and responds locally to all FPSE requests to save at least 5 round trips per each request, resulting in performance improvements. SSL connections and files smaller than 5 MB can experience significant performance improvements. This setting is disabled by default.
webdav <yes | no>	Specify to enable or disable Sharepoint Web-based Distributed Authoring and Versioning (WebDAV) on a subnet or hostname. WebDAV is an open-standard extension to the HTTP 1.1 protocol that enables file management on remote Web servers. WebDAV is used by the WebDAV redirector, Web Folders, SMS/SCCM, and many other Microsoft components. SharePoint clients typically issue a Depth 0 request, then subsequently issue a Depth 1 request. RiOS fetches the Depth 1 response in place of the Depth 0 response and then serves subsequent Depth 1 and Depth 0 requests on collection/internal members locally. Serving requests locally saves multiple round trips and makes browsing the SharePoint file repository more responsive. This setting is disabled by default.
fsshttp <yes | no>	Specify to enable or disable Sharepoint File Synchronization via SOAP over HTTP (FSSHTTP) on a subnet or hostname. This setting is disabled by default.

Usage

This command applies HTTP optimization settings to a subnet or server hostname. This functionality eliminates the need to add servers one at a time.

The **no** command option removes the server subnet or server hostname from the list to optimize.

Example

```
amnesiac (config) # protocol http server-table subnet 10.10.10.10/24 insert-cookie yes
amnesiac (config) # protocol http server-table subnet 10.10.10.10/24 url-learning no
amnesiac (config) # protocol http server-table default webdav yes
```

Product

Steelhead appliance

Related Topics

"show protocol http," "show protocol http server-table"

protocol http space-in-uri enable

Description

Enables HTTP to parse the space in the URI.

Syntax

[no] protocol http space-in-uri enable

Parameters

None

Usage

The **no** version of the command disallows HTTP to parse the space in the URI.

Example

```
amnesiac (config) # protocol http space-in-uri enable
```

Product

Steelhead appliance

Related Topics

"show protocol http"

Oracle Forms Support Commands

This section describes the Oracle Forms support commands.

protocol oracle-forms enable

Description

Enables Oracle Forms optimization in native mode, also known as socket mode. Oracle Forms is browser plug-in that accesses Oracle Forms and Oracle E-Business application suite content from within the browser.

Syntax

[no] protocol oracle-forms enable

Parameters

None

Usage

Oracle Forms native mode optimization is enabled by default. Disable Oracle Forms only if your network users do not use Oracle applications.

Before enabling Oracle Forms optimization, you need to know the mode in which Oracle Forms is running at your organization. For detailed information, see the *Steelhead Appliance Management Console User's Guide*.

The Steelhead appliance decrypts, optimizes, and then re-encrypts Oracle Forms native, HTTP, and HTTPS mode traffic.

If you want to optimize HTTP mode traffic, you must also enable HTTP mode. For details, see "protocol oracle-forms http-enable"

Use Oracle Forms optimization to improve Oracle Forms traffic performance. RiOS v5.5.x or higher and later supports 6i, which comes with Oracle Applications 11i. RiOS v6.0 and later supports 10gR2, which comes with Oracle E-Business Suite R12.

Optionally, you can enable IPsec encryption to protect Oracle Forms traffic between two Steelhead appliances over the WAN.

To optimize Oracle Forms traffic

1. Make sure Oracle Forms optimization is enabled.
2. Create an in-path rule (fixed-target or auto-discovery) that specifies:
   - destination port: **9000** (native mode, using the default forms server)
   - preoptimization policy: **oracle-forms** or **oracle-forms+ssl**
   - optimization policy: **normal**
   - latency optimization policy: **normal**
   - Neural framing: **always**

The Oracle Forms optimization also supports Oracle Forms over SSL. To configure Oracle Forms over SSL specify the preoptimization policy in the in-path rules as **oracle-forms+ssl**.

The **no** command option disables Oracle Forms optimization.

Example

```
amnesiac (config) # protocol oracle-forms enable
amnesiac (config) # in-path rule auto-discover dstaddr 10.11.41.14/32 dstport 9000 preoptimization
oracle-forms latency-opt normal neural-mode always rulenum 1
```

Product

Steelhead appliance, CSH

Related Topics

"protocol oracle-forms http-enable," "show protocol oracle-forms"

protocol oracle-forms http-enable

Description

Enables Oracle Forms HTTP mode optimization. Oracle Forms is a browser plug-in that accesses Oracle forms and Oracle E-Business application suite content from within the browser.

Syntax

[no] protocol oracle-forms http-enable

Parameters

None

Usage

Before enabling Oracle Forms optimization, you need to know the mode in which Oracle Forms is running at your organization. For detailed information, see the *Steelhead Appliance Management Console User's Guide*.

Use this command to have the forms server listen for HTTP connections in addition to native mode optimization. All internal messaging between the forms server and the Java client is encapsulated in HTTP packets. Native mode Oracle Forms optimization must be enabled as well.

To optimize Oracle Forms HTTP traffic

1. Make sure Oracle Forms HTTP optimization is enabled.
2. Create an in-path rule (fixed-target or auto-discovery) that specifies:
   - destination subnet and port: **8000** (HTTP mode)
   - preoptimization policy: **oracle-forms** or **oracle-forms+ssl**
   - optimization policy: **normal**
   - latency optimization policy: **normal**
   - Neural framing: **always**

The Oracle Forms optimization also supports Oracle Forms over SSL. To configure Oracle Forms over SSL specify the preoptimization policy in the in-path rules as **oracle-forms+ssl**.

The **no** command option disables Oracle Forms HTTP optimization.

Example

```
amnesiac (config) # protocol oracle-forms http-enable
amnesiac (config) # in-path rule auto-discover dstaddr 10.11.41.14/32 dstport 8000 preoptimization
oracle-forms latency-opt normal neural-mode always rulenum 1
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol oracle-forms"

MAPI Support Commands

This section describes the MAPI support commands.

protocol mapi 2k3 enable

Description

Enables Exchange MAPI 2003 acceleration, which allows increased optimization of traffic between Exchange 2003 and Outlook 2003.

Syntax

[no] protocol mapi 2k3 enable

Parameters

None

Usage

MAPI optimization is enabled by default.

For out-of-path deployments, to optimize MAPI Exchange 2003, you must define fixed-target, in-path rules that specify the following ports on the client-side Steelhead appliance: the Microsoft end-point mapper port: 135; the Steelhead appliance port for Exchange traffic: 7830; the Steelhead appliance port for Exchange Directory Name Service Provider Interface (NSPI) traffic: 7840.

You must restart the optimization service for your changes to take effect.

The **no** command option disables MAPI 2003 acceleration.

Example

```
amnesiac (config) # no protocol mapi 2k3 enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol mapi"

protocol mapi 2k7 native enable

Description

Enables optimization to occur if you have Outlook 2007 and Exchange Server 2003 or Exchange Server 2007.

Syntax

[no] protocol mapi 2k7 native enable

Parameters

None

Usage

Sharing calendars between Outlook 2007 and Exchange 2007 increases the number of connections (anywhere from 1 to 2 extra connections per each user sharing calendars). The connections are persistent and remain even when users are not actively checking other user's calendars. Enabling this option helps keep connection counts at sustained, low levels, thereby increasing optimization.

Important: In contrast to Outlook 2003, Outlook 2007 uses encrypted communication with the Exchange Server by default, regardless of the Exchange Server Version (Exchange Server 2003 or Exchange Server 2007). Leaving encryption on will disable MAPI optimizations. You must disable encryption on the Exchange (Outlook) 2007 clients before enabling this option.

You can apply a group policy to disable encryption for the Outlook 2007 clients on a wider scale.

If you have Outlook 2007, regardless of the Exchange Server version (Exchange Server 2003 or Exchange Server 2007), communication is encrypted by default. To enable optimization to take place, you must perform the following steps:

1. Make sure you are running v3.0.8 or higher of the Steelhead software. If you are not, you must upgrade your software. For details, see the *Steelhead Appliance Management Console User's Guide*.
2. Disable encryption on the Exchange (Outlook) 2007 clients. For information, refer to your Microsoft documentation.
3. At the Steelhead appliance CLI system prompt, enter the following command:

   ```
   protocol mapi 2k7 native enable
   ```

For details on disabling encryption, see https://support.riverbed.com/kb/solution.htm?id=501700000008VT8AAM.

You must restart the optimization service for your changes to take effect.

The **no** command option disables fallback. Optimization does not occur if you specify the **no** command option.

Example

```
amnesiac (config) # no protocol mapi 2k7 native enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol mapi"

protocol mapi enable

Description

Enables MAPI optimization support.

Syntax

[no] protocol mapi enable

Parameters

None

Usage

MAPI optimization is enabled by default. Typically, you disable MAPI optimization to troubleshoot problems with the system. For example, if you are experiencing problems with Outlook clients connecting with Exchange, you can disable MAPI latency acceleration (while continuing to optimize with SDR for MAPI).

The **no** command option disables MAPI optimization for testing purposes.

You must restart the optimization service for your changes to take effect.

For example, if you are experiencing problems with Outlook clients connecting with Exchange, you can disable MAPI latency acceleration (while continuing to optimize with SDR for MAPI) by issuing the **no protocol mapi enable** command.

Example

```
amnesiac (config) # no protocol mapi enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol mapi"

protocol mapi encrypted delegation enable

Description

Provides encrypted MAPI optimization using the Kerberos delegation facility.

Syntax

[no] protocol mapi encrypted delegation enable

Parameters

None

Usage

Enable this option if you are encrypting MAPI traffic for Windows 7 or earlier client versions. Both the server-side and client-side Steelhead appliances must be running RiOS v6.1.

In RiOS v6.1, delegation mode includes support for trusted domains, wherein users are joined to a different domain from the filer being accessed.

For detailed information about encrypted MAPI optimization, see the *Steelhead Appliance Management Console User's Guide*.

Delegation mode requires additional configuration. For details, see "Windows Domain Authentication Delegation Commands" on page 604.

You must restart the optimization service for your changes to take effect.

The **no** command disables this feature.

Example

```
amnesiac (config) # protocol mapi encrypted delegation enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"Windows Domain Authentication Delegation Commands"

protocol mapi encrypted enable

Description

Enables encrypted MAPI RPC traffic optimization between Outlook and Exchange. By default, this option is disabled.

Syntax

[no] protocol mapi encrypted enable

Parameters

None

Usage

The basic steps to enable encrypted optimization are:

- The server-side Steelhead appliance must join the same Windows Domain that the Exchange server belongs to and operate as a member server.
- Verify that Outlook is encrypting traffic.
- Enable this option on the server-side and client-side Steelhead appliance.
- Restart the Steelhead appliance.

Notes:

- When this option and MAPI Exchange 2007 acceleration are enabled on either Steelhead appliance, MAPI Exchange 2007 acceleration remains in effect for unencrypted connections.
- By default, this feature supports NTLM authentication.
- The Steelhead appliance passes through Kerberos encrypted traffic.

MAPI encryption is not supported on Windows 7.

You must restart the optimization service for your changes to take effect.

The **no** command option disables this option.

Example

```
amnesiac (config) # protocol mapi encrypted enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol mapi"

protocol mapi encrypted native-krb enable

Description

Enables end-to-end Kerberos authentication support for encrypted MAPI signing.

Syntax

[no] protocol mapi encrypted native-krb enable

Parameters

None

Usage

The **no** command option disables end-to-end Kerberos support for encrypted MAPI signing.

Example

```
amnesiac (config) # protocol mapi encrypted native-krb enable
```

Product

Steelhead appliance

Related Topics

"show protocol mapi"

protocol mapi encrypted ntlm-auth enable

Description

Enables NTLM authorization for encrypted MAPI RPC traffic between Outlook and Exchange. This feature is enabled by default.

Syntax

[no] protocol mapi encrypted ntlm-auth enable

Parameters

None

Usage

You must restart the optimization service for your changes to take effect.

The **no** command option disables this option.

Example

```
amnesiac (config) # no protocol mapi encrypted ntlm-auth enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol mapi"

protocol mapi outlook-anywhr auto-detect

Description

Enables Remote Procedure Call (RPC) over HTTP and HTTPS Auto-Detect Outlook Anywhere connections.

Syntax

[no] protocol mapi outlook-anywhr auto-detect

Parameters

None

Usage

This command automatically detects RPC over the HTTP and HTTPS protocols used by Outlook Anywhere.

You can enable RPC over HTTP and HTTPS using this command or you can set in-path rules. The auto-detect option in the MAPI page is best for simple Steelhead configurations with only a single Steelhead at each site and when the IIS server is also handling Web sites. If the IIS server is only used as RPC Proxy, and for configurations with asymmetric routing, connection forwarding or Interceptor installations, add in-path rules that identify the RPC Proxy server IP addresses and use this command. For more information on Outlook Anywhere configuration, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # protocol mapi outlook-anywhr auto-detect
```

Product

Steelhead appliance

Related Topics

"show protocol mapi"

protocol mapi outlook-anywhr enable

Description

Enables RPC over HTTP and HTTPS for Outlook Anywhere.

Syntax

[no] protocol mapi outlook-anywhr enable

Parameters

None

Usage

Enables Outlook Anywhere latency optimization. Outlook Anywhere is a feature for Microsoft Exchange Server 2007 and 2010 that allows Microsoft Office Outlook 2003, 2007, and 2010 clients to connect to their Exchange servers over the Internet using the RPC over HTTP(S) Windows networking component. By default, this feature is disabled.

To use this feature, you must also enable HTTP optimization on the client-side and server-side Steelheads (HTTP optimization is enabled by default). If you are using Outlook Anywhere over HTTPS, you must enable the secure inner channel and the Microsoft Internet Information Server (IIS) SSL certificate must be installed on the server-side Steelhead appliance. For more information on Outlook Anywhere, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # protocol mapi outlook-anywhr enable
```

Product

Steelhead appliance

Related Topics

"show protocol mapi," "protocol http enable"

protocol mapi outlook-anywhr ex365domain

Description

Enables the Exchange 365 domain for Outlook Anywhere.

Syntax

[no] protocol mapi outlook-anywhr ex365domain <domain>

Parameters

<domain>	Specify a comma separated list of Exchange 365 domains for Outlook Anywhere. The default value is ".office365.com,outlook.com".

Usage

For more information on Outlook Anywhere, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # protocol mapi outlook-anywhr ".office365.com,.outlook.com"
```

Product

Steelhead appliance

Related Topics

"show protocol mapi," "protocol http enable"

protocol mapi port

Description

Sets the incoming MAPI Exchange port.

Syntax

[no] protocol mapi port <port>

Parameters

<port>	Specify the MAPI port number. The default value is 7830.

Usage

Specify the MAPI Exchange port for optimization. Typically, you do not need to modify the default value, 7830.

If you have changed the MEISI port in your Exchange Server environment, change port 7830 to the static port number you have configured in your Exchange environment. For further information about changing (MEISI) ports, see the Microsoft Exchange Information Store Interface at: https://support.microsoft.com/kb/270836/en-us

You must restart the optimization service for your changes to take effect.

The **no** command option resets the MAPI port to the default value.

Example

```
amnesiac (config) # protocol mapi port 2125
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol mapi"

protocol mapi port-remap enable

Description

Sets MAPI port remapping settings.

Syntax

[no] protocol mapi port-remap enable

Parameters

None

Usage

You must restart the optimization service for your changes to take effect.

The **no** command option resets the MAPI port to the default value.

Example

```
amnesiac (config) # protocol mapi port-remap enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol mapi"

protocol mapi prepop enable

Description

Enables MAPI transparent prepopulation.

Syntax

[no] protocol mapi prepop enable | max-connections <number> | poll-interval <minutes> | timeout <seconds>]

Parameters

enable	Enables MAPI transparent prepopulation.
max-connections <number>	Specify the maximum number of virtual MAPI connections to the Exchange Server for Outlook clients that have shut down. Setting the maximum connections limits the aggregate load on all Exchange servers through the configured Steelhead appliance. The default value varies by model; for example, on a 5520 the default is 3750. You must configure the maximum connections on both the client and server-side of the network. The **no** option resets max-connections to the default.
poll-interval <minutes>	Specify the polling interval in minutes. The default value is 20. The **no** option resets max-connections to the default.
timeout <seconds>	Specify the time out period in seconds. The default value 96. The **no** option resets max-connections to the default.

Usage

This feature allows email data to be delivered between the Exchange server and the client-side appliance while the Outlook client is off-line. When a user logs into their MAPI client, the mail has already been seen by the client-side appliance and can be retrieved with LAN-like performance. This feature enables email to be optimized even though it has not been seen before by the client.

You must restart the optimization service for your changes to take effect.

The **no** command option disables MAPI prepopulation support. If you specify the **no** option and parameters, you do not disable MAPI prepopulation support; you reset the specified parameter to its default value.

Example

```
amnesiac (config) # no protocol mapi prepop enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol mapi,""show prepop"

MS-SQL Blade Support Commands

This section describes the MS-SQL blade support commands. The commands for MS-SQL support must be implemented by Riverbed professional services. Improper use can result in undesirable effects.

The MS-SQL blade supports other database applications, but you must define SQL rules to obtain maximum optimization. If you are interested in enabling the MS-SQL blade for other database applications, contact Riverbed professional services.

You must restart the Steelhead service after enabling this feature.

protocol ms-sql default-rule query-rule

Description

Sets MS-SQL protocol default-query rule settings.

Syntax

[no] protocol ms-sql default-rule query-rule rule-id <rule-id> action-id <action-id> arg-offset enable

Parameters

rule-id <rule-id>	Specify and MS-SQL protocol query-rule ID.
action-id <action-id>	Specify an MS-SQL protocol query-rule action-id.
arg-offset <arg-offset>	Specify a protocol query-rule argument off-set.

Usage

The **no** command option disables query rule settings.

Example

```
amnesiac (config) # protocol ms-sql default-rule query-rule rule-id 10 enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql default-rule rpc-rule

Description

Sets MS-SQL protocol default query rule settings.

Syntax

[no] protocol ms-sql default-rule rpc-rule rule-id <rule-id> action-id <action-id> [arg-offset | enable]

Parameters

rule-id <rule-id>	Specify and MS-SQL protocol RPC-rule ID.
action-id <action-id>	Specify an ID that uniquely identifies a match.
arg-offset <arg-offset>	Specify a protocol RPC-rule argument off-set.

Usage

The **no** command option disables default query rule ID.

Example

```
amnesiac (config) # protocol ms-sql default-rule rpc-rule rule-id 12 enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql enable

Description

Enables MS-SQL blade support. Enabling the MS-SQL blade supports MS Project optimization.

Syntax

[no] protocol ms-sql enable

Parameters

None

Usage

The commands for MS-SQL support must be implemented by Riverbed professional services. Improper use can result in undesirable effects.

The MS-SQL blade supports other database applications, but you must define SQL rules to obtain maximum optimization. If you are interested in enabling the MS-SQL blade for other database applications, contact Riverbed professional services.

You must restart the Steelhead service after enabling this feature.

The **no** command option disables SQL blade support.

Example

```
amnesiac (config) # protocol ms-sql enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql fetch-next enable

Description

Enables pre-fetching requests to request the next row in MS Project. The server-side Steelhead appliance pre-fetches sequential row results and the client-side Steelhead appliance caches them. You decide which cursors or queries are cacheable.

Syntax

[no] protocol ms-sql fetch-next enable

Parameters

None

Usage

To determine which cursors or queries are cacheable, you configure rules. By default, all fetch next queries are cacheable.

You must restart the Steelhead service after enabling this feature.

The **no** command option removes pre-fetching requests.

Example

```
amnesiac (config) # protocol ms-sql fetch-next enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql num-preack

Description

Specify the maximum number of **sp_execute** (or save project) requests to pre-acknowledge before waiting for a server response to be returned.

Syntax

[no] protocol ms-sql num-preack <number-preack>

Parameters

<number-preack>	Specify the maximum number of pre-acknowledgements. The default value is 5.

Usage

You can enable pre-acknowledgement if the client application does not need a result value from the server.

For example, when you save a project in MS Project, server-side procedures are invoked many times to write or update database data. To maximize optimization, the **protocol ms-sql num-preack** command limits the number of pre-acknowledgements from the server.

The **no** command option disables pre-acknowledgement.

Example

```
amnesiac (config) # protocol ms-sql num-preack 6
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql port

Description

Specify the server port to listen on for SQL requests.

Syntax

[no] protocol ms-sql port <port>

Parameters

<port>	Specify the SQL server port to listen on for requests. The default value is 1433.

Usage

The **no** command option resets the SQL server port to the default value.

Example

```
amnesiac (config) # protocol ms-sql port 2433
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql query-act rule-id action-id num-reps

Description

Specify a query action when the corresponding query match occurs.

Syntax

[no] protocol ms-sql query-act rule-id <rule_id> action-id <action_id> num-reps <num_reps> | invalidate {flush-all | flush-rule}] [miss-policy <policy> | allow-preack {true | false} | scope {sfe | cfe}]]

Parameters

rule-id <rule_id>	Specify the rule identification number that uniquely identifies the rule.
action-id <action_id>	Specify the action identification number that uniquely identifies this action within the rule.
num-reps <num_reps>	Specify how many times the action is to be repeated.
invalidate <invalidate_action> {flush-all | flush-rule}	Invalidates the specified action: **flush-all** or **flush-rule**.
miss-policy <policy>	Specify the MS-SQL cache miss policy.
allow-preack {true | false}	Specify whether to allow the MS-SQL pre-acknowledgment (**true**) or not (**false**).
scope {sfe | cfe}	Specify MS-SQL scope: **sfe** or **cfe**.

Usage

You can specify the following types of actions:

- prefetch requests as specified in query argument actions.
- invalidate prefetched cache entries.

The **no** command option disables the query action.

Example

```
amnesiac (config) # protocol ms-sql query-act rule-id 10 action-id 1 num-reps 1 miss-policy 1
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql query-arg-act rule-id action-id arg-offset expr

Description

Specify how the query arguments should be modified when prefetching queries.

Syntax

[no] protocol ms-sql query-arg-act rule-id <rule_id> action-id <action_id> arg-offset <arg_offset> expr <expression>

Parameters

rule-id <rule_id>	Specify the rule identification number that uniquely identifies the rule.
action-id <action_id>	Specify the action identification number that uniquely identifies this action within the rule.
arg-offset <arg_offset>	Specify the SQL query argument to be modified.
expr <expression>	Specify the SQL query expression.

Usage

The **no** command option disables the SQL query argument.

Example

```
amnesiac (config) # protocol ms-sql query-arg-act rule-id 1 action-id 1 arg-offset 15 expr "select *"
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql query-rule rule-id app-name-regex query-regex

Description

Specify how the query arguments should be modified when prefetching queries.

Syntax

[no] protocol ms-sql query-rule rule-id <rule-id> app-name-regex <app_name> query-regex <query-regex>

Parameters

rule-id <rule_id>	Specify the rule identification number that uniquely identifies the rule.
app-name-regex <app_name>	Specify the client application name (standard string expression).
query-regex <query-regex>	Specify string specifying regex match for RPC query.

Usage

The **no** command option disables the SQL query argument.

Example

```
amnesiac (config) # protocol ms-sql query-rule rule-id 3 app-name-regex test query-regex "string
specifying regex match for RPC query"
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql rpc-act rule-id action-id

Description

Specify an RPC action when a match occurs.

Syntax

[no] protocol ms-sql rpc-act rule-id <rule_id> action-id <action_id> [[num-reps <num_reps> | invalidate {flush-all | flush-rule}] [miss-policy <policy> | allow-preack {true | false} | allow-prefetch {true | false} | scope {sfe | cfe}]]

Parameters

rule-id <rule_id>	Specify the rule identification number that uniquely identifies the rule.
action-id <action_id>	Specify the action identification number that uniquely identifies this action within the rule.
num-reps <num_reps>	Specify how many times the action is to be repeated
invalidate <invalidate_action> {flush-all | flush-rule}	Invalidates the specified action: **flush-all** or **flush-rule**.
miss-policy <policy>	Specify the MS-SQL cache miss policy.
allow-preack {true | false}	Specify whether to allow the MS-SQL pre-acknowledgment (**true**) or not (**false**).
allow-prefetch {true | false}	Specify whether to allow MS-SQL pre-fetch (**true**) or not (**false**).
scope {sfe | cfe}	Specify MS-SQL scope: **sfe** or **cfe**.

Usage

You can specify the following types of actions:

- prefetch requests as specified in query argument actions.
- invalidation of prefetched cache entries.
- whether the fetch next requests can be prefetched.
- whether **spe_execute** requests can be pre-acknowledged.

The **no** command option disables the RPC action.

Example

```
amnesiac (config) # protocol ms-sql rpc-act rule-id 2 action-id 1 invalidate flush-all
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql rpc-arg rule-id action-id arg-offset expr

Description

Specify how the RPC argument should be modified when prefetching queries.

Syntax

[no] protocol ms-sql rpc-arg rule-id <rule_id> action-id <action_id> expr <expr>

Parameters

rule-id <rule_id>	Specify the rule identification number that uniquely identifies the rule.
action-id <action_id>	Specify the action identification number that uniquely identifies this action within the rule.
arg-offset <arg_offset>	Specify the RPC argument parameter.
expr <expr>	Specify the regular expression for the RPC value.

Usage

The **no** command option disables the RPC argument.

Example

```
amnesiac (config) # protocol ms-sql rpc-arc rule-id 1 arg-offset 1 expr "replace select
PROJ_READ_COUNT, PROJ_LOCKED, PROJ_READ_WRITE,PROJ_READ_ONLY, PROJ_ID, PROJ_MACHINE_ID,
PROJ_DATA_SOURCE from MSP_PROJECTS where PROJ_NAME = '$1' "
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql rpc-arg-act rule-id arg-offset expr

Description

Specify a RPC argument used to determine if the RPC request matches a rule.

Syntax

[no] protocol ms-sql rpc-arg-act rule-id <rule_id> arg-offset <arg_offset> expr <expr>

Parameters

rule-id <rule_id>	Specify the rule identification number that uniquely identifies the rule.
arg-offset <arg_offset>	Specify the RPC argument parameter.
expr <expr>	Specify the regular expression for the RPC value.

Usage

The **no** command option disables the RPC argument.

Example

```
amnesiac (config) # protocol ms-sql rpc-arg-act rule-id 2 arg-offset 1 arg-offset 0 expr "replace
select PROJ_READ_COUNT, PROJ_LOCKED, PROJ_READ_WRITE,PROJ_READ_ONLY, PROJ_ID, PROJ_MACHINE_ID,
PROJ_DATA_SOURCE from MSP_PROJECTS where PROJ_NAME = '$1' "
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql rpc-rule rule-id app-name-regex

Description

Specify the RPC rule.

Syntax

[no] protocol ms-sql rpc-rule rule-id <rule-id <rule_id> app-name-regex <app_name> {[rpc-id <rpc_id> num-params <num_params>] | [rpc-query-regex <regex_match_for_rpc_query_string>] | [cursor-type <cursor_type>]}

Parameters

rule-id <rule_id>	Specify the rule identification number that uniquely identifies the rule.
app-name-regex <app_name>	Specify the client application name (standard string expression).
rpc-id <rpc_id>	Specify the RPC identifier.
num-params <num_params>	Specify the expected number of parameters in the SQL query.
rpc-query-regex <regex_match_for_rpc_query_string>	Specify the RPC name (standard string expression).
cursor-type <cursor_type>	Specify the cursor type for the RPC query. Depending on cursor type, the client can read forward or backward, from beginning or end, or read an arbitrary position in the result set: • **forward-only** - Only the next rows can be read. The row pointer cannot be moved back. • **dynamic** - The rows must be read in forward or reverse relative to current row pointer. The row pointer cannot be moved to an arbitrary index except for first and last positions. • **static** - The rows can be read forward or reverse or at an arbitrary position.

Usage

The **no** command option disables the rule.

Example

```
amnesiac (config) # protocol ms-sql rpc-rule rule-id 1 app-name-regex test rpc-id 2 num-params 1
rpc-query-regex test cursor-type static
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

protocol ms-sql support-app

Description

Specify a regular expression (standard string) for an application name that can be optimized using the MS-SQL blade.

Syntax

[no] protocol ms-sql support-app <name> collation <collation> | misc <misc> | unicode {-1, 0, 1}

Parameters

support-app <name>	Specify the name of the application to be supported by the MS-SQL blade.
collation <collation>	Specify MS-SQL protocol collation mode settings.
misc <misc>	Specify MS-SQL protocol miscellaneous settings.
unicode {-1, 0, 1}	Specify the unicode character set: -1, 0 or 1.

Usage

The **no** command option removes the application from MS-SQL blade support.

Example

```
amnesiac (config) # protocol ms-sql support-app msproject
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ms-sql"

NFS Support Commands

This section describes the NFS support commands.

protocol nfs alarm v2-v4 clear

Description

Resets the NFS v2 and v4 alarm.

Syntax

[no] protocol nfs alarm v2-v4 clear

Parameters

None

Usage

You can also access this command in enable mode.

The **no** command option sets the NFS v2 and v4 alarm.

Example

```
amnesiac (config) # protocol nfs alarm v2-v4 clear
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol nfs"

protocol nfs default server

Description

Configures default settings for NFS servers.

Syntax

[no] protocol nfs default server {direntrymap <cr> | policy [custom | global_rw] | read-ahead [small-files <cr> | transfer-size <size>] | read-dir [optimize <cr> | read-size <size>] | threshold multiple <multiple> | write [optimize <cr> | max-data <max>]}

Parameters

direntrymap <cr>	Enables the directory entry map.
policy [custom | global_rw]	Specify one of the following policies: • **custom** - Enables you to turn on or off the root squash feature for NFS volumes from this server. • **global-rw** - Specify a policy that provides a trade-off of performance for data consistency. All of the data can be accessed from any client, including LAN based NFS clients (which do not go through the Steelhead appliances) and clients using other file protocols like CIFS. This option severely restricts the optimizations that can be applied without introducing consistency problems. This is the default configuration.
read-ahead [small-files <cr> | transfer-size <size>]	Enables read-ahead for small files; sets the transfer size in bytes.
read-dir [optimize <cr> | read-size <size>]	Enables read optimization for the directory; sets the read size in bytes.
threshold multiple <multiple>	Specify the threshold multiple.
write [optimize <cr> | max-data <max>	Enables write optimization for the directory; sets the maximum write size in bytes.

Usage

The **no** command option resets the value of a given option. For example, no protocol nfs default server policy resets the policy to the default value.

Example

```
amnesiac (config) # protocol nfs default server read-dir optimize
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol nfs"

protocol nfs default volume

Description

Configures default settings for the NFS volumes.

Syntax

[no] protocol nfs default volume {perm_cache | policy [custom | global_rw] |root-squash <cr>}

Parameters

perm_cache	Enables a permission cache. Specify this option if the server uses ACLs or if your server is configured to map client user IDs. This option enables the Steelhead appliance to optimize traffic without violating the permissions model.
policy [custom | global_rw]	Specify one of the following policies: • **custom** - Enables you to turn on or off the root squash feature for NFS volumes from this server. • **global-rw** - Specify a policy that provides a trade-off of performance for data consistency. All of the data can be accessed from any client, including LAN based NFS clients (which do not go through the Steelhead appliances) and clients using other file protocols like CIFS. This option severely restricts the optimizations that can be applied without introducing consistency problems. This is the default configuration.
root-squash <cr>	Enables root squashing. Root-squashing allows an NFS server to map any incoming user ID 0 or guest ID 0 to another number that does not have super user privileges, often -2 (the nobody user).

Usage

NFS file system objects have owners and permissions and the NFS optimizer conforms to the file system permissions model by enforcing file server and volume policies.

The **no** command option resets the value of a given option.

```
Example
amnesiac (config) # protocol nfs default volume root-squash
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol nfs"

protocol nfs enable

Description

Enables the NFS optimizer. The NFS optimizer provides latency optimization improvements for NFS operations primarily by prefetching data, storing it on the client Steelhead appliance for a short amount of time, and using it to respond to client requests.

Syntax

[no] protocol nfs enable

Parameters

None

Usage

The **no** command option disables the NFS optimizer.

Example

```
amnesiac (config) # protocol nfs enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol nfs"

protocol nfs max-directories

Description

Sets the maximum size of NFS directories.

Syntax

[no] protocol nfs max-directories <bytes>

Parameters

<bytes>	Specify a number of bytes between 0 and 4294967295.

Usage

The **no** command option resets the size to the default.

Example

```
amnesiac (config) # protocol nfs max-directories 4294967295
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol nfs"

protocol nfs max-symlinks

Description

Specify, in bytes, the maximum size of NFS symbolic link directories.

Syntax

[no] protocol nfs max-symlinks <bytes>

Parameters

<bytes>	Specify a number of bytes between 0 and 4294967295.

Usage

The **no** command option resets the size to the default.

Example

```
amnesiac (config) # protocol nfs max-symlinks 4294967295
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol nfs"

protocol nfs memory

Description

Specify, in percent, the soft-limit size (warning threshold) and hard-limit size (error threshold) of memory usage.

Syntax

[no] protocol nfs memory [soft-limit <percent> | hard-limit <percent>]

Parameters

<percent>	Specify a percent to establish the respective thresholds.

Usage

The **no** command option resets the limit to the default.

Example

```
amnesiac (config) # protocol nfs memory hard-limit 95
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol nfs"

protocol nfs server

Description

Configures settings for the specified NFS server.

Syntax

[no] protocol nfs server <name> default volume enable | default volume perm-cache | default volume policy [custom | global_rw | read_only] | default volume root-squash | direntrymap <cr> | ip <address> | policy [custom | global_rw | read_only] | read-ahead [small-files <cr> | transfer-size <size>] | read-dir [optimize <cr> | read-size <size>] | threshold multiple <multiple> | volume id <fsid> <cr> volume id <fsid> policy [custom | global_rw | home_dir] volume id <fsid> root-squash write [optimize <cr> | max-data <max>]

Parameters

<name>	Specify the name of the NFS server.
default volume enable	Enables defaults to be used by all volumes on the server.
default volume perm-cache	Enables the permission cache.
default volume policy [custom | global_rw | read_only]	Specify the default volume policy to the type specified: • **custom** - Enables you to turn on or off the root squash feature for NFS volumes from this server. • **global-rw** - Specify a policy that provides a trade-off of performance for data consistency. All of the data can be accessed from any client, including LAN based NFS clients (which do not go through the Steelhead appliances) and clients using other file protocols like CIFS. This option severely restricts the optimizations that can be applied without introducing consistency problems. This is the default configuration. • **read-only** - Any client can read the data on the NFS server or volume but cannot make changes.
default volume root-squash	Enables root-squashing by default on new volumes. Root-squashing allows an NFS server to map any incoming user ID 0 or guest ID 0 to another number that does not have super user privileges, often -2 (the nobody user).
direntrymap <cr>	Enables the directory entry map.
ip <address>	Specify the IP address of the NFS server.
policy [custom | global_rw | read_only]	On the NFS server, sets one of the following policies: • **custom** - Enables you to turn on or off the root squash feature for NFS volumes from this server. • **global-rw** - Specify a policy that provides a trade-off of performance for data consistency. All of the data can be accessed from any client, including LAN based NFS clients (which do not go through the Steelhead appliances) and clients using other file protocols like CIFS. This option severely restricts the optimizations that can be applied without introducing consistency problems. This is the default configuration. • **read-only** - Any client can read the data on the NFS server or volume but cannot make changes.
read-ahead [small-files <cr> |transfer-size <size>]	Enables read-ahead for small files; sets the transfer size in bytes.
read-dir [optimize <cr> | read-size <size>]	Enables read optimization for the directory and sets the read size in bytes.
threshold multiple <multiple>	Specify the threshold multiple.
volume id <fsid> <cr>	Specify the file system volume identification (ID).

volume id <fsid> policy [custom | global_rw | read_only]	Specify the file system ID and policy. On the specified volume, sets one of the following policies: • **custom** - Enables you to turn on or off the root squash feature for NFS volumes from this server. • **global-rw** - Specify a policy that provides a trade-off of performance for data consistency. All of the data can be accessed from any client, including LAN based NFS clients (which do not go through the Steelhead appliances) and clients using other file protocols like CIFS. This option severely restricts the optimizations that can be applied without introducing consistency problems. This is the default configuration. • **read-only** - Any client can read the data on the NFS server or volume but cannot make changes.
volume id <fsid> root-squash	Enables root-squashing on the specified volume.
write [optimize <cr> | max-data <max>	Enables write optimization for the directory; sets the maximum write size in bytes.

Usage

NFS objects have owners and permissions and the NFS optimizer conforms to the file system permissions model by enforcing file server and volume policies.

The **no** command option disables the NFS server.

Example

```
amnesiac (config) # protocol nfs server exampleserver volume id 21
```

Product

Steelhead appliance, CSH

Related Topics

“show protocol nfs”

protocol nfs v2-v4-alarm

Description

Enables the NFS v2 and v4 alarm.

Syntax

[no] protocol nfs v2-v4-alarm

Parameters

None

Usage

The **no** command option disables the alarm.

Example

```
amnesiac (config) # protocol nfs v2-v4-alarm
```

Product

Steelhead appliance, CSH

Related Topics

“show protocol nfs”

Lotus Notes Commands

This section describes the Lotus Notes support commands.

protocol notes enable

Description

Enables Lotus Notes optimization.

Syntax

[no] protocol notes enable

Parameters

None

Usage

Lotus Notes is a client-server collaborative application that provides mail, instant messaging, calendar, resource, and file sharing. RiOS provides latency and bandwidth optimization for Lotus Notes v6.0 and later traffic across the WAN, accelerating email attachment transfers and server-to-server or client-to-server replications.

RiOS saves bandwidth by automatically disabling socket compression (which makes SDR more effective), and by decompressing Huffman-compressed attachments and LZ-compressed attachments when they are sent or received and recompressing them on the other side. This allows SDR to recognize attachments which have previously been sent in other ways, that is; over CIFS, HTTP, or other protocols, and also allows SDR to optimize the sending and receiving of attachments that are slightly changed from previous sends and receives.

To use this feature both the client-side and server-side Steelhead appliances must be running RiOS v5.5.x or later.

Enabling Lotus Notes provides latency optimization regardless of the compression type (Huffman, LZ, or none). RiOS can optimize Lotus Notes with port encryption on or off. To optimize Lotus Notes with port encryption and decryption, both the client-side and server-side Steelhead appliances must be running RiOS v6.0.x or later. The client-side and server-side Steelhead appliances become a trusted part of the Lotus client-server security model to retrieve the session ID keys.

When optimizing Lotus Notes traffic with encryption on, you can optionally use the Steelhead inner channel trust to ensure all Notes traffic sent between the client-side and the server-side Steelhead appliances are secure.

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol notes enable
```

Product

Steelhead appliance, CSH

Related Topics

"protocol notes pull-repl enable," "show protocol notes"

protocol notes encrypt blacklist remove-ip

Description

Removes the specified IP address from the blacklist.

Syntax

[no] protocol notes encrypt blacklist remove-ip {<ip-address> | all}

Parameters

<ip-address>	Specify the IP address to remove from the blacklist.
all	Clear the blacklist.

Usage

The **protocol notes encrypt blacklist remove-ip <ip-address>** command option removes the specified IP address from the blacklist. The **protocol notes encrypt blacklist remove-ip all** command clears the blacklist.

Example

```
amnesiac (config) # protocol notes encrypt blacklist remove-ip 10.1.1.2
```

Product

Steelhead appliance

Related Topics

"protocol notes encrypt enable," "show protocol notes encrypt"

protocol notes encrypt enable

Description

Enables encrypted Lotus Notes optimization.

Syntax

[no] protocol notes encrypt enable

Parameters

None

Usage

The **no protocol notes encrypt enable** command disables encrypted Lotus Notes.

Example

```
amnesiac (config) # protocol notes encrypt enable
```

Product

Steelhead appliance

Related Topics

"protocol notes enable," "show protocol notes encrypt"

protocol notes encrypt import server-id

Description

Imports the specified server ID file.

Syntax

protocol notes encrypt import server-id <url> [password <password>]

Parameters

<url>	Specify the URL to upload the server ID file from. Contact the Domino server administrator to obtain the location of the file. Use one of the following formats:
	`http://domain/path/to/file`
	`ftp://user:password@domain/relative/path/to/file`
	`ftp://user:password@domain//absolute/path/to/file`
	`scp://user:password@domain/absolute/path/to/file`

password <password>	Optionally, specify an alphanumeric password if the server ID file is encrypted with a password.

Usage

The **protocol notes encrypt import server-id** command uploads the file from the specified URL, decrypts it, and stores decrypted information in the secure vault. The original file is not stored.

The server ID file might or might not be encrypted with a password. Contact the Domino server administrator to determine whether you need to specify a password.

Example

```
amnesiac (config) # protocol notes encrypt import server-id scp://user:password@server/path/
server.id
```

Product

Steelhead appliance

Related Topics

"protocol notes enable," "show protocol notes encrypt"

protocol notes encrypt remove server-id

Description

Removes the decrypted information for an imported server ID from the Steelhead appliance.

Syntax

protocol notes encrypt remove server-id <servername>

Parameters

<servername>	Specify the server name to remove.

Usage

Use the **protocol notes encrypt remove server-id** command if you need to remove the decrypted information from the Steelhead appliance.

Example

```
amnesiac (config) # protocol notes encrypt remove server-id CN=gcs-120/O=acme
```

Product

Steelhead appliance

Related Topics

"protocol notes enable," "show protocol notes encrypt"

protocol notes encrypt server-port

Description

Sets the unencrypted server port setting used by the server-side Steelhead appliance.

Syntax

[no] protocol notes encrypt server-port <port-number>

Parameters

<port-number>	Specify the port number.

Usage

Use the **protocol notes encrypt server-port** command to specify which unencrypted port on the Domino server the server-side Steelhead appliance connects to. You must first configure an alternate unencrypted port on the Domino server. If the standard TCP port 1352 is not configured to require encryption, you can use it instead of configuring an alternate unencrypted port.

For details on how to configure the alternate unencrypted port on the Domino server, see the *Steelhead Appliance Deployment Guide - Protocols.*

Example

```
amnesiac (config) # protocol notes encrypt server-port 1352
```

Product

Steelhead appliance

Related Topics

"protocol notes enable," "show protocol notes encrypt"

protocol notes port

Description

Configures the Lotus Notes port for optimization. Typically, you do not need to modify the port.

Syntax

[no] protocol notes port <port-number>

Parameters

<port-number>	Specify the port number for optimization. The default value is 1352.

Usage

The **no** command option reverts to the default port.

Example

```
amnesiac (config) # protocol notes port 1222
```

Product

Steelhead appliance, CSH

Related Topics

"protocol notes enable," "protocol notes port," "protocol notes pull-repl enable," "show protocol notes"

protocol notes pull-repl enable

Description

Enables pull replication for Lotus Notes protocol connections.

Syntax

[no] protocol notes pull-repl enable

Parameters

None

Usage

In pull replication, the current Steelhead appliance requests information from the source Steelhead appliance. The request specifies the information that the current Steelhead appliance needs, based on its knowledge of changes already received from the source Steelhead appliance and from all other domain controllers in the domain. When the current Steelhead appliance receives information from the source, it updates that information. The current Steelhead appliance's next request to the source Steelhead appliance excludes the information that has already been received and applied.

The **no** command disables this feature.

Example

```
amnesiac (config) # protocol notes pull-repl enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol notes"

Citrix Support Commands

This section describes the Citrix support commands.

protocol citrix cdm enable

Description

Enables Citrix client device mapping.

Syntax

[no] protocol citrix cdm enable

Parameters

None

Usage

Use the **protocol citrix cdm enable** command on the client-side and server-side Steelhead appliances to provide latency optimization for file transfers that use CDM between the Citrix client and server. CDM allows a remote application running on the server to access printers and disk drives attached to the local client machine. The applications and system resources appear to the user at the client machine as if they are running locally during the session. For example, in the remote session, C: is the C drive of the remote machine and the C drive of the local thin client appears as H:.

Bidirectional file transfers between the local and remote drives use one of many virtual channels within the ICA protocol. The individual data streams that form the communication in each virtual channel are all multiplexed onto a single ICA data stream. This feature provides latency optimization for file transfers in both directions.

You can use CDM optimization with or without secure ICA encryption. Both the client-side and server-side Steelhead appliances must be running RiOS v7.0.

By default, CDM optimization is disabled.

Enabling CDM optimization requires an optimization service restart.

Example

```
amnesiac (config) # protocol citrix cdm enable
amnesiac (config)# service restart
```

Product

Steelhead appliance

Related Topics

"protocol citrix enable"

protocol citrix enable

Description

Enables Citrix optimization.

Syntax

[no] protocol citrix enable

Parameters

None

Usage

To consolidate operations, some organizations install thin clients in their branch offices and install a Citrix Presentation Server in the data center to front-end the applications. The proprietary protocol that Citrix uses to move updates between the client and the server is called ICA (Independent Computing Architecture). The thin clients at the branch offices have a Citrix ICA client accessing the services at the data center which are front-ended by a Citrix Presentation Server (also called Citrix Metaframe Server in earlier versions).

RiOS v6.0 and later provides the following ways to recognize, prioritize, and optimize Citrix traffic:

- Optimize the native ICA traffic bandwidth.
- Classify and shape Citrix ICA traffic using QoS.

For details on shaping Citrix traffic using QoS, see the *Steelhead Appliance Deployment Guide - Protocols*.

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol citrix enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol citrix"

protocol citrix ica

Description

Configures the Citrix ICA port for optimization. Typically, you do not need to modify the port.

Syntax

[no] protocol citrix ica port <port>

Parameters

<port>	Specify the Citrix ICA port for optimization. The default value is 1494.

Usage

The **no** command option reverts to the default port.

Example

```
amnesiac (config) # protocol citrix ica port 1222
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol citrix"

protocol citrix multiport enable

Description

Enables support for the Citrix multiport ICA.

Syntax

[no] protocol citrix multiport enable

Parameters

None

Usage

The **no** command option disables support for Citrix multiport ICA.

Example

```
amnesiac (config) # protocol citrix multiport enable
```

Product

Steelhead appliance

Related Topics

"show protocol citrix"

protocol citrix multiport priority

Description

Configures the priority and port for Citrix multiport ICA support.

Syntax

[no] protocol citrix multiport priority <priority> port <port>

Parameters

<priority>	Specify the priority number. The range is from 0 through 3.
<port>	Specify the Citrix ICA port. Port 2598 is the default port for Citrix priority 0.

Usage

The priority and port parameters specified by the **protocol citrix multiport priority** command override the default values. The **no** command option removes the specified port and priority.

Example

```
amnesiac (config) # protocol citrix multiport priority 0 port 25980
amnesiac (config) # protocol citrix multiport priority 1 port 2598
amnesiac (config) # protocol citrix multiport priority 2 port 25982
amnesiac (config) # protocol citrix multiport priority 3 port 25983
```

Product

Steelhead appliance

Related Topics

"show protocol citrix"

protocol citrix secure-ica enable

Description

Enables Citrix SecureICA encryption.

Syntax

[no] protocol citrix secure-ica enable

Parameters

None

Usage

Citrix SecureICA optimization will not function properly while either or both ICA port 1494 and CGP port 2598 are in the Interactive Port Label list. To view port labels, see "show port-label". To remove a port label, see "Port Label Commands" on page 500.

The **no** command option disables SecureICA.

Example

```
amnesiac (config) # protocol citrix secure-ica enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol citrix"

protocol citrix session reliability port

Description

Configures the Common Gateway Protocol (CGP) connections. Typically, you do not need to modify the port.

Syntax

[no] protocol citrix session reliability port <port>

Parameters

<port>	Specify the port number for CGP connections. The session reliability port uses CGP to keep the session window open even if the connection to the application experiences an interruption. The session window remains open while the system restores the connection. The default value is 2598.

Usage

To use session reliability, you must enable Citrix optimization on the Steelhead appliance in order to classify the traffic correctly. For details, see *Steelhead Appliance Management Console User's Guide*.

You can use session reliability with optimized traffic only. Session reliability with RiOS QoS does not support pass-through traffic. For details about disabling session reliability, go to http://support.citrix.com/proddocs/index.jsp?topic=/xenapp5fp-w2k8/ps-sessions-sess-rel.html

The **no** command option reverts to the default port.

Example

```
amnesiac (config) # protocol citrix session reliability port 2333
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol citrix"

protocol citrix smallpkts enable

Description

Enables Citrix low-overhead traffic optimization.

Syntax

[no] protocol citrix smallpkts enable

Parameters

None

Usage

Riverbed recommends as a best practice that you enable enhanced data reduction for low-overhead real-time Citrix traffic such as keyboard, mouse, and other Citrix packets of fewer than 64 bytes. Citrix low-overhead traffic optimization is disabled by default.

Example

```
amnesiac (config) # protocol citrix smallpkts enable
```

Product

Steelhead appliance

Related Topics

"protocol citrix smallpkts threshold,""show protocol citrix"

protocol citrix smallpkts threshold

Description

Sets the threshold for Citrix low-overhead traffic optimization.

Syntax

[no] protocol citrix smallpkts threshold <threshold>

Parameters

<threshold>	Specify the threshold value for Citrix small packets.

Usage

The default threshold is 64 bytes.

Example

```
amnesiac (config) # protocol citrix smallpkts threshold 62
```

Product

Steelhead appliance

Related Topics

"protocol citrix smallpkts enable,""show protocol citrix"

FCIP Support Commands

This section describes the FCIP (Fiber Channel over IP) support commands. For details on FCIP optimization, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide - Protocols*.

protocol fcip enable

Description

Enables FCIP (Fiber Channel over IP) optimization. By default, RiOS directs all traffic on the standard ports 3225, 3226, 3227, and 3228 through the FCIP optimization module.

FCIP optimization is disabled by default.

Environments with RF-originated SRDF traffic between VMAX arrays need additional configuration to isolate and optimize the DIFs embedded within the headers of the FCIP data payload. For details, see "protocol fcip rule".

Syntax

[no] protocol fcip enable

Parameters

None

Usage

Fibre Channel over TCP/IP (FCIP) is a transparent Fibre Channel (FC) tunneling protocol that transmits FC information between FC storage facilities over IP networks. FCIP is designed to overcome the distance limitations of FC.

FCIP storage optimization provides support for environments using storage technology that originates traffic as FC and then uses either a Cisco MDS or a Brocade 7500 FCIP gateway to convert the FC traffic to TCP for WAN transport.

To increase the data reduction LAN-to-WAN ratio with either equal or greater data throughput in environments with FCIP traffic, RiOS separates the FCIP headers from the application data workload written to storage. The FCIP headers contain changing protocol state information, such as sequence numbers. These headers interrupt the network stream and reduce the ability of SDR to match large, contiguous data patterns. After isolating the header data, the Steelhead appliance performs SDR network deduplication on the larger, uninterrupted storage data workload and LZ compression on the headers. RiOS then optimizes, reassembles, and delivers the data to the TCP consumer without compromising data integrity.

Environments with SRDF traffic originated through Symmetrix FC ports (RF ports) only require configuration of the RiOS FCIP storage optimization module. Traffic originated through Symmetrix GigE ports (RE ports) require configuration of the RiOS SRDF storage optimization module. For details on storage technologies that originate traffic through FC, see the *Steelhead Appliance Deployment Guide*.

You configure the RiOS FCIP storage optimization module on the Steelhead appliance closest to the FCIP gateway that opens the FCIP TCP connection by sending the initial SYN packet. This can vary by environment. If you are unsure which gateway initiates the SYN, enable FCIP on both the client-side and server-side Steelhead appliances.

If you have enabled or disabled FCIP optimization or changed a port, you must restart the optimization service.

The **no** command option disables this feature.

For details, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # protocol fcip enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol fcip rules," "show protocol fcip settings"

protocol fcip ports

Description

Add ports to the list of FCIP ports.

Syntax

[no] protocol fcip ports <port list>

Parameters

<port list>	Specify a comma-separated list of port numbers. The default port numbers are the standard FCIP ports: 3225, 3226, 3227, and 3228.

Usage

Optionally, you can add FCIP port numbers separated by commas or remove a port number. Do not specify a port range

For details on FCIP optimization, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

To delete one or more port number settings, use the following syntax:

```
   no protocol fcip ports <port list>
```

Example

```
amnesiac (config) # protocol fcip ports 3225,3226,3227,3228
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol fcip rules," "show protocol fcip settings"

protocol fcip rule

Description

Configures FCIP rules.

Syntax

[no] protocol fcip rule [src-ip <ip-addr>] [dst-ip <ip-addr>] | [dif <enable | disable>] | [dif-blocksize <bytes>]

Parameters

src-ip <ip-addr>	Specify the connection source IP address of the FCIP gateway tunnel endpoints. Use the format XXX.XXX.XXX.XXX. The source IP address cannot be the same as the destination IP address.
dst-ip <ip-addr>	Specify the connection destination IP address of the FCIP gateway tunnel endpoints. Use the format XXX.XXX.XXX.XXX.
dif <enable | disable>	Specify this option to isolate and optimize the DIFs embedded within the FCIP data workload
dif-blocksize <bytes>	Specify the size of a standard block of storage data, in bytes, after which a DIF header begins. The valid range is from 1 - 2048 bytes. The default value is 512, which is a standard block size for Open System environments. When you enable DIF, RiOS FCIP optimization looks for a DIF header after every 512 bytes of storage data unless you change the default setting. Open System environments (such as Windows, UNIX, and Linux) inject the DIF header into the data stream after every 512 bytes of storage data. IBM iSeries (AS/400) host environments inject the DIF header into the data stream after every 520 bytes. This parameter is required when you enable DIF.

Usage

For rules to take effect, FCIP optimization must be enabled by the "protocol fcip enable" command.

Environments with RF-originated SRDF traffic between VMAX arrays need additional configuration beyond enabling FCIP optimization. You need to add FCIP rules to isolate the Data Integrity Field (DIF) headers within the FCIP data stream. These DIF headers further interrupt the data stream. You can add or remove FCIP rules by defining a match for source or destination IP traffic.

The FCIP default rule optimizes all remaining traffic that has not been selected by another rule. It always appears as the last in the list. You cannot remove the default rule; however, you can change its DIF setting. The default rule uses 0.0.0.0 in the source and destination IP address fields, specifying all IP addresses. You cannot specify 0.0.0.0 as the source or destination IP address for any other rule.

For details on FCIP, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # protocol fcip rule src-ip 1.1.1.1 dst-ip 2.2.2.2 dif enable
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"protocol fcip enable," "protocol fcip ports," "show protocol fcip rules," "show protocol fcip settings"

protocol fcip stat-port

Description

Set the port for FCIP aggregate statistics.

Syntax

[no] protocol fcip stat-port <port>

Parameters

<port>	Specify the port for FCIP aggregate statistics.

Usage

You can view combined throughput and reduction statistics for two or more FCIP tunnel ports using this command.

If you have enabled or disabled FCIP optimization or changed a port, you must restart the optimization service.

For details on FCIP, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # protocol fcip stat-port 1243
amnesiac (config) # service restart
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show protocol fcip rules," "show protocol fcip settings"

SRDF Support Commands

This section describes the SRDF (Symmetrix Remote Data Facility) support commands. For details on SRDF optimization, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

protocol srdf enable

Description

Enables Symmetrix Remote Data Facility (SRDF) optimization. By default, RiOS directs all traffic on the standard port 1748 through the SRDF module for enhanced SRDF header isolation.

Environments with RF-originated SRDF traffic between VMAX arrays need additional configuration to isolate and optimize the DIFs embedded within the headers of the data payload. For details, see "protocol srdf rule" on page 597.

RE ports are Symmetrix Fiber Channel ports.

SRDF optimization is disabled by default.

Syntax

[no] protocol srdf enable

Parameters

None

Usage

SRDF storage optimization provides support for environments using storage technology that originates traffic through Symmetrix GigE ports (RE ports). For details on storage technologies that originate traffic through GigE RE ports, see the *Steelhead Appliance Deployment Guide*.

To increase the data reduction LAN-to-WAN ratio with either equal or greater data throughput in environments with SRDF traffic, RiOS separates the SRDF headers from the application data workload written to storage. The SRDF headers contain changing protocol state information, such as sequence numbers. These headers interrupt the network stream and reduce the ability of SDR to match large, contiguous data patterns. After isolating the header data, the Steelhead appliance performs SDR network deduplication on the larger, uninterrupted storage data workload and LZ compression on the headers. RiOS then optimizes, reassembles, and delivers the data to the TCP consumer without compromising data integrity.

Traffic originated through Symmetrix GigE ports (RE ports) require configuration of the RiOS SRDF storage optimization module. Environments with SRDF traffic originated through Symmetrix FC ports (RE ports) require configuration of the RiOS FCIP storage optimization module. For details, see "protocol fcip enable" on page 593.

You configure the SRDF storage optimization module on the Steelhead appliance closest to the Symmetrix array that opens the SRDF TCP connection by sending the initial SYN packet. This can vary by environment. If you are unsure which array initiates the SYN, configure SRDF on both the client-side and server-side Steelhead appliances.

If you have enabled or disabled SRDF optimization or changed a port, you need to restart the optimization service.

For details on SRDF optimization in general, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol srdf enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol srdf rules", "show protocol srdf settings"

protocol srdf ports

Description

Add ports to the list of SRDF ports.

Syntax

[no] protocol srdf ports <port list>

Parameters

<port list>	Specify a comma-separated list of ports. The default SRDF port number is 1748.

Usage

Optionally, you can add SRDF port numbers separated by commas or remove a port number. Do not specify a port range

For details on SRDF optimization, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

If you have enabled or disabled SRDF optimization or changed a port, you need to restart the optimization service.

Example

```
amnesiac (config) # protocol srdf ports 139,445,1748
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol srdf rules", "show protocol srdf settings"

protocol srdf rule

Description

Adds or deletes a manual SRDF rule.

Syntax

[no] protocol srdf rule [src-ip <ip-addr>] [dst-ip <ip-addr>] | [dif <enable | disable>] | [dif-blocksize <bytes>]

Parameters

src-ip <ip-addr>	Specify the connection source IP address of the Symmetrix DMX or VMAX GigE ports (RE ports) originating the replication. **Note:** The source IP address cannot be the same as the destination IP address.
dst-ip <ip-addr>	Specify the connection destination IP address of the Symmetrix DMX or VMAX GigE ports (RE ports) receiving the replication. Use the format XXX.XXX.XXX.XXX.
dif <enable | disable>	Specify this option to isolate and optimize the Data Integrity Fields embedded within the SRDF data workload. For example, VMAX.
dif-blocksize <bytes>	Specify the size of a standard block of storage data, in bytes, after which a DIF header begins. The valid range is from 1 - 2048 bytes. The default value is 512, which is a standard block size for Open System environments. When you enable DIF, RiOS SRDF optimization looks for a DIF header after every 512 bytes of storage data unless you change the default setting. Open System environments (such as Windows, UNIX, and Linux) inject the DIF header into the data stream after every 512 bytes of storage data. IBM iSeries (AS/400) host environments inject the DIF header into the data stream after every 520 bytes. This field is required when you enable DIF.

Usage

Environments with GigE-based (RE port) originated SRDF traffic between VMAX arrays need to isolate DIF headers within the data stream. These DIF headers further interrupt the data stream.

When the R1 Symmetrix array is running Enginuity microcode version 5875 or newer, manual SRDF rules are not necessary. In 5875+ environments, RiOS is capable of auto-detecting the presence of DIF headers and DIF blocksize for GigE-based (RE port) SRDF traffic.

To manually isolate the DIF headers when the R1 Symmetrix array is running Enginuity microcode version 5874 or older, you add SRDF rules by defining a match for source or destination IP traffic.

The SRDF default rule optimizes all remaining traffic that has not been selected by another rule. It always appears as the last in the list. You cannot remove the default rule; however, you can change the DIF setting of the default rule. The default rule uses 0.0.0.0 in the source and destination IP address fields, specifying all IP addresses. You cannot specify 0.0.0.0 as the source or destination IP address for any other rule.

Do not add a module rule isolating DIF headers in mainframe environments, as SRDF environments that replicate mainframe traffic do not currently include DIF headers.

Auto-detected SRDF settings in Enginuity 5875+ environments will override any manual SRDF rules that might be configured.

For details on SRDF, see the *Steelhead Appliance Management Console User's Guide* and the *Steelhead Appliance Deployment Guide*.

Example

```
amnesiac (config) # protocol srdf rule src-ip 1.1.1.1 dst-ip 2.2.2.2 dif enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol srdf rules", "show protocol srdf settings"

protocol srdf symm id address

Description

Creates a Symmetrix ID for SRDF selective optimization. The SRDF selective optimization enables you to set different optimization levels for RDF groups.

Syntax

[no] protocol srdf symm id <group ID> address <ip-addr>

Parameters

id <group id>	Specify a Symmetrix ID. The Symmetrix ID is an alpha-numeric string (for example, a standard Symmetrix serial number: 000194900363).
address <ip-addr>	Specify an IP address of the of the Symmetrix DMX or VMAX GigE ports (RE ports) originating the replication.

Usage

A Symmetrix ID allows the Steelhead appliance to identify the traffic coming from a Symmetrix storage array using the Symmetrix GigE port (RE port) IP address.

Use this command to create a new Symmetrix ID with the specified IP address or you can add an IP address to an existing Symmetrix ID.

The **no protocol srdf symm id <group ID>** removes the group ID. The **no protocol srdf symm id <group ID> address <ip-addr>** removes the specified IP address from the group ID.

Example

```
amnesiac (config) # protocol srdf symm id 001213 address 1.1.1.1
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol srdf symm"

protocol srdf symm id base_rdf_group

Description

Sets the Remote Data Facility (RDF) group number value to a 0-based or a 1-based group type.

Syntax

[no] protocol srdf symm id <Symm ID> base_rdf_group <RDF base-type>

Parameters

id <group id>	Specify a Symmetrix ID. The Symmetrix ID is an alpha-numeric string (for example, a standard Symmetrix serial number: 000194900363).
rdf_group <RDF base-type>	Specify the RDF base type: • **0** - Specify if your RDF group is a 0-based group type. • **1** - Specify if your RDF group is a 1-based group type. This is the default value for RDF groups.

Usage

RiOS allows you to configure RDF group numbers starting from 0 or 1. EMC tools used in Open Systems environments (such as EMC Solutions Enabler) typically refer to RDF groups in the 1-based notation. Mainframe-based tools typically use the 0-based notation.

Use this command if you want to change from the default 1-based type to the 0-based type, such as to match the notation that for a Symmetrix mainframe environment.

Example

```
amnesiac (config) # protocol srdf symm id 0123 base_rdf_group 0
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol srdf symm"

protocol srdf symm id rdf_group

Description

Adds a selective optimization Remote Data Facility (RDF) rule for traffic coming from Symmetrix GigE ports (RE ports).

Syntax

[no] protocol srdf symm id <group ID> rdf_group <RDF group ID> optimization <sdr-default | lz-only | none> | [description <description>]

Parameters

id <group id>	Specify a Symmetrix ID. The Symmetrix ID is an alpha-numeric string (for example, a standard Symmetrix serial number: 000194900363).
rdf_group <RDF group ID>	Specify the RDF group. An RDF group is a number from 1-255 by default, or 0-254 if the **protocol symm id base_rdf_group** setting has been set to 0.
optimization <sdr-default | lz-only | none>	Specify an optimization policy: • **sdr-default** - Specify to enable SDR and LZ compression. The default value is **sdr-default**. • **lz-only** - Specify to enable LZ compression only. There is no SDR optimization with this setting. • **none** - Specify to disable SDR and LZ compression.
description <"description">	Optionally, provide a description that describes the RDF rule. For example, Oracle Applications.

Usage

SRDF selective optimization enables you to set different optimization levels for RDF groups. The optimization level is based on the compression characteristics of the data in the groups. For each Symmetrix ID, you specify an optimization policy for the RDF groups that appear in the data stream associated with the specified ID.

You can configure the optimization level from no compression (**none**) to full Scalable Data Replication (**sdr-default**). SDR optimization includes LZ compression on the *cold*, first-pass of the data. You can also configure LZ-compression alone (**lz-only**) with no SDR. For some applications, it might be more important to get maximum throughput with minimal latency, and without compression, (such as, when excess WAN bandwidth is available and when it's known that the data in that RDF Group will not be reducible), and for others getting maximum reduction is more important.

The **no protocol srdf symm id <group ID>** removes the optimization setting for the group ID.

Example

```
amnesiac (config) # protocol srdf symm id 0815 rdf_group 1 optimization lz-only description "Oracle
Forms"
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol srdf symm"

SnapMirror Support Commands

This section describes commands that provide optimization support for NetApp SnapMirror data replication operations. SnapMirror is a licensed utility used for disaster recovery and replication. The Steelhead appliance improves the performance of the WAN for NetApp SnapMirror by overcoming limited bandwidth restrictions, high latency, and poor network quality commonly associated with wide-area networks. RiOS 8.5 introduces new advanced benefits that further improve WAN performance, visibility, and control of NetApp SnapMirror. Advanced SnapMirror optimization support is for environments using NetApp Data ONTAP v7 or Data ONTAP v8 operating in 7-mode.

protocol snapmirror enable

Description

Enables support for SnapMirror data replication optimization on the Steelhead appliance.

Syntax

[no] protocol snapmirror enable

Parameters

None

Usage

RiOS v8.5 introduces new advanced benefits that further improve WAN performance, visibility, and control for NetApp SnapMirror. RiOS presents performance statistics and applies optimization policies based on source and destination volumes and/or filer pairs. RiOS provides the ability to fine tune network QoS policies for individual volumes and filers, or for SnapMirror as a whole.

To benefit from advanced SnapMirror optimization, both the destination filer-side and source filer-side Steelhead appliances must be running RiOS v8.5.

The **no protocol snapmirror enable** command disables SnapMirror optimization support. By default, SnapMirror optimization support is disabled. If you have enabled or disabled SnapMirror optimization or changed a port, you must restart the optimization service.

Example

```
amnesiac (config) # protocol snapmirror enable
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"show protocol snapmirror"

protocol snapmirror filer address

Description

Creates a new filer identifier with a specified address or modifies an existing filer ID.

Syntax

[no] protocol snapmirror filer <name> address <ipv4-address>

Parameters

<name>	Specify the name of the filer.
<ipv4-address>	Specify the source IPv4 address to associate with the filer.

Usage

A filer is a NetApp storage device.

Use this command to create a new filer ID with the specified IP address or you can add an IP address to an existing filer ID. By default, SnapMirror optimization support is disabled. If you have enabled or disabled SnapMirror optimization or changed a setting, you must restart the optimization service.

Example

```
amnesiac (config) # protocol snapmirror filer CENTRALFILER address 10.32.146.160
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"show protocol snapmirror"

protocol snapmirror filer

Description

Configures SnapMirror settings for a filer.

Syntax

[no] protocol snapmirror filer <name> [optimization <policy>] [priority <policy>] [description <description>]

Parameters

filer <name>	Specify the name of the filer.
optimization <policy>	Specify an optimization policy for the filer: • **sdr-default** - Specify to enable SDR and LZ compression. The default value is **sdr-default**. • **lz-only** - Specify to enable LZ compression only. There is no SDR optimization with this setting. • **none** - Specify to disable SDR and LZ compression.
priority <policy>	Specify the priority policy for the filer: • **highest** - Highest priority • **high** - High priority • **medium** - Medium priority • **low** - Low priority • **lowest** - Lowest priority • **none** - Priority not set
description <description>	Optionally, specify a filer description or provide additional comments.

Usage

A filer is a NetApp storage device. Use this command to prioritize replication job priority and optimization policy by filer.

You can configure the optimization level from no compression (**none**) to full Scalable Data Replication (**sdr-default**). SDR optimization includes LZ compression on the *cold*, first-pass of the data. You can also configure LZ-compression alone (**lz-only**) with no SDR. For some applications, it might be more important to get maximum throughput with minimal latency, and without compression, and for others getting maximum reduction is more important.

The **no** version of the command removes the optimization settings for the filer. By default, SnapMirror optimization support is disabled. If you have enabled or disabled SnapMirror optimization or changed a setting, you must restart the optimization service

Example

```
amnesiac (config) # protocol snapmmirror filer ksnap1 address 10.11.100.1
amnesiac (config) # protocol snapmmirror filer ksnap1 optimization lz-only priority medium
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"show protocol snapmirror"

protocol snapmirror filer volume

Description

Configures SnapMirror settings for a volume.

Syntax

[no] protocol snapmirror filer <name> volume <volume> [optimization <policy>] [priority <policy>] [description <description>]

Parameters

filer <name>	Specify the name of the filer.
volume <volume>	Specify the name of the volume.
optimization <policy>	Specify an optimization policy used only as a volume policy: • **sdr-default** - Specify to enable SDR and LZ compression. • **lz-only** - Specify to enable LZ compression only. There is no SDR optimization with this setting. • **filer-default** - Specify to match the optimization policy of the filer. This is the default policy for a volume. • **none** - Specify to disable SDR and LZ compression.
priority <policy>	Specify the priority policy for the volume: • **highest** - Highest priority • **high** - High priority • **medium** - Medium priority • **low** - Low priority • **lowest** - Lowest priority • **none** - Priority not set.
description <description>	Optionally, specify a volume description or provide additional comments.

Usage

A filer is a NetApp storage device. Use this command to prioritize replication job priority and optimization policy by volume.

You can configure the optimization level from no compression (**none**) to full Scalable Data Replication (**sdr-default**). SDR optimization includes LZ compression on the *cold*, first-pass of the data. You can also configure LZ-compression alone (**lz-only**) with no SDR. For some applications, it might be more important to get maximum throughput with minimal latency, and without compression, and for others getting maximum reduction is more important. The **filer-default** option is the default option for a volume.

The **no** version of the command removes the optimization settings for the volume. By default, SnapMirror optimization support is disabled. If you have enabled or disabled SnapMirror optimization or changed a setting, you need to restart the optimization service

Example

```
amnesiac (config) # protocol snapmmirror filer ksnap1 address 10.11.100.1
amnesiac (config) # protocol snapmmirror filer ksnap1 volume vol1 optimization sdr-default
amnesiac (config) # protocol snapmmirror filer ksnap1 volume vol2 optimization lz-only priority
medium
amnesiac (config) #protocol snapmirror filer ksnap1 volume vol3 optimization none priority highest
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"show protocol snapmirror"

protocol snapmirror ports

Description

Adds ports to the list of SnapMirror ports.

Syntax

[no] protocol snapmirror ports <port list>

Parameters

<port-list>	Specify a comma-separated list of ports.

Usage

By default, RiOS directs all traffic on the standard port 10566 through the SnapMirror module for optimization. Optionally, you can specify nonstandard individual SnapMirror port numbers, separated by commas. Do not specify a port range. SnapMirror optimization does not support port 10565 for multipath traffic.

The **no protocol snapmirror ports <port-list>** command removes the list of SnapMirror ports.

If you have enabled or disabled SnapMirror optimization or changed a port, you must restart the optimization service.

Example

```
amnesiac (config) # protocol snapmirror ports 10566,345,1755
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"show protocol snapmirror settings"

Windows Domain Authentication Delegation Commands

Delegation mode in RiOS v6.1 or later automatically updates the delegate user in Active Directory with delegation rights to servers. The service updates the user in real-time, eliminating the need to grant the user access to delegate on every server. This section describes how to give special privileges to the delegate user so they have automatic delegation rights to servers.

Before you enable domain authentication delegation, you must first create a Delegate User with a Service Principal Name (SPN). A delegate user is required in each of the domains where a server is going to be optimized. After you create a Delegate User, you enable delegation for the user on the domain controller. For details, see the *Steelhead Appliance Management Console User's Guide*.

You can only add one delegate user per domain. A delegate user is required in each of the domains where a server is going to be optimized. A delegate user that is an Administrator already has the correct delegation rights for auto-delegation mode.

protocol domain-auth delegation auto-mode enable

Description

Enables auto-delegation mode.

Syntax

[no] protocol domain-auth delegation auto-mode enable

Parameters

None

Usage

This command enables delegate user authentication and automatically discovers the servers on which to delegate and sign. This eliminates the need to set up the servers to sign to for each domain.

Before performing Windows Domain authentication delegation using the CLI, Windows-side domain controller and SPN (Service Principal Names) configuration is required. For details, see the *Steelhead Appliance Management Console User's Guide*.

Use this mode if you have previously enabled SMB Signing with RiOS v5.5.x, SMB2 signing, or if you are enabling MAPI encryption for Windows 7 in RiOS v6.1 or later.

The **no** command option disables this feature.

Note: A delegate user is required in each of the domains where a server is going to be optimized.

Example

```
amnesiac (config) # protocol domain-auth delegation auto-mode enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show protocol domain-auth delegation auto-mode," "show protocol domain-auth delegation rules,""show protocol domain-auth oneway-trust"

protocol domain-auth delegation auto-mode enable

Description

Enables auto-delegation mode.

Syntax

[no] protocol domain-auth delegation auto-mode enable

Parameters

None

Usage

This command enables delegate user authentication and automatically discovers the servers on which to delegate and sign. This eliminates the need to set up the servers to sign to for each domain.

Before performing Windows Domain authentication delegation using the CLI, Windows-side domain controller and SPN (Service Principal Names) configuration is required. For details, see the *Steelhead Appliance Management Console User's Guide*.

Use this mode if you have previously enabled SMB Signing with RiOS v5.5.x, SMB2 signing, or if you are enabling MAPI encryption for Windows 7 in RiOS v6.1 or later.

The **no** command option disables this feature.

Note: A delegate user is required in each of the domains where a server is going to be optimized.

Example

```
amnesiac (config) # protocol domain-auth delegation auto-mode enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show protocol domain-auth delegation auto-mode," "show protocol domain-auth delegation rules," "show protocol domain-auth delegation rules," "show protocol domain-auth oneway-trust"

protocol domain-auth delegation delegate-user

Description

Configures a delegate account for the Active Directory domain.

Syntax

[no] protocol domain-auth delegation delegate-user [domain <domain>] [user <username>] [password <password>]

Parameters

domain <domain>	Specify the delegation domain in which you want to make the delegate user a trusted member, for example: `SIGNING.TEST`
user <username>	Specify the delegate user name. The maximum length is 20 characters. The username cannot contain any of the following characters: / \ [ ] : ; | = , + * ? < > @ " **Note:** The system translates the user name into uppercase to match the registered server realm information.
password <password>	Specify the password.

Usage

Before performing Windows Domain authentication delegation using the CLI, Windows-side domain controller and SPN (Service Principal Names) configuration is required. For details, see the *Steelhead Appliance Management Console User's Guide*.

Use this mode if you have previously enabled SMB signing with RiOS v5.5.x, SMB2 signing, or if you are enabling MAPI encryption for Windows 7 in RiOS v6.1 or later.

Note: A delegate user that is an administrator already has the correct delegation rights for automatic delegation mode.

The **no** command removes the specified user.

Example

```
amnesiac (config) # protocol domain-auth delegation delegate-user domain SIGNING.TEST user testname
password RR1243
amnesiac (config) # service restart
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show protocol domain-auth delegation rules," "show protocol domain-auth delegation rules," "show protocol domain-auth oneway-trust"

protocol domain-auth delegation rule dlg-all-except

Description

Allows delegated Windows Domain authentication to intercept all of the connections except those destined for the servers in this list.

Syntax

[no] protocol domain-auth delegation rule dlg-all-except <ip-addr>

Parameters

<ip-addr>	Specify the file server IP addresses that do not require SMB signing, SMB2 signing, or MAPI encryption in the text box, separated by commas. By default, this setting is disabled. Only the file servers that do not appear in the list are signed or encrypted. You must register any servers on not this list with the domain controller or be using Auto-Delegation Mode.

Usage

Before performing Windows Domain authentication delegation using the CLI, Windows-side domain controller and SPN (Service Principal Names) configuration is required. For details, see the *Steelhead Appliance Management Console User's Guide*.

The **no** command option allows the specified server IP addresses.

Example

```
amnesiac (config) # protocol domain-auth delegation rule dlg-all-except 3.3.3.3,4.4.4.4
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show protocol domain-auth delegation auto-mode," "show protocol domain-auth delegation rules," "show protocol domain-auth delegation rules," "show protocol domain-auth oneway-trust"

protocol domain-auth delegation rule dlg-only

Description

Allows delegated Windows Domain authentication to only the specified servers.

Syntax

[no] protocol domain-auth delegation rule dlg-only <ip-addr>

Parameters

<ip-addr>	Specify the file server IP addresses for SMB signed or MAPI encrypted traffic in the text box, separated by commas. You can switch between the Delegate-Only (**dlg-only**) and Delegate-All-Except (**dlg-all-except**) controls without losing the list of IP addresses for the control. Only one list is active at a time.

Usage

Before performing Windows Domain authentication delegation using the CLI, Windows-side domain controller and SPN (Service Principal Names) configuration is required. For details, see the *Steelhead Appliance Management Console User's Guide*.

The **no** command disallows the specified server IP addresses.

Example

```
amnesiac (config) # protocol domain-auth delegation rule dlg-only 3.3.3.3,4.4.4.4
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show protocol domain-auth delegation rules," "show protocol domain-auth delegation rules," "show protocol domain-auth oneway-trust"

protocol domain-auth delegation rule select

Description

Specifies which set of server rules (Delegate-Only or Delegate-All-Except) to apply.

Syntax

protocol domain-auth delegation rule select {dlg-only | dlg-all-except}

Parameters

dlg-only	Specify this option to apply the rule defined by the "protocol domain-auth delegation rule dlg-only" command.
dlg-all-except	Specify this option to apply the rule defined by the "protocol domain-auth delegation rule dlg-all-except" command.

Usage

After configuring the commands "protocol domain-auth delegation rule dlg-all-except" and "protocol domain-auth delegation rule dlg-only", use this command to specify which resulting list to apply.

Example

```
amnesiac (config) # protocol domain-auth delegation rule select dlg-only
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show protocol domain-auth delegation auto-mode," "show protocol domain-auth delegation rules," "show protocol domain-auth oneway-trust"

protocol domain-auth encrypted-ldap enable

Description

Enables encrypted Lightweight Directory Access Protocol (LDAP) support for auto-delegation mode.

Syntax

protocol domain-auth encrypted-ldap enable

Parameters

None

Usage

This command provides support for auto-delegation mode in Active Directory environments that require encrypted LDAP communication.

Example

```
amnesiac (config) # protocol domain-auth encrypted-ldap enable
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth delegation auto-mode"

protocol domain-auth migrate

Description

Migrates domain authentication credentials to the secure vault.

Syntax

protocol domain-auth migrate

Parameters

None

Usage

This command configures the Steelhead appliance to use the secure vault for domain authentication credentials.

Example

```
amnesiac (config) # protocol domain-auth migrate
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth credentials location"

protocol domain-auth restricted-krb enable

Description

Enables or disables Kerberos authentication for domains with restricted trust models.

Syntax

[no] protocol domain-auth restricted-krb enable

Usage

Use the **no** command to disable Kerberos authentication for domains with restricted trust models. See the *Steelhead Appliance Deployment Guide - Protocols* for more information on deployment scenarios.

Example

```
amnesiac (config) # protocol domain-auth restricted-krb enable
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth restricted-krb"

protocol domain-auth oneway-trust

Description

Configures a valid one-way trusted domain for Windows Domain authentication.

Syntax

[no] protocol domain-auth oneway-trust [dns-name <domain>] [netbios-name <netbios-name>] | [all]

Parameters

<domain>	Specify the hostname of the delegation domain.
<netbios-name>	Specify the NetBIOS domain name of the delegation domain.
all	Clears all entries in the one-way trust list. **Note:** The **all** parameter is only used with the **no** command.

Usage

Use the **no** command for the following:

- To clear an entry in the one-way trust list keyed on the NetBIOS name:

  ```
  no protocol domain-auth oneway-trust netbios-name
  ```

- To clear an entry in the one-way trust list keyed on dns name:

  ```
  no protocol domain-auth oneway-trust dns-name
  ```

- To clear all entries in the one-way trust list:

  ```
  no protocol domain-auth oneway-trust all
  ```

Example

```
amnesiac (config) # protocol domain-auth oneway-trust dns-name ns1.something.en.wikipedia.org
netbios-name wikipedia
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show protocol domain-auth delegation auto-mode," "show protocol domain-auth delegation rules," "show protocol domain-auth delegation rules," "show protocol domain-auth oneway-trust"

Windows Domain Authentication Replication Commands

Kerberos end-to-end authentication in RiOS 7.0 relies on Active Directory replication to obtain machine credentials for any servers that require secure protocol optimization. The RiOS replication mechanism requires a domain user with AD privileges and involves the same AD protocols used by Windows domain controllers.

protocol domain-auth replication replicate-user

Description

Configures trusted domain authentication replication settings.

Syntax

[no] protocol domain-auth replication replicate-user domain <domain> user-domain <user-domain> user <name> password <password> [rodc {<true | false} dcname <dcname>]

Parameters

domain <domain>	Specify the Active Directory replication domain. The domain name must be in Active Directory domain name format. The Steelhead appliance replicates accounts from this domain.
user-domain <user-domain>	Specify the domain that the user belongs to, if different from the Active Directory domain name. Riverbed recommends that you configure the user domain as close to the root as possible.
user <name>	Specify the replication user name. The maximum length is 20 characters. The username cannot contain any of the following characters: / \ [ ] : ; | = , + * ? < > @ " **Note:** The system translates the user name into uppercase to match the registered server realm information.
password <password>	Specify the user account password.
rodc <true | false>	Function as read-only domain controller (RODC) settings for this domain. Specify **true** to enable the RODC function. Specify **false** to disable the RODC function.
dcname <dcname>	Specify the Windows domain controller for this domain.

Usage

Kerberos end-to-end authentication in RiOS 7.0 relies on Active Directory replication to obtain machine credentials for any servers that require secure protocol optimization. The RiOS replication mechanism requires a domain user with AD replication privileges and involves the same AD protocols used by Windows domain controllers.

Example

```
amnesiac (config) # protocol domain-auth replication replicate-user domain REPLICATION.TEST user
testname password RR1243
```

Product

Steelhead appliance

Related Topics

"show protocol domain-auth replication replicate-user"

Remote Packet Analysis Integration Commands

This section describes the remote packet analysis integration commands.

cascade shark enable

Description

Enables the Shark function.

Syntax

[no] cascade shark enable

Parameters

None

Usage

The **cascade shark enable** command enables Cascade Pilot software to perform remote packet analysis integration on trace files captured and stored on the Steelhead appliance.

The Steelhead appliance automatically opens ports 61898 and 61899 when this command is enabled and connects directly to the Shark function through these TCP ports. None of the RiOS processes are involved in this connection.

Remote packet analysis integration is enabled only if the Shark user has a password.

Example

```
amnesiac (config) # cascade shark enable
```

Product

Steelhead appliance

Related Topics

"user shark," "show cascade shark"

user shark

Description

Configures the Shark user account settings.

Syntax

[no] user shark [comment | disable | gecos | nopassword | password <cleartext> | password {0 <cleartext>| 7 <encrypted-string>}]

Parameters

comment <comment>	Add comment to the user account.
disable	Disable the user account.
gecos	Set the gecos option.
nopassword	Allow login to this account without a password.
password { 0 <cleartext> |7 <encrypted-string>}	Specify the password. Choose one of the following: • <cleartext> - Specify a login password in clear text. This option is the same as the 0 <cleartext> option and is provided for backward compatibility. • **0** - Specify a login password in clear text. • **7** - Specify a login password with an encrypted string.

Usage

The **no user shark** command deletes the user account. The **no user shark disable** command option reenables the account.

Example

```
amnesiac (config) # user shark password 0 administrator
```

Product

Steelhead appliance

Related Topics

"cascade shark enable," "show cascade shark"

PFS Support Commands

This section describes the PFS support commands. PFS is an integrated virtual file server that allows you to store copies of files on the Steelhead appliance with Windows file access, creating several options for transmitting data between remote offices and centralized locations with improved performance. Data is configured into file shares and the shares are periodically synchronized transparently in the background, over the optimized connection of the Steelhead appliance. PFS leverages the integrated disk capacity of the Steelhead appliance to store file-based data in a format that allows it to be retrieved by NAS clients.

Important: Do not configure both RSP and PFS on the same Steelhead appliance. Riverbed does not support this configuration because PFS has no disk boundaries and can overwrite the space allocated to RSP.

Note: PFS is supported on Steelhead appliance models 150, 250, 520, 550, 1010, 1020, 1050, 1520, 2010, 2011, 2020, 2050, 2510, 2511, 3010, 3020, 3030, 3510, 3520, and 5010. Virtual Steelhead and Cloud Steelhead models do not support PFS. PFS is not supported on Steelhead appliance CX *xx*55 models.

Note: RiOS v7.0 and later does not run on the *xx*20 models.

Note: The PFS commands **pfs domain** and **pfs workgroup** have been replaced by **domain join** and **workgroup join**. For detailed information, see "domain rejoin" on page 505 and "workgroup join" on page 508.

pfs enable

Description

Enables PFS. PFS is an integrated virtual file server that allows you to store copies of files on the Steelhead appliance with Windows file access, creating several options for transmitting data between remote offices and centralized locations with improved performance. Data is configured into file shares and the shares are periodically synchronized transparently in the background, over the optimized connection of the Steelhead appliance. PFS leverages the integrated disk capacity of the Steelhead appliance to store file-based data in a format that allows it to be retrieved by NAS clients.

For detailed information about PFS, see the *Steelhead Appliance Deployment Guide*.

Syntax

[no] pfs enable

Parameters

None

Usage

In RiOS v3.x or higher, you do not need to install the RCU service on the server to synchronize shares. RCU functionality has been moved to the Steelhead appliance. When you upgrade from v2.x to v3.x, your existing shares will be running as v2.x shares.

PFS is not appropriate for all network environments. For example, in a collaborative work environment when there are many users reading, writing, and updating a common set of files and records, you should consider not enabling PFS. For detailed information about whether PFS is appropriate for your network environment, see the *Steelhead Appliance Deployment Guide*.

- Before you enable PFS, configure the Steelhead appliance to use NTP to synchronize the time. To use PFS, the Steelhead appliance and DC clocks must be synchronized.
- The PFS Steelhead appliance must run the same version of the Steelhead appliance software as the server side Steelhead appliance.
- PFS traffic to and from the Steelhead appliance travels through the Primary interface. PFS requires that the Primary interface is connected to the same switch as the LAN interface. For detailed information, see the *Steelhead Appliance Installation and Configuration Guide*.
- The PFS share and origin-server share names cannot contain Unicode characters.

Using PFS can reduce the overall connection capacity for optimized TCP connections, as memory and CPU resources are diverted to support the PFS operation.

If you set up a PFS share on a NetApp filer, the filer allows all users access regardless of the permissions set on the NetApp share. For example, if you set **No Access** for a user for a share, the NetApp filer does not translate it into the appropriate ACL entry on the folder. When a PFS share is created from this origin share, the user is allowed access to the share because there is not a deny entry present in the ACL.

The **no** command option disables PFS support.

Example

```
amnesiac (config) # pfs enable
amnesiac (config) # restart
```

Product

Steelhead appliance

Related Topics

“show pfs all-info shares”

pfs settings

Description

Configures settings for a PFS file share.

Syntax

pfs settings [admin-password <password>] [log-level <0-10>] | [conn-timeout <minutes>] [max-log-size <size in KB>] | [server-signing enabled | disabled | required]

Parameters

admin-password <password>	Specify the local administrator password.
log-level <0-10>	Specify the log level: **0-10**. The **no** command option resets the log level to the default.
conn-timeout <minutes>	Specify the number of minutes after which to time-out idle connections. If there is no read or write activity on a mapped PFS share on a client machine, then the TCP connection times out according to the value set and the client has to re-map the share. The **no** command option resets the time-out to the default.
max-log-size <size>	Specify the maximum log size in KB. The **no** command option resets the size to the default.
server signing {enabled | disabled | required}	Specify the SMB server signing mode: • **enabled** - Specify any type of security signature setting requested by the client machine. • **disabled** - Specify the default value. In this setting, PFS does not support clients with security signatures set to **required**. • **required** - Specify clients with security signatures set to **enabled** or **required**.

Usage

This command requires at least one option.

Example

```
amnesiac (config) # pfs settings server-signing enabled
```

Product

Steelhead appliance.

Related Topics

"show pfs all-info shares"

pfs share cancel-event

Description

Cancels PFS synchronization and verification.

Syntax

[no] pfs share cancel-event local-name <name>

Parameters

local-name <name>	Specify the local share name. A local share is the data volume exported from the origin server to the Steelhead appliance.

Example

```
amnesiac (config) # pfs share cancel-event local-name test
```

Product

Steelhead appliance.

Related Topics

"show pfs all-info shares"

pfs share configure

Description

Configures a PFS file share.

This command applies to v3.x or later shares. For information on version 2.x shares, see "pfs share configure (RiOS v2.0.x only)" on page 618.

You cannot run a mixed system of v2.x and v3.0 (or later) PFS shares.

Riverbed recommends that you upgrade your v2.x shares to v3.x (or higher) shares so that you do not have to run the RCU on a server.

For detailed information, see the *Steelhead Appliance Deployment Guide*.

Syntax

[no] pfs share configure local-name <local name> version 3 mode {broadcast | local | standalone} remote-path <remote path> server-account <login> server-password <password> interval <seconds> [full-interval <seconds>] [comment <"description">] [start-time <yyyy/mm/dd hh:mm:ss>] [full-start-time <yyyy/mm/dd hh:mm:ss>]

Parameters

local-name <local name>	Specify the local share name. A local share is the data volume exported from the origin server to the Steelhead appliance. The local share name cannot contain Unicode characters.
mode {broadcast | local | standalone}	Specify the mode of file sharing: **Broadcast -** Use Broadcast mode for environments seeking to broadcast a set of read-only files to many users at different sites. Broadcast mode quickly transmits a read-only copy of the files from the origin-file server to your remote offices. The PFS share on the Steelhead appliance contains read-only copies of files on the origin-file server. The PFS share is synchronized from the origin-file server according to parameters you specify. **Local -** Use Local mode for environments that need to efficiently and transparently copy data created at a remote site to a central data center, perhaps where tape archival resources are available to back up the data. Local mode enables read-write access at remote offices to update files on the origin file server. After the PFS share on the Steelhead appliance receives the initial copy from the origin server, the PFS share copy of the data becomes the master copy. New data generated by clients is synchronized from the Steelhead appliance copy to the origin server based on parameters you specify when you configure the share. The folder on the origin server essentially becomes a back-up folder of the share on the Steelhead appliance. If you use Local mode, users must not directly write to the corresponding folder on the origin server. **Caution:** In Local mode, the Steelhead appliance copy of the data is the master copy; do not make changes to the shared files from the origin server while in Local mode. Changes are propagated from the remote office hosting the share to the origin server. **Important:** Riverbed recommends that you do not use Windows file shortcuts if you use PFS. For detailed information, contact Riverbed Support at https:// support.riverbed.com. • **Stand-Alone -** Use Stand-Alone mode for network environments where it is more effective to maintain a separate copy of files that are accessed locally by the clients at the remote site. The PFS share also creates additional storage space. The PFS share on the Steelhead appliance is a one-time, working copy of data mapped from the origin server. You can specify a remote path to a directory on the origin server, creating a copy at the branch office. Users at the branch office can read from or write to stand-alone shares but there is no synchronization back to the origin server since a stand-alone share is an initial and one-time only synchronization. **Note:** When you configure a v3.x Local mode share or any v2.x share (except a Stand-Alone share in which you do not specify a remote path to a directory on the origin server), a text file (**._rbt_share_lock. txt**) that keeps track of which Steelhead appliance owns the share is created on the origin server. Do not remove this file. If you remove the**._rbt_share_lock. txt** file on the origin file server, PFS will not function properly (v3.x or higher). Broadcast and Stand-Alone shares do not create this text file.
remote-path <remote path>	Specify, using UNC format, the path to the data on the origin server that you want to make available to PFS.
server-account <login> **server-password <password>**	Specify the login and password to be used to access the shares folder on the origin file server. The login must be a member of the Administrators group on the origin server, either locally on the file server (the local Administrators group) or globally in the domain (the Domain Administrator group).
interval <seconds>	Specify the interval that you want incremental synchronization to occur. The first synchronization, or the initial copy, retrieves data from origin file server and copies it to the local disk on the Steelhead appliance. Subsequent synchronizations are based on the synchronization interval. In incremental synchronization, the system attempts to fetch modified data from the origin-file server, but some changes might not be propagated.

full-interval <seconds>	Specify the frequency of updates (full synchronization) in seconds. In full synchronization, a full directory comparison is performed and all changes since the last full synchronization are sent between the proxy file server and the origin file server. Use full synchronization if performance is not an issue.
start-time <yyyy/mm/dd hh:mm:ss>	Specify the date and time to start initial synchronization.
full-start-time <yyyy/ mm/dd hh:mm:ss>	Specify the start time for full synchronization.
[comment <"description">]	Optionally, specify a description for the share.

Usage

For v3.x (or higher) PFS shares, you do not need to install the RCU service on a Windows server.

Make sure the **server-account** you specify is a member of the Administrators group on the origin server, either locally on the file server (the local Administrators group) or globally in the domain (the Domain Administrator group).

Example

```
amnesiac (config) # pfs share configure local-name test version 2 mode local remote-path c:/data
server-name test port 81 interval 5 full-interval 5 start-interval 2006/06/06 02:02:02 comment
"test"
```

Product

Steelhead appliance.

Related Topics

"show pfs all-info shares"

pfs share configure (RiOS v2.0.x only)

Description

Configures a PFS file share for v2.x Steelhead appliance software.

You cannot run a mixed system of v2.x and v3.0 (or higher) PFS shares.

For information about configuring v3.x (or later) shares, see **"pfs share configure" on page 616**.

Syntax

[no] pfs share configure local-name <local name> version 2 mode {broadcast | local | standalone} server-name <name> port <port> remote-path <remote path> interval <seconds> [full-interval <seconds>] [comment <"description">] [start-time <yyyy/mm/dd hh:mm:ss>] [full-start-time <yyyy/mm/dd hh:mm:ss>]

Parameters

version 2	Specify to configure v2.x Steelhead appliance software.
local-name <local name>	Specify the local share name. A local share is the data volume exported from the origin server to the Steelhead appliance. The local share name cannot contain Unicode characters.
mode [broadcast | local | standalone]	Specify the mode of file sharing. For details, see "pfs share configure" on page 616.
server-name <name> port <port>	Specify the origin server and port located in the data center which hosts the origin data volumes (folders). The origin-server share name cannot contain Unicode characters.
remote-path <remote path>	Specify the remote path for the share folder on the origin file server. For v2.x, you must have the RCU service running on a Windows server (this can be the origin file server or a separate server). If the origin server is not the RCU server, you specify the remote path using the UNC format for the mapped drive. If the origin server is the same as the RCU server then you must type its full path including the drive letter, for example **C:\data**.
interval <seconds>	Specify the interval that you want incremental synchronization to occur. The first synchronization, or the initial copy, retrieves data from origin file server and copies it to the local disk on the Steelhead appliance. Subsequent synchronizations are based on the synchronization interval.
full-interval <seconds>	Specify the frequency of full synchronization updates in seconds. In full synchronization, a full directory comparison is performed and all changes since the last full synchronization are sent between the proxy file server and the origin file server. Use full synchronization if performance is not an issue.
start-time <yyyy/mm/dd hh:mm:ss>	Specify the date and time to commence initial synchronization.
full-start-time <yyyy/mm/dd hh:mm:ss>	Specify the start time for full synchronization.
[comment <"description">]	Optionally, specify an administrative description for the share.

Usage

Riverbed strongly recommends that you upgrade your shares to v3.x shares. If you upgrade any v2.x shares, you must upgrade all of them. After you have upgraded shares to v3.x, you should only create v3.x shares.

By default, when you configure PFS shares with Steelhead appliance software v3.x and higher, you create v3.x PFS shares. PFS shares configured with Steelhead appliance software v2.x are v2.x shares. Version 2.x shares are not upgraded when you upgrade Steelhead appliance software.

If you do not upgrade your v.2.x shares:

- You should not create v3.x shares.
- You must install and start the RCU on the origin server or on a separate Windows host with write-access to the data PFS uses. The account that starts the RCU must have write permissions to the folder on the origin file server that contains the data PFS uses. You can download the RCU from the Riverbed Support site at https://support.riverbed.com. For detailed information, see the *Riverbed Copy Utility Reference Manual*.
- Make sure the account that starts the RCU has permissions to the folder on the origin file server and is a member of the Administrators group on the remote share server, either locally on the file server (the local Administrators group) or globally in the domain (the Domain Administrator group).
- In Steelhead appliance software version 3.x and higher, you do not need to install the RCU service on the server for synchronization purposes. All RCU functionality has been moved to the Steelhead appliance.
- You must configure domain, not workgroup, settings, using the "domain rejoin" command. Domain mode supports v2.x PFS shares but Local Workgroup mode is supported only in v3.x (or higher).

Example

```
amnesiac (config) # pfs share configure local-name test version 2 mode local remote-path c:/data
server-name test port 81 interval 5 full-interval 5 start-time 2006/06/06 02:02:02 comment "test"
```

Product

Steelhead appliance.

Related Topics

"show pfs all-info shares"

pfs share dry-run

Description

Enables a dry run of a share synchronization.

Syntax

[no] pfs share dry-run share-name <remote-path>

Parameters

share-name <remote-path>	Specify the remote path of the share. Use the format `'\\server\share'`.

Usage

The **pfs share dry-run** command allows an administrator to view details about share synchronization and the amount of data expected to be transferred. No actual data is transferred.

Example

```
amnesiac (config) # pfs share dry-run share-name '\\10.11.61.66\backup'
```

Product

Steelhead appliance

Related Topics

"show pfs all-info shares"

pfs share local-name

Description

Removes a local share.

Syntax

no pfs share local-name <local-name> [force {<true | false>}]

Parameters

local-name <local name>	Specify the local share name to be removed.
force <true | false>	Specify **true** to enable forced removal of PFS share. Specify **false** to disable forced removal of PFS share. The default value is false.

Usage

You can execute this command only with the preceding *no*.

Example

```
amnesiac (config) # no pfs share local-name test force true
```

Product

Steelhead appliance

Related Topics

"show pfs all-info shares"

pfs share manual-sync

Description

Performs a manual synchronization of a PFS share.

Syntax

pfs share manual-sync local-name <local name>

Parameters

local-name <local name>	Specify the local share name. A local share is the data volume exported from the origin server to the Steelhead appliance.

Example

```
amnesiac (config) # pfs share manual-sync local-name test
```

Product

Steelhead appliance

Related Topics

"show pfs all-info shares"

pfs share modify

Description

Modifies properties of a PFS file share.

You cannot run a mixed system of v2.x and v3.0 (or higher) PFS shares.

Syntax

[no] pfs share modify local-name <local name> [acl-group-ctrl {true | false}] [acl-inherit {true | false}] [syncing {true | false}] | [sharing {true | false}] [port <port>] [mode broadcast | local | standalone <cr>] [remote-path <remote path>] [server-name <name>] [server-account <login>] [server-password <password>] [port <port>] [interval <seconds>] [full-interval <seconds>] [full-start-time <yyyy/mm/dd hh:mm:ss>] [start-time <yyyy/mm/dd hh:mm:ss>] comment <"description">]

Parameters

local-name <local name>	Specify the local share name. A local share is the data volume exported from the origin server to the Steelhead appliance. The local share name cannot contain Unicode characters.
acl-group-ctrl {true | false}	Specify **true** if you want accounts in the primary owner's group to be able to assign permissions. Specify **false** if you want only the primary owner or local administrator to be able to assign permissions. The default value is false.
acl-inherit {true | false}	Specify **true** if you want shared folders to inherit permissions from parents. Specify **false** if you do not want to retain inherited permissions. The default value is false.
syncing {true | false}	Specify **true** to enable synchronization. Specify **false** to disable synchronization. The default value is false.
sharing {true | false}	Specify **true** to enable sharing. Specify **false** to disable sharing. The default value is false.
port <port>	Specify the share port.
mode broadcast | local | standalone <cr>	Specify the mode of file sharing. For details, see "pfs share configure" on page 616.
remote-path <remote path>	For version 3.x (or higher) shares, specify the remote path using UNC format to specify the server name and remote path. For version 2.x shares, specify the remote path for the share folder on the origin file server. For version 2.x shares, you must have the RCU service running on a Windows server (this can be the origin file server or a separate server). If the origin server is not the RCU server, you specify the remote path using the UNC format for the mapped drive. If the origin server is the same as the RCU server then you must type its full path including the drive letter, for example C:\data.
server-name <name> port <port>	*Version 2.x shares only*. Specify the origin server and port located in the data center which hosts the origin data volumes (folders). The origin-server share name cannot contain Unicode characters.
server-account <login> **server-password <password>**	*Version 3.x or higher shares only*. Specify the login to be used to access the shares folder on the origin file server. The login must be a member of the Administrators group on the origin server, either locally on the file server (the local Administrators group) or globally in the domain (the Domain Administrator group).
interval <seconds>	Specify the interval that you want incremental synchronization updates to occur. The first synchronization, or the initial copy, retrieves data from origin file server and copies it to the local disk on the Steelhead appliance. Subsequent synchronizations are based on the synchronization interval.
full-interval <seconds>	Specify the frequency of full synchronization updates, in seconds. Use full synchronization if performance is not an issue.
full-start-time <yyyy/mm/dd hh:mm:ss>	Specify the start time for full synchronization.

start-time <yyyy/mm/dd hh:mm:ss>	Specify the date and time to commence initial synchronization.
[comment <"description">]	Optionally, specify an administrative description for the share.

Usage

You must specify at least one option.

You cannot run a mixed system of v2.x and v3.0 (or higher) PFS shares; Riverbed strongly recommends you upgrade your v2.x shares to 3.x or higher shares.

Example

```
amnesiac (config) # pfs share modify local-name test remote-path /tmp server-name mytest mode
broadcast frequency 10
```

Product

Steelhead appliance

Related Topics

"show pfs all-info shares"

pfs share upgrade

Description

Upgrades PFS shares from v2.x to v3.x software.

Syntax

pfs share upgrade local-name <local name> remote-path <remote path> server-account <login> server-password <server password>

Parameters

local-name <local name>	Specify the local share name. A local share is the data volume exported from the origin server to the Steelhead appliance.
remote-path <remote path>	Specify the remote path to the share.
server-account <server login>	Specify the server login.
server-password <server login>	Specify the server password.

Usage

Riverbed strongly recommends that you upgrade your shares to v3.x shares. If you upgrade any v2.x shares, you must upgrade all of them. After you have upgraded shares to v3.x, you should only create v3.x shares.

By default, when you configure PFS shares with Steelhead appliance software v3.x and higher, you create v3.x PFS shares. PFS shares configured with Steelhead appliance software v2.x are v2.x shares. Version 2.x shares are not upgraded when you upgrade Steelhead appliance software.

If you do not upgrade your v.2.x shares:

- Do not create v3.x shares.
- You must install and start the RCU on the origin server or on a separate Windows host with write-access to the data PFS uses. The account that starts the RCU must have write permissions to the folder on the origin file server that contains the data PFS uses. You can download the RCU from the Riverbed Support site at https://support.riverbed.com. For detailed information, see the *Riverbed Copy Utility Reference Manual*.

- Make sure the account that starts the RCU has permissions to the folder on the origin file server and is a member of the Administrators group on the remote share server, either locally on the file server (the local Administrators group) or globally in the domain (the Domain Administrator group).
- In Steelhead appliance software version 3.x and higher, you do not need to install the RCU service on the server for synchronization purposes. All RCU functionality has been moved to the Steelhead appliance.
- You must configure domain, not workgroup, settings, using the "domain rejoin" command. Domain mode supports v2.x PFS shares but Local Workgroup mode is supported only in v3.x (or higher).

Example

```
amnesiac (config) # pfs share upgrade myshare remote-path \\remoteshare server-account mylogin
server-password mypassword
```

Product

Steelhead appliance.

Related Topics

"show pfs all-info shares"

pfs share verify

Description

Verifies a PFS share.

Syntax

pfs share verify local-name <local name>

Parameters

local-name <local name>	Specify the local share name. A local share is the data volume exported from the origin server to the Steelhead appliance.

Example

```
amnesiac (config) # pfs share verify local-name test
```

Product

Steelhead appliance

Related Topics

"show pfs all-info shares"

pfs start

Description

Starts the PFS service.

Syntax

[no] pfs start

Parameters

None

Example

```
amnesiac (config) # pfs start
```

Product

Steelhead appliance

Related Topics

"show pfs all-info shares", "pfs share configure"

DNS Cache Commands

This section describes the DNS cache commands.

dns cache clear

Description

Clear contents of DNS cache.

Syntax

dns cache clear

Parameters

None

Example

```
amnesiac (config) # dns cache clear
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns cache freeze enable

Description

Sets whether DNS cache entries should expire.

Syntax

[no] dns cache freeze enable

Parameters

None

Usage

The **no** command option disables cache entries expiration.

Example

```
amnesiac (config) # dns cache freeze enable
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns cache frozen-min-ttl

Description

Sets the minimum time-to-live value on an expired entry in a frozen cache. The minimum time-to-live value applies to all entries when the cache is frozen, whether they are expired or not.

Syntax

[no] dns cache frozen-min-ttl <seconds>

Parameters

<seconds>	Specify the smallest time-to-live in seconds that a response from the server can have. This setting affects the contents of the response, not how long the entry is actually cached (which is forever), and this is not specific to negative responses. The range is 0-604800. The default value is 10.

Usage

The **no** command option resets the frozen minimum time-to-live value to the default.

Example

```
amnesiac (config) # dns cache frozen-min-ttl 604800
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns cache fwd enable

Description

Enables or disables caching of DNS entries.

Syntax

[no] dns cache fwd enable

Parameters

None

Usage

The **no** command option disables forwarding of name servers.

Example

```
amnesiac (config) # dns cache fwd enable
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns cache max-ncache-ttl

Description

Sets maximum time a negative response can be cached.

Syntax

[no] dns cache max-ncache-ttl <seconds>

Parameters

<seconds>	Specify the number of seconds a negative response caches. The range is 2-2592000. The default value is 10800.

Usage

The **no** command option resets the value to the default.

Example

```
amnesiac (config) # dns cache max-ncache-ttl 12
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns cache max-ttl

Description

Sets the maximum time a response can be cached.

Syntax

[no] dns cache max-ttl <seconds>

Parameters

<seconds>	Specify the number of seconds a response caches. The range is 2-2592000. The default value is 604800.

Usage

The **no** command option resets the value to the default.

Example

```
amnesiac (config) # dns cache max-ttl 12
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns cache min-ncache-ttl

Description

Sets minimum time that a negative response can be cached.

Syntax

[no] dns cache min-ncache-ttl <seconds>

Parameters

<seconds>	Specify the number of seconds a negative response to be cached. The range is 0-2592000 (30 days). The default value is 0.

Usage

The **no** command option resets the value to the default.

Example

```
amnesiac (config) # dns cache min-ncache-ttl 2
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns cache min-ttl

Description

Sets the minimum time that a response can be cached.

Syntax

[no] dns cache min-ttl <seconds>

Parameters

<seconds>	Specify the minimum number of seconds that a response can be cached. The default value is 0.

Usage

The **no** command option resets the value to the default.

Example

```
amnesiac (config) # dns cache min-ttl 2
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns cache size

Description

Sets size of DNS cache in bytes.

Syntax

[no] dns cache size <bytes>

Parameters

<bytes>	Specify the size of the DNS cache in bytes. The range is 524288 through 2097152.

Usage

The **no** command option resets the value to the default.

Example

```
amnesiac (config) # dns cache size 2097152
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns enable

Description

Enables a DNS server. Forwards name resolution requests to a DNS name server, then stores the address information locally in the Steelhead appliance. By default, the requests go to the root name servers, unless you specify another name server.

Syntax

[no] dns enable

Parameters

None

Usage

A DNS name server resolves hostnames to IP addresses and stores them locally in a single Steelhead appliance. Any time your browser requests a URL, it first looks in the local cache to see if it is there before querying the external name server. If it finds the resolved URL locally, it uses that IP. Hosting the DNS name server function provides:

- Improved performance for Web applications by saving the round trips previously needed to resolve names. Whenever the name server receives address information for another host or domain, it stores that information for a specified period of time. That way, if it receives another name resolution request for that host or domain, the name server has the address information ready, and does not need to send another request across the WAN.
- Improved performance for services by saving round trips previously required for updates.
- Continuous DNS service locally when the WAN is disconnected, with no local administration needed, eliminating the need for DNS servers at branch offices.

The **no** command option disables a DNS server.

Example

```
amnesiac (config) # dns enable
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns forwarder

Description

Adds a new DNS forwarding name server. Optionally sets, moves, or removes an integer index position for each name server.

Syntax

dns forwarder add <ip-addr> [idx <index>] | move <index> to <index> | remove <integer> to <integer>

Parameters

add <ip-addr> [idx <index>]	Specify the IP address of the forwarder. A forwarder is a DNS server to which the Steelhead appliance caching-name server will forward requests. Forwarder is added to the end of the index of forwarders by default. Optionally, use **idx** to specify the order in which the Steelhead appliance contacts forwarder by assigning the forwarder a numeric position in the forwarder index. The Steelhead appliance first sends a request to the forwarder with index **0**, next to the forwarder with index **1**, and so on, to an upper index limit of 2147483647.
move <index> to <index>	Specify the index number of the forwarder. Moves a forwarder from one index position to another.
remove <index>	Specify the index number of the forwarder. Removes a forwarder from the index.

Usage

You can also access this command from enable mode.

Example

```
amnesiac (config) # dns forwarder add 10.0.0.1 idx 2
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings,""show stats dns"

dns forwarder enable

Description

Sets the ID of the forwarder IP address to enable.

Syntax

[no] dns forwarder enable <integer>

Parameters

<integer>	Specify the ID in the form of an integer. The integer indicates the positions on the list.

Usage

The **no** command option disables use of the forwarder with the specified index.

Example

```
amnesiac (config) # dns forwarder enable 2
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns fwd-fail-count

Description

Sets the number of consecutive dropped requests until a forwarder is considered down.

Syntax

[no] dns fwd-fail-count <requests>

Parameters

<requests>	Specify the number of dropped requests before a forwarder is considered down. When both the specified number of requests to the forwarder have been dropped and all requests have been dropped for the amount of time specified by **dns fwd-fail-time**, a forwarder is considered down.

Usage

The **no** command option resets the value to the default.

Example

```
amnesiac (config) # dns fwd-fail-count 12
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns fwd-fail-dtxn enable

Description

Detects unresponsive forwarders and requests responses from them only after trying responsive forwarders.

Syntax

[no] dns fwd-fail-dtxn enable

Parameters

None

Usage

The **no** command option resets the value to the default.

Example

```
amnesiac (config) # dns fwd-fail-dtxn enable
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns fwd-fail-time

Description

Sets the number of consecutive seconds of no response from a forwarder until it is considered down.

Syntax

[no] dns fwd-fail-time <seconds>

Parameters

<seconds>	Specify the number of seconds for non-response from a forwarder.

Usage

The **no** command option resets the value to the default.

Example

```
amnesiac (config) # dns fwd-fail-time 12
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns fwd-tm-staydown

Description

Sets the number of seconds that a forwarder is considered down before it is considered up again.

Syntax

[no] dns fwd-tm-staydown <seconds>

Parameters

<seconds>	Specify the number of seconds of down time for the forwarder.

Usage

The **no** command option resets the value to the default.

Example

```
amnesiac (config) # dns fwd-tm-staydown 12
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns interface

Description

Sets the interfaces on which DNS is enabled.

Syntax

dns interface {add <interface> | remove <interface>}

Parameters

add <interface>	Specify the name of the interface.
remove <interface>	Specify the name of the interface.

Example

```
amnesiac (config) # dns interface add aux
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns root-fallback enable

Description

Sets the use of root name servers.

Syntax

[no] dns root-fallback enable

Parameters

None

Usage

The **no** command option disables the use of root of name servers.

Example

```
amnesiac (config) # dns root-fallback enable
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns round-robin enable

Description

Configures the DNS service round-robin setting.

Syntax

[no] dns round-robin enable

Parameters

None

Usage

The **no** command option disables the use of the round-robin feature.

Example

```
amnesiac (config) # dns round-robin enable
```

Product

Steelhead appliance

Related Topics

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

RSP Commands

This section describes the Riverbed Services Platform(RSP) commands. To run RSP packages you must first install the RSP image, then install the RSP package, and finally, configure dataflow rules.

Note: RSP is supported on Steelhead appliance models 250, 550, 1050, 2050, 5050, 6050, and 7050.

Note: RiOS v7.0 and later does not run on the *xx*20 models.

Note: RSP is not supported on Steelhead appliance CX *xx*55 models.

For detailed information about installing and configuring RSP, see the *RSP User's Guide*.

legacy-rsp destroy

Description

Deletes existing v5.0.x RSP data.

Syntax

legacy-rsp destroy

Parameters

None

Example

```
amnesiac (config) # legacy-rsp destroy
```

Product

Steelhead appliance, Steelhead EX appliance

Related Topics

"show rsp backups"

rsp backup delete

Description

Deletes the RSP backup file from the Steelhead appliance.

Syntax

rsp backup delete <backup filename>

Parameters

<backup filename>	Specify the backup name: **<Steelhead appliance name>-<slotname>-<date>.bkup**

Example

```
amnesiac (config) # rsp backup delete gen-sh1-1-20090908-223616.bkup
```

Product

Steelhead appliance

Related Topics

"show rsp backups"

rsp backup fetch

Description

Downloads the RSP backup file.

Syntax

rsp backup fetch <backup URL> [as <backup-filename>]

Parameters

<backup URL>	Specify the backup file URL or name. You can use HTTP, FTP, or SCP to transfer the backup file. For example: `scp://username:password@host/path`
[as <backup-filename>]	Optionally, specify a different filename for the backup file that you download.

Example

```
amnesiac (config) # rsp backup fetch scp://admin:password@gen-sh2/var/tmp/rsp_backups/amnesiac-
20090908-223616.bkup
```

Product

Steelhead appliance

Related Topics

"show rsp backups," "show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp backup upload

Description

Uploads the RSP backup file onto a remote server or another Steelhead appliance.

Syntax

rsp backup upload <backup filename> remote <backup URL>

Parameters

<backup filename>	Specify the backup filename: **<Steelhead appliance name>-<slotname>-<date>.bkup.**
<backup URL>	Specify the backup file URL or path name. You can use FTP, or SCP to transfer the backup file.

Example

```
amnesiac (config) # rsp backup upload amnesiac-1-20090908-223616.bkup remote scp://
admin:mypassword@amnesiac-sh2/var/tmp/rsp_backups/
```

Product

Steelhead appliance

Related Topics

"show rsp backups," "show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp clone all

Description

Clones all slots to a remote Steelhead appliance.

Syntax

rsp clone all [hostname <remote-steelhead>] [password <password>]

Parameters

hostname <remote-steelhead>	Specify the hostname or IP address of the remote Steelhead appliance to which all slots are to be cloned.
password <password>	Specify the RSP clone password for the remote Steelhead appliance to which all slots are to be cloned. **Note:** The password value is set by the "rsp clone password" command.

Example

```
amnesiac (config) # rsp clone all hostname branch003 password rsppw003
```

Product

Steelhead appliance

Related Topics

"rsp clone password," "show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp clone cancel

Description

Cancels the specified clone operation.

Syntax

rsp clone cancel <clone id>

Parameters

<clone-id>	Specify the clone ID for the clone to be cancelled.

Usage

When an RSP clone is created, a clone ID is generated.

Example

```
amnesiac (config) # rsp clone cancel 1243
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp clone password

Description

Sets the password that remote Steelhead appliances need to clone RSP virtual machines to the current Steelhead appliance.

Syntax

[no] rsp clone password <password>

Parameters

<password>	Specify the password that other Steelhead appliances require to clone RSP virtual machines to the current appliance.

Usage

The **no** command clears the password and prevents HA on this Steelhead appliance.

Example

```
amnesiac (config) # rsp clone password rsppw003
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp clone slots

Description

Clones the specified slots to the specified remote Steelhead appliance.

Syntax

rsp clone slots <slot-names> hostname <remote-steelhead> password <password>

Parameters

<slot-names>	Specify the slots to be cloned as a comma-separated list (that is, **1,2,3**).
hostname <remote-steelhead>	Specify the hostname or IP address of the remote Steelhead appliance to which the specified slots are to be cloned.
password <password>	Specify the RSP clone password for the remote Steelhead appliance to which the specified slots are to be cloned. **Note:** The password value is set by the "rsp clone password" command.

Example

```
amnesiac (config) # rsp clone slots 1,2,3,4 hostname branch003 password rsppw003
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp clone test

Description

Tests the connection to the specified clone.

Syntax

rsp clone test hostname <remote-steelhead> password <password>

Parameters

hostname <remote-steelhead>	Specify the hostname or IP address of the remote Steelhead appliance.
password <password>	Specify the rsp clone password for the remote Steelhead appliance. **Note:** The password value is set by the "rsp clone password" command.

Example

```
amnesiac (config) # rsp clone test hostname gen-sh1 password rsppw003
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp dataflow

Description

Configures RSP data flow.

Syntax

[no] rsp dataflow <dataflow name> {add opt-vni <vni name> vni-num <vni-number> | move vni-num <vni-number> to <vni-number>}

Parameters

<dataflow name>	Specify the dataflow name. For example: **inpath0_0** For example, inpath0_0 represents and controls the flow of data through the lan0_0, inpath0_0, and wan0_0 interfaces.
add	Adds an optimization VNI to the dataflow.
opt-vni <vni name>	Specify the Virtual Network Interface (VNI) name. The optimization VNI name is a combination of the slot name and the VNI name. For example: **1:lan0** VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
vni-number <vni-number>	Specify the order number of the VNI in the rule list. The order number in the rule list determines which VNI a packet goes to first, second, third, fourth, and last.: • **1-n -** Specifies the order number of the VNI in the rule list. Lower numbers locate the VNI closer to the LAN. Higher numbers locate the VNI closer to the WAN. • **start** - Locates the VNI next to the LAN. A packet coming from the Steelhead appliance LAN interface goes to this VNI first. • **end** - Locates the VNI next to the WAN. A packet coming from the Steelhead appliance WAN interface goes to this VNI first.
move <vni-number> to <vni-number>	Specify VNI numbers to move a VNI in the dataflow.

Usage

Each RSP package uses its own RSP network interfaces, equivalent to VMware network interfaces, to communicate with the outside world. These network interfaces are matched up with the physical intercept points that create VNIs. VNIs are network taps that enable data to flow in and out of the RSP slots. VNIs are available on the LAN, WAN, primary, and auxiliary interfaces of the Steelhead appliance.

For detailed information about configuring RSP, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Each package is capable of having ten RSP network interfaces which means it can support ten VNIs. The VNIs provide a great deal of configuration flexibility, providing the basis of how packages are chained together and how data flows through the various slots in a multiple VM scenario. VNIs fall into two categories:

Optimization VNIs

Optimization VNIs are used with in-band packages. Optimization VNIs are part of the optimized data flow on either the LAN- or WAN-side of RiOS. There are several types of optimization VNIs:

- **In-path** - In-path VNIs are used for packages such as security packages. The following types of in-path optimization VNIs are available:
  - **LAN** - LAN VNIs forward packets from the LAN-side to the virtual machine, to the WAN-side, or both. LAN VNIs unconditionally forward packets from the virtual machine to the LAN-side for RSP. LAN VNIs cannot receive packets from the WAN-side. For VRSP, packets from LAN or WAN VNIs can go in either direction, depending on the subnet-side rules.
  - **WAN** - WAN VNIs forward packets from the WAN-side to the virtual machine, to the LAN-side, or both. WAN VNIs unconditionally forward packets from the virtual machine to the WAN-side. WAN VNIs cannot receive packets from the LAN-side.
- **Virtual In-Path**: These optimization VNIs belong to in-band packages that need some form of redirection to intercept traffic. The types of virtual in-path VNIs are:
  - **DNAT** - Use with proxy-based solutions; for example, video proxies.
  - **Mirror** - Use with network monitoring-based solutions; acts like a SPAN port to copy traffic for monitoring.

For details about adding optimization VNI rules, see “rsp opt-vni vlan” on page 653.

Management VNIs

Management VNIs reside on the Steelhead appliance primary or auxiliary port. Management VNIs are used as a management interface for in-band packages. Management VNIs are the primary communication path for out-of-band packages.

For details about adding optimization VNI rules, see “rsp opt-vni def-ip-pol” on page 645.

The **no** command option disables dataflow on the specified VNI.

Example

```
amnesiac (config) # rsp dataflow inpath0_0 add opt-vni 1:testVNI vni-num 1
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp enable

Description

Enables the RSP service.

Syntax

[no] rsp enable

Parameters

None

Usage

In RiOS v5.5 or later, the Riverbed Services Platform (RSP), offers branch-office-in-a-box services.

Riverbed recommends you install and configure RSP using the Management Console. For detailed information, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

RSP is supported on models 250, 520, 550, 1020, 1050, 1520, 2020, 2050, 3020, 3520, 5050, 6050, and 7050.

RSP in RiOS v5.5.x or later uses VMware Server 2.0 as the virtualization platform. Both 32 and 64-bit versions of the RSP image are available. VM Server does not need a separate license.

After installing the RSP installation image, you can add packages to run additional services and applications. RSP includes configuration options that enable you to determine the data flow to and from a VM, and the ability to chain VM together.

After installing the RSP image, you can install the RSP packages that run additional services and applications. RSP packages are available as a separate release from a third-party vendor or from Riverbed. For example, you can run out-of-band packages such as Internet Protocol Address Management (IPAM) and in-band packages such as security solutions that provide firewall, VPN, and content filtering. You can also run proxy solutions such as video streaming packages. You can run up to five packages simultaneously, depending on the package and the Steelhead appliance model.

The configuration options include rules to determine the data flow to and from a package, and the ability to chain packages together.

Important: For detailed information about installing and configuring RSP, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Basic Steps

- Download and install the RSP image, which installs the VM server on the Steelhead appliance. The Steelhead appliance RiOS image does not include the RSP image. You must install the RSP image separately.
- RSP is pre-installed on newly manufactured Steelhead appliances if you ordered RSP.To download the image, go to the Riverbed Support site at https://support.riverbed.com.
- Start RSP on the Steelhead appliance.
- Obtain an RSP package by using an existing package from Riverbed, a third-party vendor, or from within your organization or create your own package. For detailed information about creating your own package, see the Riverbed Partner Website.
- Install the package in a slot.
- Enable the slot.
- View slot status.

- Configure the package. For example, to install a Windows package you would need to configure an IP address for the interface.
- Disable the slot as a safety precaution while you configure the traffic data flow. This step is not required for out-of-band packages.
- Configure data flow. This step is not required for out-of-band packages.
- Add data flow rules to the VNI. This step is not required if you use the default rules for the package.
- Optionally, configure RSP watchdog.
- Optionally, modify the memory footprint.
- Enable the slot.
- Open the VMware Console.

The **no** command option disables RSP.

Example

```
amnesiac (config) # rsp enable
amnesiac (config) # show rsp
  Supported:   Yes
  Installed:   Yes
  Release:     6.0.0
  Enabled:     Yes
  State:       Running
  Disk Space:  11.26 GB used / 195.44 GB free / 206.70 GB total
  Memory:      0 MB used / 128 MB free / 128 MB total
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp image delete

Description

Deletes an RSP installation image from disk.

Syntax

rsp image delete <RSP image>

Parameters

<RSP image>	Specify the RSP image to delete.

Usage

This command does not uninstall RSP. It simply removes one of the previous downloaded RSP installation images from the disk, thus freeing space on the disk.

Example

```
amnesiac (config) # rsp image delete rsp-image.img
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp image fetch

Description

Downloads an RSP installation image from a URL.

Syntax

rsp image fetch [http | ftp | scp] <URL>

Parameters

http <URL>	Uses the HTTP protocol to fetch the RSP installation image. For example, `http://server-hostname/path-to-rsp-image/rsp-image.img`
ftp <URL>	Uses the FTP protocol to fetch the RSP installation image. For example, `ftp://username:password@server-hostname/path-to-rsp-image/rsp-image.img`
scp <URL>	Uses the SCP protocol to fetch the RSP installation image. For example, `scp://username:password@server-hostname/path-to-rsp-image/rsp-image.img`

Example

```
amnesiac (config) # rsp image fetch http://server-hostname/path-to-rsp-image/rsp-image.img
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp image install

Description

Installs an RSP installation image.

Syntax

rsp image install

Parameters

<rsp image>	Specify the image name.

Usage

RSP requires at least 2 GB of additional memory on the Steelhead appliance.

You must have role-based permission for RSP to install RSP. For information on permissions, see the *Riverbed Services Platform Installation Guide*.

Before installing a new RSP image, you must stop the RSP service currently running on the Steelhead appliance.

If you have previously installed RSP for RiOS v5.0.x, you must reinstall the RSP image for RiOS v5.5 and later. RSP for RiOS v5.0.x is not compatible with RSP for RiOS v5.5 or later.

Installing a new RSP image replaces the previously installed image (the RSP packages and all slots).

For details on Steelhead appliance RSP support for guest operating systems, see the product specification sheets at: http://www.riverbed.com/products/appliances/

Example

```
amnesiac (config) # rsp image fetch http://server-hostname/path-to-rsp-image/rsp-image.img
amnesiac (config) # rsp image install rsp-image.img
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp image move

Description

Renames or moves an RSP installation image on the disk.

Syntax

rsp image move <old filename> to <new filename>

Parameters

<old filename>	Specify the source RSP image that you want to change.
<new filename>	Specify the new RSP image name.

Example

```
amnesiac (config) # rsp image move examp1-rsp-image.img to newexamp1-rsp-image.img
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp job

Description

Schedules an RSP clone job to the specified remote Steelhead appliance at the specified date and time. Optionally, you can set the job to recur at a specified interval.

Syntax

rsp job {[time <time>] [date <date>] [interval <duration>] [clone {all | slots <slot-names>}] [hostname <hostname>] [password <password>]}

Parameters

time <time>	Specify the time for the RSP job. Use the following format: HH:MM:SS.
date <date>	Specify the date for the RSP job. Use the following format: YYYY/MM/DD
interval <duration>	Optionally, specify the interval of job recurrence in days, hours, minutes, and seconds, as necessary. Use the following format: <D>d <H>h <M>m <S>s For example: `interval 2d6h6m6s`
clone {slots <slot-names> | all}	Indicates whether all (**clone all**) or only specified slots (**clone slots 1,3,4**) are to be cloned in the job.
hostname <remote-steelhead>	Specify the hostname or IP address of the remote Steelhead appliance to which the specified slots are to be cloned.
password <password>	Specify the RSP clone password for the remote Steelhead appliance to which the specified slots are to be cloned. The password value is set by the "rsp clone password" command.

Example

```
amnesiac (config) # rsp job time 09:00:00 date 2010/06/21 clone all hostname coloSH003 password
sh003123
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show rsp," "show rsp clones," "show rsp clones status," "show rsp slots"

rsp mgmt-vni

Description

Bridges a management Virtual Network Interface (VNI) to either the auxiliary or primary interface.

Syntax

rsp mgmt-vni <mgmt-vni> interface [aux | primary]

Parameters

<mgmt-vni>	Specify the management VNI. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: **wowzaSlot:Rsp0In**, **1:LanRSPInf** VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
interface [aux | primary]	Specify the physical interface to bind to: **aux** or **primary**.

Usage

Management VNIs reside on the Steelhead appliance primary or auxiliary port. Management VNIs are used as a management interface for in-band packages. Management VNIs are the primary communication path for out-of-band packages.

You bridge a management VNI to either the primary or auxiliary interface to connect the management VNI to the respective physical Ethernet adapter on the Steelhead appliance. The management VNI becomes part of the network connected to the physical primary or auxiliary port of the Steelhead appliance.

For detailed information, see the *RSP User's Guide*.

Example

```
amnesiac (config) # rsp mgmt-vni 1:testmgmtF interface aux
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp opt-vni def-ip-pol

Description

Sets the default policy for IP traffic.

Syntax

rsp opt-vni <opt-vni> def-ip-pol <def-ip-pol>

Parameters

<opt-vni>	Specify the optimization VNI. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: **wowzaSlot:Rsp0In**, **1:LanRSPInf** VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
def-ip-pol <def-ip-pol>	Specify one of the following policies: • **l2-swtich** - Enables L2 swtiching. • **redirect** - Redirects the packet to a VM. • **pass** - Passes traffic along the dataflow, bypassing the VM • **copy** - Copy the packet to the VM and also pass it along the data flow.

Usage

For detailed information, see the see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Example

```
amnesiac (config) # rsp opt-vni 1:testVNI def-ip-pol redirect
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp opt-vni def-non-ip-pol

Description

Sets the default policy for non-IP traffic.

Syntax

rsp opt-vni <opt-vni> def-non-ip-pol <def-ip-pol>

Parameters

<opt-vni>	Specify the management VNI. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: **wowzaSlot:Rsp0In**, **1:LanRSPInf** VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
<def-ip-pol>	Specify one of the following policies: • **l2-swtich** - Enables L2 swtiching. • **redirect** - Redirects the packet to a VM. • **pass** - Passes traffic along the data flow, bypassing the VM • **copy** - Copy the packet to the VM and also pass it along the data flow.

Usage

For detailed information, see the see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Example

```
amnesiac (config) # rsp opt-vni 1:testVNI def-non-ip-pol redirect
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp opt-vni dnat def-target-ip

Description

Configures the default DNAT target IP address.

Syntax

rsp opt-vni <opt-vni> dnat def-target-ip <ip-addr>

Parameters

<opt-vni>	Specify the management VNI. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: **wowzaSlot:Rsp0In**, **1:LanRSPInf** VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
<ip-addr>	Specify the destination NAT IP address.

Usage

For detailed information, see the see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Example

```
amnesiac (config) # rsp opt-vni 1:testVNI dnat def-target-ip 10.0.0.1
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp opt-vni dnat enable

Description

Enables Destination Network Address Translation (DNAT).

Syntax

rsp opt-vni <opt-vni> dnat enable

Parameters

<opt-vni>	Specify the management VNI. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: **wowzaSlot:Rsp0In**, **1:LanRSPInf** VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.

Usage

DNAT VNIs are used for proxy-based solutions, such as video proxies.

By default, DNAT is disabled. When DNAT is enabled, it translates the network address of packets that match the source and destination IP and the port (or port range) to the target IP and, optionally, the target port. It then routes them to the correct device, host, or network.

For example, you can install an RSP package for live video streaming and add a DNAT rule (using the IP address, port number, or both) that transparently proxies all traffic redirected to the local RSP video instance.

Consequently, the local RSP video instance responds to the local clients on behalf of the original server, simultaneously communicating with the original server in the background over the WAN. This process streamlines the number of requests over the WAN, resulting in time and bandwidth savings.

For detailed information, see the see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Example

```
amnesiac (config) # rsp opt-vni 1:testVNI dnat enable
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp opt-vni rule dnat

Description

Configures optimization VNI data flow rules. This type of VNI rule is used with in-band packages and is part of the optimized data flow either on the LAN or WAN side of RiOS. Riverbed recommends you use the Management Console to configure VNI data flow rules.

Syntax

rsp opt-vni <VNI name> rule dnat [targetip <ip-addr>| targetport <port>] <cr> | [srcaddr <srcaddr> srcport <srcport>] | [dstaddr <dstaddr> dstport <dstport>] |[protocol {all | tcp | udp | <protocol-num>}] | [rulenum <rulenum>]

Parameter

<VNI name>	Specify the VNI name. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: **wowzaSlot:Rsp0In**
targetip <ip-addr> | targetport <port>	Specify a single target IP address. Specify the target port of the packet, either a single port value or a port range of **port1-port2**. **port1** must be less than **port2**.
srcaddr <srcaddr> srcport <srcport>	Optionally, specify the source subnet and port of the packet. For example, **1.2.3.0/24**, or leave blank to specify all. Specify the source port of the packet, either a single port value or a port range of **port1-port2**. **port1** must be less than **port2**.
dstaddr <dstaddr> dstport <dstport>	Optionally, specify the destination network. Specify the port can be either a single port value or a port range of **port1-port2**. **port1** must be less than **port2**.
protocol {all | tcp | udp| <protocol-number>]}	Optionally, specify **all**, **tcp**, **udp**, or a protocol number (**1-254**) from the drop-down list. The default setting is **all**.
rulenum <rulenum>	Optionally, specify a number (**0 - 65535)** to replace the default rule number.

Usage

Destination Network Address Translation (DNAT) rules are used for in-path proxy-based solutions. You can only add DNAT rules for virtual in-path optimization VNIs.

By default, DNAT is disabled. When DNAT is enabled, it translates the network address of packets that match the source and destination IP and the port (or port range) to the target IP and, optionally, the target port. It then routes them to the correct device, host, or network.

For example, you can install an RSP package for live video streaming and add a DNAT rule (using the IP address, port number, or both) that transparently proxies all traffic redirected to the local RSP video instance.

Consequently, the local RSP video instance responds to the local clients on behalf of the original server, simultaneously communicating with the original server in the background over the WAN. This process streamlines the number of requests over the WAN, resulting in time and bandwidth savings.

The RSP rule that determines which traffic is network address translated is provided in the data flow rules for the virtual in-path VNI.

- Data flow rules are per VNI.
- Data flow rules are unidirectional. For example, typically you have a LAN-to-WAN rule for the LAN VNI, and a reverse WAN-to-LAN rule for the WAN VNI. WAN VNIs do not see data coming from the LAN, and LAN VNIs do not see packets coming from the WAN.
- For a WAN VNI, only WAN-to-LAN rules are applicable.
- For a LAN VNI, only LAN-to-WAN rules are applicable.
- You must create WAN-to-LAN rules and LAN-to-WAN rules separately.
- You can only add DNAT rules for a virtual in-path VNI.
- You can specify a target port range with DNAT rules.
- Typical rule actions that you can use to control the data flow for the various VNI types:
- **LAN** - Pass traffic around a VM or redirect it to the VM within a slot.
- **WAN** - Pass traffic around a VM or redirect it to the VM within a slot.
- **Virtual In-Path DNAT** - Pass traffic to the target IP or redirect it to a target IP.
- **Virtual In-Path Mirror** - Pass traffic along the data flow and copy it for monitoring.

For detailed information, see the see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Example

```
amnesiac (config) # rsp opt-vni 1:Rsp0VinPath rule dnat targetip 10.0.0.1/16 dstaddr 10.12.0.0./16
rulenum 3
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp opt-vni rule dnat move rulenum

Description

Moves a DNAT rule.

Syntax

rsp opt-vni <opt-vni> rule dnat move rulenum <number> to <number>

Parameters

<opt-vni>	Specify the management VNI. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: **wowzaSlot:Rsp0In**, **1:LanRSPInf** VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
<number>	Specify the original rule number and the rule number to move to. Optionally, type a descriptive name for the rule to replace the default rule number.

Usage

For detailed information, see the see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Example

```
amnesiac (config) # rsp opt-vni 1:TestVlan rule dnat move rulenum 2 to 4
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp opt-vni rule lan-to-wan

Description

Configures LAN to WAN VNI data flow rules.

Syntax

rsp opt-vni <VNI name> rule lan-to-wan [action {redirect | pass | copy}] |[srcaddr <srcaddr> srcport <srcport>] | [dstaddr <dstaddr> dstport <dstport>] | [protocol {all | tcp | udp | <protocol-number>}] |[vlan <vlan-id>] | [rulenum <rulenum>]

Parameter

<VNI name>	Specify the VNI name. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: **wowzaSlot:Rsp0In**
action {redirect | pass | copy}	Specify the action to perform on the rule: • **redirect** - Redirect the packet to a VM. • **pass** - Pass the packet along the data flow, bypassing the VM. • **copy** - Copy the packet to the VM and also pass it along the data flow.
srcaddr <srcaddr> srcport <srcport>	Optionally, specify the source subnet and port of the packet. For example, **1.2.3.0/24**, or leave blank to specify all. Specify the source port of the packet, either a single port value or a port range of **port1-port2**. **port1** must be less than **port2**.
dstaddr <dstaddr> dstport <dstport>	Optionally, specify the destination network. Specify the port can be either a single port value or a port range of **port1-port2**. **port1** must be less than **port2**.
protocol {all | tcp | udp| <protocol-number>}	Optionally, specify **all**, **tcp**, **udp**, or a protocol number (**1-254**). The default setting is **all**.
vlan <vlan-id>	Specify a VLAN tag ID for this rule
rulenum <rulenum>	Optionally, specify a number (**0 - 65535)** to replace the default rule number.

Usage

VNI rules determine what the VNI does with the traffic it receives. After you install a package and add it to a slot, you need to add rules to configure the data flow for the package unless you use the default rules for the package. For a LAN VNI, you add LAN-to-WAN rules to direct traffic. The redirection can be controlled by rules based on IP or port.

Rules are used with in-path and virtual in-path optimization VNIs. You do not need to add rules to management VNIs. Rules can perform one of these actions:

- Redirect the packets to the VM.
- Pass the packets along the data flow to the next VNI.
- Pass the packets along the data flow and also send a copy of the packets to the VM.

Note: The LAN-to-WAN and WAN-to-LAN rules are not used with Virtual RSP.

Suppose that you have installed a video streaming package, a security package, and a VPN package on the Steelhead appliance. You could define rules to invoke the following data path:

- A rule redirects all Flash video traffic coming in from the LAN side of the Steelhead appliance to a video proxy RSP package on the Steelhead appliance.
- A rule directs all of the other data directly to the next in-line package, RiOS, which optimizes the traffic.
- After RiOS optimizes the traffic, a rule intercepts the traffic on the WAN side and redirects it to a security package that checks the data (or, if it is a VPN solution, encrypts it), and sends it back out the WAN. You can control the data redirection using rules based on IP address or port number.

For detailed information, see the see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Example

```
amnesiac (config) # rsp opt-vni 1:Rsp0VinPath rule lan-to-wan action copy srcaddr 10.0.0.1/16
dstaddr 10.12.0.0./16 rulenum 3
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp opt-vni rule lan-to-wan move rulenum

Description

Moves a LAN to WAN rule.

Syntax

rsp opt-vni <opt-vni> rule lan-to-wan move rulenum <number> to <number>

Parameters

<opt-vni>	Specify the management VNI. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: **wowzaSlot:Rsp0In**, **1:LanRSPInf** VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
<number>	Specify the original rule number and the rule number to move to. Optionally, type a descriptive name for the rule to replace the default rule number.

Usage

For detailed information, see the see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Example

```
amnesiac (config) # rsp opt-vni rule lan-to-wan move rulenum 2 to 4
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp opt-vni rule wan-to-lan

Description

Configures WAN to LAN VNI data flow rules.

Syntax

rsp opt-vni <VNI name> rule wan-to-lan [action {redirect | pass | copy}]|[srcaddr <srcaddr> srcport <srcport>] | [dstaddr <dstaddr> dstport <dstport>] | protocol {all | tcp | udp] | <protocol-number>}] | [vlan <vlan-id>] | [rulenum <rulenum>]

Parameter

<VNI name>	Specify the VNI name. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: **wowzaSlot:Rsp0In**
action {redirect | pass | copy}	Specify the action to perform on the rule: • **redirect** - Redirect the packet to a VM. • **pass** - Pass the packet along the data flow, bypassing the VM. • **copy** - Copy the packet to the VM and also pass it along the data flow.
srcaddr <srcaddr> srcport <srcport>	Optionally, specify the source subnet and port of the packet. For example, **1.2.3.0/24**, or leave blank to specify all. Specify the source port of the packet, either a single port value or a port range of **port1-port2**. **port1** must be less than **port2**.
dstaddr <dstaddr> dstport <dstport>	Optionally, specify the destination network. Specify the port can be either a single port value or a port range of **port1-port2**. **port1** must be less than **port2**.
protocol {all | tcp | udp | <protocol-number>}	Optionally, select **All**, **TCP**, **UDP**, or a protocol number (**1-254**) from the drop-down list. The default setting is All.
vlan <vlan-id>	Specify a VLAN tag ID for this rule
rulenum <rulenum>	Optionally, type a number (**0 - 65535)** to replace the default rule number.

Usage

VNI rules determine what the VNI does with the traffic it receives. After you install a package and add it to a slot, you need to add rules to configure the data flow for the package unless you use the default rules for the package. For a LAN VNI, you add LAN-to-WAN rules to direct traffic. The redirection can be controlled by rules based on IP or port.

For a WAN VNI, only WAN-to-LAN rules apply. Data flow rules are unidirectional; for example, typically you have add a LAN-to-WAN for the LAN VNI and a reverse WAN-to-LAN rule for the WAN VNI.

For detailed information, see the see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Example

```
amnesiac (config) # rsp opt-vni 1:Rsp0VinPath rule wan-to-lan action copy srcaddr 10.0.0.1/16
dstaddr 10.12.0.0./16 rulenum 3
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp opt-vni rule wan-to-lan move rulenum

Description

Moves a WAN to LAN rule.

Syntax

rsp opt-vni <opt-vni> rule wan-to-lan move rulenum <number> to <number>

Parameters

<opt-vni>	Specify the management VNI. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: **wowzaSlot:Rsp0In**, **1:LanRSPInf** VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
<number>	Specify the original rule number and the rule number to move to. Optionally, type a descriptive name for the rule to replace the default rule number.

Usage

For detailed information, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Example

```
amnesiac (config) # rsp opt-vni 1:Rsp0VinPath rule wan-to-lan move rulenum 2 to 4
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp opt-vni vlan

Description

Sets the VLAN for the optimization VNI.

Syntax

rsp opt-vni <VNI name> vlan <vlan>

Parameter

<VNI name>	Specify the VNI name. VNI names have the following format: <SlotName>:<RSPinterfaceName> For example: **wowzaSlot:Rsp0In**, **1:LanRSPInf**, **firewall:eth0** VNI names must be between 1 and 30 characters long and can contain only alphanumeric, hyphen (-), and underscore (_) characters.
<vlan>	Specify the VLAN: **trunk**, **none**, or **0-4094**

Example

```
amnesiac (config) # rsp opt-vni 2:QAWan vlan trunk
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp package delete

Description

Deletes a package from the disk.

Syntax

rsp package delete <package>

Parameters

<package>	Specify the package name.

Usage

You can delete an RSP package installation file to release disk space. Deleting the RSP package installation file removes the file used to install the package into a slot. It does not uninstall the package from the slot. To install the package again, you must download the package and then install it into a slot.

Example

```
amnesiac (config) # rsp package delete SCPS_factory1.pkg
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp package fetch

Description

Downloads a package.

Syntax

rsp package fetch <http, ftp, or scp URL (e.g. scp://username:password@host/path)>

Parameters

<http, ftp, scp URL>	Specify the HTTP, FTP, or scp URL path. For secure copy, use the following path: /rsp/packages

Usage

Before installing a package, you must install RSP. After installing the RSP image, you can download and install packages. A package can be a virtual machine (VM) created:

- by a third-party vendor that also contains configuration files specific to the RSP implementation.
- by Riverbed.
- internally within your organization.

You can download any number of packages to the Steelhead appliance, but you can only run up to five packages at a time. The exact number depends on the package size, the amount of resources available, and your Steelhead appliance model.

RSP packages contain the service or applications in the virtual machine. RSP packages also contain Riverbed configuration files including the package VNIs. RSP packages include a .vmx file and one ore more .vmdk files. You need not open or modify any of the files in the package. The package files can be quite large and can take up several GBs of disk space.

RSP provides the following packages:

- **In-band packages** - In-band packages work in conjunction with the Steelhead appliance optimization services. You can use the following in-band packages:
  - **In-band LAN packages** - In-band LAN packages intercept data on the Steelhead appliance LAN interface before or after the data flows through RiOS, depending on the traffic direction. Examples of this type of package include Intrusion Detection System or Intrusion Prevention System packages.

- **In-band WAN packages** - In-band WAN packages intercept data on the Steelhead appliance WAN interface before or after the data flows through RiOS, depending on the traffic direction. Examples of this type of package include firewall, content filtering, and VPN packages.
- **In-band hybrid packages** - In-band hybrid packages intercept data on both the LAN interface and the WAN interface of the Steelhead appliance. Typically, in-band hybrid packages are network monitoring packages.
- **Out-of-band packages** - Out-of-band packages are not required to work in conjunction with the Steelhead appliance optimization service. Typically, out-of-band packages are located on the Steelhead appliance primary interface. Examples of this type of package include IPAM, print, DNS, and DHCP.

When you install an RSP package you must select an RSP slot. A slot is a directory on disk. When you install a package into a slot, the system unpacks the VM into the directory. When you remove a package, the system deletes the files from the slot.

After you install a package into a slot, you configure data flow rules for the RSP package. Data flow rules are similar to in-path rules, except they are unidirectional. Riverbed recommends you use the Management Console to define your data flow rules for your packages.

For detailed information, see the see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*, and the *RSP User's Guide*.

Example

```
amnesiac (config) # rsp package fetch http://example.com/newcentospkg.pkg
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp package move

Description

Renames a package.

Syntax

rsp package move <old-filename> to <new-filename>

Parameters

<old-filename>	Specify the package filename.
<new-filename>	Specify the new package filename.

Usage

After you load an RSP package on the Steelhead appliance, you can rename the package.

Example

```
amnesiac (config) # rsp package move centospkg.pkg to newcentospkg.pkg
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp shell

Description

Provides console access to RSP.

Syntax

rsp shell <slot-name>

Parameters

<slot-name>	Specify the slot name: 1, 2, 3, 4, 5

Example

```
amnesiac (config) # rsp shell 1
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot backup create

Description

Creates an RSP backup file.

Syntax

rsp slot <slot-name> backup create | nocompress | remote <URL>

Parameters

<slot-name>	Specify the slot name.
nocompress	Creates an uncompressed backup file.
remote <URL>	Specify a destination URL for the backup file.

Usage

This feature enables you to create a snapshot (a VMware feature that freezes a copy of the memory and disk contents), compress the snapshot, delete the snapshot, and move the compressed snapshot file.

The backup command generates a .zip file with a .bkup file extension. The default backup filename is <Steelhead appliance name>-<slotname>-<date>.bkup

You can use the **nocompress** option to create an uncompressed backup file. The **nocompress** option enables you to transfer the backup file efficiently using the Steelhead de-duplication feature.

Example

```
amnesiac (config) # rsp slot 1 backup create nocompress
```

Product

Steelhead appliance

Related Topics

"show rsp backups," "show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot backup restore

Description

Restores RSP data.

Syntax

rsp slot <slot-name> backup restore <backup filename>

Parameters

<slot-name>	Specify the slot name.
<backup filename>	Specify the backup filename.

Usage

Use the RSP backup feature to restore the RSP data in case the Steelhead appliance fails.

Important: Restores are only supported on the same Steelhead appliance model and slot.

Example

```
amnesiac (config) # rsp slot 1 backup restore amnesiac-sh1-1-20090211.bkup
```

Product

Steelhead appliance

Related Topics

"show rsp backups," "show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot clone

Description

Clones a single, specified slot to a remote Steelhead appliance.

Syntax

rsp slot <slot-name> clone [hostname <remote-steelhead>] [password <password>]

Parameters

<slot-name>	Specify the slot to be cloned to the remote Steelhead appliance.
<remote-steelhead>	Specify the hostname or IP address of the remote Steelhead appliance to which all slots are to be cloned.
<password>	Specify the RSP clone password for the remote Steelhead appliance to which all slots are to be cloned. The password value is set by the "rsp clone password" command.

Example

```
amnesiac (config) # rsp slot 2 clone hostname branchSHA003 password rsppw003
```

Product

Steelhead appliance

Related Topics

"rsp clone slots"

rsp slot enable

Description

Enables a slot (disk space) and starts the virtual machine.

Syntax

[no] rsp slot <slot-name> enable

Parameters

<slot-name>	Specify the slot name: 1, 2, 3, 4, 5

Usage

When you install an RSP package you must select an RSP slot. A slot is a directory on disk. When you install a package into a slot, the system unpacks the VM into the directory. When you remove a package, the system deletes the files from the slot.

You can install one package per slot. By default, the RSP slots are numbered 1 to 5. You can change a slot name to more make it more descriptive.

Verify that enough free memory is still available to run the virtual machine in the slot. If there is not enough free memory available you receive an insufficient memory error message, and the slot is not enabled. You can try reducing the memory footprint for the virtual machine, or reducing it for a virtual machine in another slot.

Note: RSP requires 2 GB additional memory on the Steelhead appliance. If the amount of available memory is less than the memory footprint for the virtual machine you are installing, you receive an insufficient memory error message.

The **no** command option disables the slot.

Example

```
amnesiac (config) # rsp slot 1 enable
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot install package

Description

Installs an RSP package into a slot.

Syntax

rsp slot <slot-name> install package <package>

Parameters

<slot-name>	Specify the slot name: 1, 2, 3, 4, 5
<package>	Specify the package name.

Usage

When you install an RSP package you must select an RSP *slot*. A slot is a directory on disk. When you install a package into a slot, the system unpacks the VM into the directory of the slot. When you uninstall a package, the system deletes the files in that slot.

You can install one package per slot. By default, the five RSP slots are numbered 1 to 5, although you can change a slot name to more make it more descriptive.

Note: Available slots are listed as null. To install an RSP package in an occupied slot, you must first uninstall the package for that slot. Installing a package into a slot and uninstalling that particular slot affects only the slot directory, not the package itself.

Example

```
amnesiac (config) # rsp slot 1 install package rsp_SCPS_factory1. pkg
Slot "1" is successfully installed.
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot priority

Description

Sets the CPU priority for the slot if there is contention for resources.

Syntax

rsp slot <slot-name> priority {high | normal | low}

Parameters

<slot-name>	Specify the slot name or number. The default names for the slots are 1, 2, 3, 4, 5.
high	Sets a higher priority relative to other slots
normal	Sets normal priority relative to other slots. The default priority setting is normal. In the event of CPU contention, CPU resources are allocated to the slots according to the priority specified. Slots with the same priority level receive equal access to the CPU.
low	Sets low priority relative to other slots.

Usage

The CPU uses the slot priority to allocate resources in the event of contention. By default all slots are set at normal priority.

Because there is only three priority levels, but five slots, it is always the case that more than one slot has the same priority. In that case, slots with the same priority are given equal access to the CPU.

Example

```
amnesiac (config) # rsp slot 1 priority high
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot rename

Description

Renames a slot.

Syntax

rsp slot <slot-name> rename <new-name>

Parameters

<slot-name>	Specify a slot name.
<new-name>	Specify a new name for the slot.

Usage

Before you rename an RSP slot, ensure that it is empty.

Example

```
amnesiac (config) # rsp slot 1 rename myslot
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot uninstall

Description

Uninstalls a slot.

Syntax

rsp slot <slot-name> uninstall

Parameter

<slot-name>	Specify the slot name.

Usage

Before you uninstall an RSP package from a slot, disable the slot in which the RSP package resides.

Example

```
amnesiac (config) # rsp slot 3 uninstall
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot vm disk attach name

Description

Attaches a virtual disk to the VM.

Syntax

rsp slot <slot-name> vm disk attach name <name> controller <integer> device <integer>

Parameters

<slot-name>	Specify the slot name.
<name>	Specify the disk name.
controller <integer>	Specify the disk controller index: • IDE: 0-1 • SCSI: 0-3
device <integer>	Specify the device index: • IDE: 0 or 1 • SCSI: 0 to 15 inclusive

Usage

You attach a virtual disk to the VM after you create it.

Currently packages must ship with all required virtual disks. This can be inefficient since most of the existing disks may be blank. You can add one or more disks to a VM. The virtual disk can be detached and removed as needed.

Example

```
amnesiac (config) # rsp slot vm disk attach name storage controller 2 device 2
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot vm disk create name

Description

Creates a virtual disk for the VM.

Syntax

rsp slot <slot-name> vm disk create name <name> size <size in MB> adapter <type>

Parameters

<slot-name>	Specify the slot name.
<name>	Specify the disk name.
size <size in MB>	Specify the new disk size in MBs.
adapter <type>	Specify one of the following the adapter types: • **ide** - Specifies an IDE adapter • **lsilogic** - Specifies an LSI Logic SCSI adapter • **buslogic** - Specifies a Bus Logic SCSI adapter

Usage

Currently packages must ship with all required virtual disks. This can be inefficient since most of the existing disks may be blank. You can add one or more disks to a VM. The virtual disk can be detached and removed as needed.

Example

```
amnesiac (config) # rsp slot 1 vm disk create name storage size 10 adapter ide
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot vm disk delete name

Description

Deletes a virtual disk from the VM.

Syntax

rsp slot <slot-name> vm disk delete name <name>

Parameters

<slot-name>	Specify the slot name.
<name>	Specify the disk name.

Example

```
amnesiac (config) # rsp slot 1 vm disk delete name storage
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot vm disk detach name

Description

Detaches a virtual disk from the VM.

Syntax

rsp slot <slot-name> vm disk detach name <name>

Parameters

<slot-name>	Specify the slot name.
<name>	Specify the disk name.

Example

```
amnesiac (config) # rsp slot 1 vm disk detach name storage
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot vm disk grow name

Description

Enlarges a virtual disk attached to the VM.

Syntax

rsp slot <slot-name> vm disk grow name <name> size <size in MB>

Parameters

<slot-name>	Specify the slot name.
name <name>	Specify the disk name.
<size in MB>	Specify the disk size in MBs.

Example

```
amnesiac (config) # rsp slot 1 vm disk grow name storage size 10
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot vm memory-size

Description

Changes the slot memory size.

Syntax

rsp slot <slot-name> vm memory-size <size>

Parameters

<slot-name>	Specify the slot name.
<size>	Specify how many megabytes of memory to allocate to the virtual machine. This value must be a multiple of 4.

Usage

To learn how much memory is available for RSP, execute the following command (or check the RSP Service page on the Management Console):

```
amnesiac (config) # show rsp
  Supported:    Yes
  Installed:    Yes
  Release:      6.0.0
  Enabled:      Yes
  State:        Running
  Disk Space:   13.54 GB used / 163.64 GB free / 177.18 GB total
  Memory:       0 MB used / 128 MB free / 128 MB total
```

Used RSP memory is defined as the sum of each enabled or powered-on virtual memory setting of the slot. If you attempt to enable a slot, free RSP memory must be equal to or greater than the virtual memory setting of the slot. If there is insufficient free RSP memory to enable a slot, a user can free up RSP memory by reducing the virtual memory setting for that slot, disable a currently enabled slot, or both.

Example

```
amnesiac (config) # rsp slot 1 vm memory-size 256
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot watchdog block

Description

Configures a watchdog for a given slot to block traffic if the package fails.

Syntax

rsp slot <slot-name> watchdog block

Parameters

<slot-name>	Specify the slot name.

Usage

Requests traffic to be blocked if the watchdog indicates that a specified slot has failed.

Example

```
amnesiac (config) # rsp slot 1 watchdog block
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot watchdog heartbeat enable

Description

Configures a regular heartbeat from a specified slot. Riverbed recommends you configure an RSP watchdog that blocks traffic in the event an in-path security package, such as a firewall, fails.

Syntax

rsp slot <slot-name> watchdog heartbeat enable

Parameters

<slot-name>	Specify the slot name.

Usage

The RSP watchdog feature allows you to monitor each installed slot for failure, and determines what should happen to the traffic and the VM within the slot should failure occur. By default the watchdog sends an email alert and, if the slot is in a Inpath configuration, routes traffic around the failed slot.

You can optionally configure the watchdog to block traffic in the case of failure. You can also configure the watchdog to reboot the VM within the slot.

Note: This is a hard reboot, that is a power-cycling of the VM. You must confirm that the VM will come up after a virtual power-cycle before enabling this feature.

The Steelhead appliance offers two types of RSP watchdog:

- **Ping Monitoring** - Ping monitoring enables you to monitor the package by simply pinging a network interface within the VM. The RSP package must have a Management Virtual Network Interface (VNI) before you can configure ping monitoring. For details on configuring ping monitoring, see "rsp slot watchdog ping enable" on page 665.
- **Heartbeat Monitoring** - Heartbeat monitoring enables you to monitor a package for a heartbeat, which is transmitted by the VM within the slot. The RSP package must have been configured separately to transmit this heartbeat. The package does not need a management VNI to use heartbeat monitoring.

Because most VMs require a certain length of time to initialize, the watchdog enables you to set a startup grace period for each slot. This startup period is effectively added to the first watchdog timeout duration and prevents false failures while the VM is initializing. For details on configuring ping monitoring see "rsp slot watchdog startup grace-period" on page 667.

You can configure one or both types. If you configure both types of watchdog, if either fails the VM is marked as failed. By default, the watchdog sends an email alert and bypasses traffic for failed packages. Traffic that normally flows through an optimization VNI on the RSP package now skips the optimization VNI, and passes through.

The RSP package must have the management interface configured before you can configure a watchdog on it.

You can configure a watchdog to block traffic destined for failed packages. You can also disable fail-to-bypass mode on the package interface. This is useful in the event of a firewall package failure. Otherwise, if the Steelhead appliance loses power or fails, traffic is allowed through the interface. For details about enabling fail-to-bypass, see the *RSP User's Guide*. For details about which interfaces support disabling fail-to-bypass, see the *Network Interface Card Installation Guide*.

Example

```
amnesiac (config) # rsp slot 1 watchdog timeout 20
amnesiac (config) # rsp slot 1 watchdog heartbeat enable
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot watchdog ping enable

Description

Configures ping monitoring from a specified slot. Riverbed recommends you configure an RSP watchdog that blocks traffic in the event an in-path security package, such as a firewall, fails.

Syntax

rsp slot <slot-name> watchdog ping enable

Parameters

<slot-name>	Specify the slot name.

Usage

Ping monitoring allows you to monitor the package by simply pinging a network interface within the VM. The RSP must have a Management Virtual Network Interface (VNI) before you can configure ping monitoring. For details about the RSP watchdog feature, see "rsp slot watchdog heartbeat enable" on page 664.

Example

```
amnesiac (config) # rsp slot 1 watchdog ping enable
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot watchdog ping interval

Description

Configures ping interval from a specified slot. Riverbed recommends you configure an RSP watchdog that blocks traffic in the event an in-path security package, such as a firewall, fails.

Syntax

rsp slot <slot-name> watchdog ping interval <seconds>

Parameters

<slot-name>	Specify the slot name.
<seconds>	Specify the number of seconds.

Example

```
amnesiac (config) # rsp slot 1 watchdog ping interval 10
amnesiac (config) # rsp slot 1 watchdog ping ip 192.179.0.1
amnesiac (config) # rsp slot 1 watchdog ping enable
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot watchdog ping ip

Description

Configures the IP address from a specified slot to ping. Riverbed recommends you configure an RSP watchdog that blocks traffic in the event an in-path security package, such as a firewall, fails.

Syntax

rsp slot <slot-name> watchdog ping ip <ip-addr>

Parameters

<slot-name>	Specify the slot name.
<ip-addr>	Specify the IP address to ping.

Example

```
amnesiac (config) # rsp slot 1 watchdog ping ip 10.0.0.1
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot watchdog slot-reboot enable

Description

Enables a slot reboot upon a VM failure.

Syntax

[no] rsp slot <slot-name> watchdog slot-reboot enable

Parameters

<slot-name>	Specify the slot name.

Usage

Requests that the VM is rebooted if the watchdog detects that it has failed.

The **no** command option disables slot reboot upon VM failure.

Example

```
amnesiac (config) # rsp slot 1 watchdog slot-reboot enable
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

rsp slot watchdog startup grace-period

Description

Configures watchdog start up grace period for the specified slot, thereby preventing false slot failure alarms from being generated during slot start up.

Syntax

rsp slot <slot-name> watchdog startup grace-period <seconds>

Parameters

<slot-name>	Specify the slot name.
<seconds>	Specify the number of seconds. The minimum grace period is 15 seconds.

Usage

Because most VMs require a certain length of time to initialize, the watchdog allows you to set a startup grace period for each slot. This startup period is effectively added to the first watchdog time-out duration and prevents false failures while the VM is initializing.

Example

```
amnesiac (config) # rsp slot 1 watchdog startup grace-period 60
amnesiac (config) # rsp slot 1 watchdog slot-reboot enable
```

Product

Steelhead appliance

Related Topics

"show rsp," "show rsp images," "show rsp opt-vni," "show rsp package," "show rsp packages," "show rsp slot," "show rsp slots"

IPSec Commands

This section describes the IPSec commands.

ip security authentication policy

Description

Sets the authentication algorithms in order of priority.

Syntax

ip security authentication policy <method 1> [<method 2>]

Parameters

<policy>	Specify the primary policy (method 1): • **hmac_md5** - Message-Digest algorithm 5 (MD5) is a widely-used cryptographic hash function with a 128-bit hash value. This is the default value. • **hmac_sha1** - Secure Hash Algorithm (SHA1) is a set of related cryptographic hash functions. SHA-1 is considered to be the successor to MD5.
<policy>	Specify the secondary policy (method 2): **hmac_md5**, **hmac_sha1**

Usage

You must specify at least one algorithm. The algorithm is used to guarantee the authenticity of each packet.

Example

```
amnesiac (config) # ip security authentication policy hmac_md5
```

Product

Steelhead appliance, CSH

Related Topics

"show ip"

ip security enable

Description

Enables IPSec support.

Syntax

[no] ip security enable

Parameters

None

Usage

Enabling IPSec support makes it difficult for a third party to view your data or pose as a machine you expect to receive data from. You must also specify a shared secret to enable IPSec support. To create a shared secret see, "ip security shared secret".

To enable IPSec authentication, you must have at least one encryption and authentication algorithm specified.

You must set IPsec support on each peer Steelhead appliance in your network for which you want to establish a secure connection. You must also specify a shared secret on each peer Steelhead appliance.

If you NAT traffic between Steelhead appliances, you cannot use the IPSec channel between the appliances because the NAT changes the packet headers, causing IPSec to reject them.

Note: RiOS v6.0 and later also provides support for SSL peering beyond traditional HTTPS traffic. For details, see "Secure Peering (Secure Inner Channel) Commands" on page 704.

The **no** command option disables IPSec support.

Example

```
amnesiac (config) # ip security enable
```

Product

Steelhead appliance, CSH

Related Topics

"show ip"

---

ip security encryption policy

Description

Sets the encryption algorithms in order of priority.

Syntax

ip security encryption policy <algorithm> [<algorithm>]

Parameters

<algorithm>	Specify the primary algorithm. If you do not have a valid SSL license key (also called the Enhanced Cryptography License key) installed on your Steelhead appliance, you can specify one of the following encryption algorithms: • **des -** The Data Encryption Standard. This is the default value. • **null_enc** - The null encryption algorithm. If you have a valid SSL license key installed on your Steelhead appliance, you can specify any of the above encryption algorithms or any of the following more secure encryption algorithms: • **des -** Triple DES encryption algorithm. • **aes -** The AES 128-bit encryption algorithm. • **aes256 -** The AES 256-bit encryption algorithm. If you do not specify an encryption algorithm, the default value, **des**, is used.
<algorithm>	Specify the alternate algorithm. If you do not have a valid SSL license key (also called the Enhanced Cryptography License key) installed on your Steelhead appliance, you can specify one of the following encryption algorithms: • **des -** The Data Encryption Standard. This is the default value. • **null_enc** - The null encryption algorithm. If you have a valid SSL license key installed on your Steelhead appliance, you can specify any of the above encryption algorithms or any of the following more secure encryption algorithms: • **des -** Triple DES encryption algorithm. • **aes -** The AES 128-bit encryption algorithm. • **aes256 -** The AES 256-bit encryption algorithm. If you do not specify an encryption algorithm, the default value, **des**, is used.

Usage

You must specify at least one algorithm. The algorithm is used to encrypt each packet sent using IPSec.

For detailed information about SSL, see “protocol ssl enable” on page 685

Example

```
amnesiac (config) # ip security encryption policy null_enc
```

Product

Steelhead appliance, CSH

Related Topics

“show ip”

ip security peer ip

Description

Sets the peer Steelhead appliance for which you want to make a secure connection.

Syntax

[no] ip security peer ip <ip-addr>

Parameters

<ip-addr>	Specify the peer IP address.

Usage

If IPSec is enabled on this Steelhead appliance, then it must also be enabled on all Steelhead appliances in the IP security peers list; otherwise this Steelhead appliance will not be able to make optimized connections with those peers that are not running IPSec.

If a connection has not been established between the Steelhead appliances that are configured to use IPSec security, the Peers list does not display the peer Steelhead appliance because a security association has not been established.

When you add a peer, there is a short service disruption (3-4 seconds) causing the state and time-stamp to change in the Current Connections report.

The **no** command option disables the peer.

Example

```
amnesiac (config) # ip security peer ip 10.0.0.2
```

Product

Steelhead appliance, CSH

Related Topics

"show ip"

ip security pfs enable

Description

Enables Perfect Forward Secrecy. Perfect Forward Secrecy provides additional security by renegotiating keys at specified intervals. With Perfect Forward Secrecy, if one key is compromised, previous and subsequent keys are secure because they are not derived from previous keys.

Syntax

[no] ip security pfs enable

Parameters

None

Usage

The **no** command option disables Perfect Forward Secrecy**.**

Example

```
amnesiac (config) # ip security pfs enable
```

Product

Steelhead appliance, CSH

Related Topics

"show ip"

ip security rekey interval

Description

Sets the time between quick-mode renegotiation of keys by IKE. IKE is a method for establishing a SA that authenticates users, negotiates the encryption method, and exchanges a secret key. IKE uses public key cryptography to provide the secure transmission of a secret key to a recipient so that the encrypted data can be decrypted at the other end.

Syntax

[no] ip security rekey interval <minutes>

Parameters

<minutes>	Specify the number of minutes between quick-mode renegotiation of keys. The value must be a number between **1** and **65535**. The default value is 240.

Usage

The **no** command options resets the interval to the default.

Example

```
amnesiac (config) # ip security rekey interval 30
```

Product

Steelhead appliance, CSH

Related Topics

"show ip"

ip security shared secret

Description

Sets the shared secret used to negotiate and renegotiate secret keys.

Syntax

ip security shared secret <secret key>

Parameters

<secret key>	Specify the secret key to ensure Perfect Forward Secrecy security.

Usage

All Steelhead appliances that need to communicate to each other using IPSec must have the same key. The **ip security shared secret** option must be set before IPSec is enabled.

Example

```
amnesiac (config) # ip security shared secret xxxx
```

Product

Steelhead appliance, CSH

Related Topics

"show ip"

SSL Support Commands

This section describes the SSL support commands.

no protocol ssl backend bypass-table

Description

Configures the SSL bypass table settings.

Syntax

no protocol ssl backend bypass-table [client-ip <ip-address>] {server-ip <ip-address> [port <port-number>] server-hostname <name> | all}

Parameters

client-ip <ip-address>	Removes a bypass entry with the specified client IP address; defaults to **all** if no client IP address is specified. You can add a wildcard entry (*) for the client IP address.
server-ip <ip-address>	Removes a bypass entry with the specified server IP address.
port <port-number>	Specify the port number; defaults to port 443 if no port is specified.
server-hostname <name>	Removes a bypass entry with the specified hostname.
all	Removes all servers and clients from the bypass table.

Usage

Traffic destined to the servers and client IP addresses (or wildcards) listed in the bypass table are passed through the Steelhead appliance and not optimized by SSL.

Example

```
amnesiac (config) # no protocol ssl backend bypass-table server-ip 10.1.2.1 server-hostname
site3server
```

Product

Steelhead appliance

Related Topics

"show protocol ssl backend bypass-table"

protocol ssl backend bypass-interval

Description

Sets the bypass interval after failed server handshake.

Syntax

[no] protocol ssl backend bypass-interval <seconds>

Parameters

<seconds>	Specify an integer value in seconds to bypass-interval.

Usage

To view current setting, use the command **show protocol ssl backend** command.

Example

```
amnesiac (config) # protocol ssl backend bypass-interval 60
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl backend"

protocol ssl backend bypass-table max-size

Description

Configures the SSL bypass table size.

Syntax

[no] protocol ssl backend bypass-table max-size <max size>

Parameters

<max size>	Specify the maximum size of the bypass table.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl backend bypass-table max-size 60
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl backend bypass-table"

protocol ssl backend bypass-table no-cert-intvl

Description

Sets the bypass interval for servers for which no suitable certificate was found.

Syntax

[no] protocol ssl backend bypass-table no-cert-intvl <no-cert-intvl> seconds

Parameters

<no-cert-intvl> seconds	Specify the interval in seconds.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl backend bypass-table no-cert-intvl 120 seconds
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl backend bypass-table"

protocol ssl backend client cipher-string

Description

Sets the cipher for use with back-end clients.

Syntax

[no] protocol ssl backend client cipher-string <cipher-string> cipher-num <ciphr-number>

Parameters

<cipher string>	Specify a cipher string for use with clients. For a complete list: **protocol ssl backend client cipher-string ?**
cipher-num <ciphr-number>	Specify the cipher number from **1-N** or **end**.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl backend client cipher-string DEFAULT cipher-num 1
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl backend"

protocol ssl backend server chain-cert cache enable

Description

Configures certificate chain caching for the back-end server.

Syntax

[no] protocol ssl backend server chain-cert cache enable

Parameters

None

Usage

Synchronizes the chain certificate configuration on the server-side Steelhead appliance with the chain certificate configuration on the back-end server. The synchronization occurs after a handshake fails between the client-side and server-side Steelhead appliance. By default, this option is disabled.

Enable this option when you replace an existing chain certificate on the back-end server with a new chain to ensure that the certificate chain remains in sync on both the server-side Steelhead appliance and the back-end server.

This option never replaces the server certificate. It updates the chain containing the intermediate certificates and the root certificate in the client context.

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl backend server chain-cert cache enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl backend"

protocol ssl backend server cipher-string

Description

Configures back-end SSL server settings.

Syntax

[no] protocol ssl backend server cipher-string <string> [cipher-num <number>]

Parameters

cipher-string <string>	Specify the cipher-strings (case-sensitive) or a combination using the underscore character (_) for communicating with clients. For a complete list, view the CLI online help. You must specify at least one cipher for peers, clients, and servers for SSL to function properly. The default cipher setting is **DEFAULT** which represents a variety of high- strength ciphers that allow for compatibility with many browsers and servers.
cipher-num <number>	Specify a number to set the order of the list. The number must be an integer greater or equal to 1-N, or **end**.

Usage

Create a preference list of cipher strings used for server-handshakes.

To view your list, use the command **show protocol ssl backend {client | server} cipher-strings**.

Example

```
amnesiac (config) # protocol ssl backend server cipher-string LOW
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl backend client cipher-strings"

protocol ssl backend server renegotiation null-cert enable

Description

Configures renegotiation settings with back-end servers.

Syntax

protocol ssl backend server renegotiation null-cert enable

Parameters

None

Example

```
amnesiac (config) # protocol ssl backend server renegotiation null-cert enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl backend"

protocol ssl backend sni enable

Description

Configures server name indication (SNI) settings.

Syntax

[no] protocol ssl backend sni enable

Parameters

None

Usage

SNI provides SSL clients a method to explicitly identify the server they are trying to contact. The server can then determine the correct SSL client for the request and properly set up the connection. Many virtual SSL clients can share the same IP address and port, and each client can own a unique certificate.

SNI support enables:

- the use of the SNI in the certificate selection process.
- the verification of the name fields in the proxy certificate against the client request

Example

```
amnesiac (config) # protocol ssl backend sni enable
```

Product

Steelhead appliance

Related Topics

"show protocol ssl backend"

protocol ssl bulk-export password

Description

Exports the current SSL configuration, keys, and certificates.

Syntax

protocol ssl bulk-export password <password> [include-servers] [incl-scep-crl]

Parameters

<password>	Specify a password used to encrypt exported data.
include-servers	Optionally, specify **include-servers** to include server certificates and keys. If you include this parameter, the data includes the peering certificate, key, all certificate authorities, and all peering trust entities. In addition, it contains all the back-end server configurations (certificates, keys, and so on). **Important:** To protect your server's private keys, do not include this parameter when performing bulk exports of peers.
incl-scep-crl	Optionally, include Simple Certificate Enrollment Protocol (SCEP) and Certificate Revocation List (CRL) configuration.

Usage

Use bulk-export to expedite backup and peer trust configurations:

- **Backup -** You can use the bulk export feature to back up your SSL configurations, including your server configurations and private keys.

- **Peer Trust -** If you use self-signed peering certificates and have multiple Steelhead appliances (including multiple server-side appliances), you can use the bulk import feature to avoid configuring each peering trust relationship between the pairs of Steelhead appliances.

To protect your server private keys, do not include server configurations (for example, Certificates and Keys) when performing bulk exports of trusted peers.

The following rules apply to bulk data when importing and exporting the data:

- **Peering Certificate and Key Data** - If the serial numbers match, the Steelhead appliance importing the bulk data overwrites its existing peering certificates and keys with that bulk data. If the serial numbers do not match, the Steelhead appliance importing the bulk data does not overwrite its peering certificate and key.
- **Certificate Authority, Peering Trust, and SSL Server Configuration Data** - For all other configuration data such as certificate authorities, peering trusts, and server configurations (if included), if there is a conflict, the imported configuration data take precedence (that is, the imported configuration data overwrites any existing configurations).

Example

```
amnesiac (config) # protocol ssl bulk-export password foo_pass include-servers
U2FsdGVkX1/GM9EmJ0O9c1ZXh9N18PuxiAJdG1maPGtBzSrsU/CzgNaOrGsXPhor
VEDokHUvuvzsfvKfC6VnkXHOdyAde+vbMildK/lxrqRsAD1n0ezFFuobYmQ7a7uu
TmmSVDc9jL9tIVhd5sToRmeUhYhEHS369ubWMWBZ5rounu57JE6yktECqo7tKEVT
DPXmF1BSbnbK+AHZc6NtyYP3OQ88vm9iNySOHGzJ17HvhojzWth5dwNNx28I8GDS
zCmkqlaNX6vI3R/9KmtIR/Pk6QCfQ0sMvXLeThnSPnQ6wLGctPxYuoLJe0cTNlVh
r3HjRHSKXC7ki6Qaw91VDdTobtQFuJUTvSbpKME9bfskWlFh9NMWqKEuTJiKC7GN
[partial example]
Product
```

Steelhead appliance, CSH

Related Topics

"show protocol ssl", "show scep service"

protocol ssl bulk-import

Description

Imports SSL configuration, keys, and certificates.

Syntax

protocol ssl bulk-import password <password> data <data>

Parameters

password <password>	Specify a password required to decrypt data.
data <data>	Specify a file that contains previously exported data or cut and paste from the output of the output of the corresponding **protocol ssl bulk-export** command.

Usage

You can import multiple files or copy and paste multiple exported data sets. Double quotes indicate to the command that input will be supplied, and the command responds with a visible cursor. This feature can be useful for scripting.

For example, if the export data has four lines and starts with **0** and ends with **j**:

```
01234
56789
abcde
fghij
```

then the command should look like this:

```
steelhead (config) # protocol ssl bulk-import password <password> data "
> 01234
> 56789
> abcde
> fghij
```

```
    > "
```

You can use the same syntax for file names. The double-quotes are required to indicate the beginning and end of the prompts.

The greater-than sign (>) cursor at the beginning of each line indicates that the CLI will continue to accept more input until the input is closed by a double quote (").

Backup and peer trust relationships

Use the bulk export and import feature to expedite configuring backup and peer trust relationships:

The bulk data that you import contains the serial number of the exporting Steelhead appliance. The Steelhead appliance importing the data compares its own serial number with the serial number contained in the bulk data. The following rules apply to bulk data when importing and exporting the data:

- **Peering Certificate and Key Data** - If the serial numbers match, the Steelhead appliance importing the bulk data overwrites its existing peering certificates and keys with that bulk data. If the serial numbers do not match, the Steelhead appliance importing the bulk data does not overwrite its peering certificate and key.
- **Certificate Authority, Peering Trust, and SSL Server Configuration Data** - For all other configuration data such as certificate authorities, peering trusts, and server configurations (if included), if there is a conflict, the imported configuration data take precedence (that is, the imported configuration data overwrites any existing configurations).

For example, if you have two servers: 1.1.1.1:443 (enabled) and 2.2.2.2:443 (disabled), the bulk data contains three servers: 1.1.1.1:443 (disabled), 2.2.2.2:443 (disabled), and 3.3.3.3:443 (enabled). After performing a bulk import of the data, there are now three servers: 1.1.1.1:443 (disabled), 2.2.2.2:443 (disabled), and 3.3.3.3:443 (enabled). The certificates and keys of servers 1.1.1.1:443 and 2.2.2.2:443 have been overwritten with those contained in the bulk data.

Bulk importing of data cannot delete configurations; it can only add or overwrite them.

Bulk importing does not require a Steelhead service restart.

Example

```
amnesiac (config) # protocol ssl bulk-import password temp data temp
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl"

protocol ssl ca cert

Description

Imports CA certificates.

Syntax

[no] protocol ssl ca cert <cert-data> [local-name <name>]

Parameters

<cert-data> <cr>	Specify the Certificate data in PEM format. You can import multiple certificates.
local-name <name>	Optionally, specify the local name for the certificate (ignored if importing multiple certificates).

Usage

Enable on a client-side Steelhead appliance to reuse the original session when the client reconnects to an SSL server. Reusing the session provides two benefits: it lessens the CPU load because it eliminates expensive asymmetric key operations and it shortens the key negotiation process by avoiding WAN round trips to the server.

By default, this option is disabled.

Both the client-side and server-side Steelheads must be configured to optimize SSL traffic.

Enabling this option requires an optimization service restart.

Example

```
amnesiac (config) # protocol ssl ca cert COMODO "-----BEGIN CERTIFICATE-----
MIIEHTCCAwWgAwIBAgIQToEtioJl4AsC7j41AkblPTANBgkqhkiG9w0BAQUFADCB
gTELMAkGA1UEBhMCR0IxGzAZBgNVBAgTEkdyZWF0ZXIgTWFuY2hlc3RlcjEQMA4G
A1UEBxMHU2FsZm9yZDEaMBgGA1UEChMRQ09NT0RPIENBIExpbWl0ZWQxJzAlBgNV
BAMTHkNPTU9ETyBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eTAeFw0wNjEyMDEwMDAw
MDBaFw0yOTEyMzEyMzU5NTlaMIGBMQswCQYDVQQGEwJHQjEbMBkGA1UECBMSR3Jl
YXRlciBNYW5jaGVzdGVyMRAwDgYDVQQHEwdTYWxmb3JkMRowGAYDVQQKExFDT01P
RE8gQ0EgTGltaXRlZDEnMCUGA1UEAxMeQ09NT0RPIENlcnRpZmljYXRpb24gQXV0
aG9yaXR5MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA0ECLi3LjkRv3
UcEbVASY06m/weaKXTuH+7uIzg3jLz8GlvCiKVCZrts7oVewdFFxze1CkU1B/qnI
2GqGd0S7WWaXUF601CxwRM/aN5VCaTwwxHGzUvAhTaHYujl8HJ6jJJ3ygxaYqhZ8
Q5sVW7euNJH+1GImGEaaP+vB+fGQV+useg2L23IwambV4EajcNxo2f8ESIl33rXp
+2dtQem8Ob0y2WIC8bGoPW43nOIv4tOiJovGuFVDiOEjPqXSJDlqR6sA1KGzqSX+
DT+nHbrTUcELpNqsOO9VUCQFZUaTNE8tja3G1CEZ0o7KBWFxB3NH5YoZEr0ETc5O
nKVIrLsm9wIDAQABo4GOMIGLMB0GA1UdDgQWBBQLWOWLxkwVN6RAqTCpIb5HNlpW
/zAOBgNVHQ8BAf8EBAMCAQYwDwYDVR0TAQH/BAUwAwEB/zBJBgNVHR8EQjBAMD6g
PKA6hjhodHRwOi8vY3JsLmNvbW9kb2NhLmNvbS9DT01PRE9DZXJ0aWZpY2F0aW9u
QXV0aG9yaXR5LmNybDANBgkqhkiG9w0BAQUFAAOCAQEAPpiem/Yb6dc5t3iuHXIY
SdOH5EOC6z/JqvWote9VfCFSZfnVDeFs9D6Mk3ORLgLETgdxb8CPOGEIqB6BCsAv
IC9Bi5HcSEW88cbeunZrM8gALTFGTO3nnc+IlP8zwFboJIYmuNg4ON8qa90SzMc/
RxdMosIGlgnW2/4/PEZB31jiVg88O8EckzXZOFKs7sjsLjBOlDW0JB9LeGna8gI4
zJVSk/BwJVmcIGfE7vmLV2H0knZ9P4SNVbfo5azV8fUZVqZa+5Acr5Pr5RzUZ5dd
BA6+C4OmF4O5MBKgxTMVBbkN+8cFduPYSo38NBejxiEovjBFMR7HeL5YYTisO+IB
ZQ==
-----END CERTIFICATE-----"
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl"

protocol ssl client-cer-auth enable

Description

Enables Client Certificate Authentication.

Syntax

[no] protocol ssl client-cer-auth enable

Parameters

None.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl client-cer-auth enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl"

protocol ssl client-side session-reuse enable

Description

Configures the client-side SSL connection-reuse settings.

Syntax

[no] protocol ssl client-side session-reuse enable

Parameters

None

Usage

Enable on a client-side Steelhead appliance to reuse the original session when the client reconnects to an SSL server. Reusing the session provides two benefits: it lessens the CPU load because it eliminates expensive asymmetric key operations and it shortens the key negotiation process by avoiding WAN round trips to the server.

By default, this option is disabled in RiOS v6.5.2 and earlier releases. Enabling this option requires an optimization service restart.

In v7.0, this option is enabled by default when a new configuration is created or when upgrading from a version prior to v7.0.

Example

```
amnesiac (config) # protocol ssl client-side session-reuse enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl client-side session-reuse"

protocol ssl client-side session-reuse timeout

Description

Configures client-side SSL connection-reuse time-out setting.

Syntax

[no] protocol ssl client-side session-reuse timeout <number of seconds>

Parameters

<number of seconds>	Specify the amount of time the client can reuse a session with an SSL server after the initial connection ends. The range is 2 minutes to 24 hours. The default value is 10 hours.

Usage

Specify the amount of time the client can reuse a session with an SSL server after the initial connection ends. Enabling this option requires an optimization service restart.

Example

```
amnesiac (config) # protocol ssl client-side session-reuse timeout 120
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl client-side session-reuse"

protocol ssl crl ca

Description

Configures Certificate Revocation Lists (CRL) for an automatically discovered CAs. You can update automatically discovered CRLs using this command.

Syntax

[no] protocol ssl crl ca <ca name> cdp <integer> ldap server <ip-addr or hostname> | crl-attr-name <attr-name> | port <port>

Parameters

<ca name>	Specify the name of a SSL CA certificate.
cdp <integer>	Specify an integer index. Index of a CRL Certificate Distribution Point (CDP) in a CA certificate. The **no protocol ssl crl ca <ca name> cdp <integer>** command option removes the update.
ldap server <ip-addr or hostname>	Specify the LDAP server IP address or hostname to modify a CDP URI.
crl-attr-name <attr-name>	Optionally, specify the attribute name of CRL in a LDAP entry.
port <port>	Optionally, specify the Lightweight Directory Access Protocol (LDAP) service port.

Usage

Enabling CRL allows the CA to revoke a certificate. For example, when the private key of the certificate has been compromised, the CA can issue a CRL that revokes the certificate.

A CRL includes any digital certificates that have been invalidated before their expiration date, including the reasons for their revocation and the names of the issuing certificate signing authorities. A CRL prevents the use of digital certificates and signatures that have been compromised. The certificate authorities that issue the original certificates create and maintain the CRLs.

To clear the CRL alarm, execute the **no stats alarm crl_error** enable command.

Example

```
amnesiac (config) # protocol ssl crl ca Go_Daddy_Class_2 cdp 512
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl crl"

protocol ssl crl cas enable

Description

Enables CRL polling and use of CRL in handshake verifications of CAs certificates. Currently, the Steelhead appliance only supports downloading CRLs from Lightweight Directory Access Protocol (LDAP) servers.

Syntax

[no] protocol ssl crl cas enable

Parameters

None

Usage

Enabling CRL allows the CA to revoke a certificate. For example, when the private key of the certificate has been compromised, the CA can issue a CRL that revokes the certificate.

A CRL includes any digital certificates that have been invalidated before their expiration date, including the reasons for their revocation and the names of the issuing certificate signing authorities. A CRL prevents the use of digital certificates and signatures that have been compromised. The certificate authorities that issue the original certificates create and maintain the CRLs.

Example

```
amnesiac (config) # protocol ssl crl cas enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl crl"

protocol ssl crl handshake fail-if-missing

Description

Configures handshake behavior for a CRL

Syntax

[no] protocol ssl crl handshake fail-if-missing

Parameters

None

Usage

Use this command to fail the handshake if a relevant CRL cannot be found.

Example

```
amnesiac (config) # protocol ssl crl handshake fail-if-missing
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl crl"

protocol ssl crl manual

Description

Manually configures a CRL Certificate Distribution Point (CDP) for CRL management.

Syntax

[no] protocol ssl crl manual ca < ca-name> uri <string>| peering ca uri <uri>

Parameters

ca <ca-name>	Specify the CA name to manually configure the CDP. The **no protocol ssl crl manual** command removes manually configured CDPs.
uri <string>	Specify the CDP LDAP URI to manually configure the CDP for the CRL.
peering ca uri <uri>	Specify the peering CA name to manually configure the CDP URI.

Usage

The Steelhead appliance automatically discovers CDPs for all certificates on the appliance. You can manually configure a CA using this command.

Example

```
amnesiac (config) # protocol ssl crl manual ca Camerfirma_Chambers_of_Commerce uri URI: http://
crl.chambersign.org/chambersroot.crl
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl crl"

protocol ssl crl

Description

Configures a CRL for an automatically discovered peering CA.

Syntax

[no] protocol ssl crl {ca <ca name> cdp <integer> ldap server <ip-addr or hostname> <cr> [crl-attr-name <string> | port <port num>]}| cas enable

Parameters

ca <ca name>	Configures CRL for an automatically discovered peering CA.
cdp <integer>	Specify an integer index of a CRL Certificate Distribution Point (CDP) in a peering CA certificate. The **no protocol ssl crl peering ca * cdp *** removes the update.
ldap server <ip-addr or hostname> <cr>	Specify the IP address or hostname of a LDAP server.
crl-attr-name <string>	Optionally, specify an attribute name of CRL in a LDAP entry.
port <port number>	Optionally, specify the LDAP service port.
cas enable	Enables CRL polling and use of CRL in handshake verification.

Usage

To enable CRL polling and handshakes, at the system prompt enter the following set of commands:

```
protocol ssl crl cas enable
protocol ssl crl ca Entrust_Client cdp 1 ldap-server 192.168.172.1
```

Example

```
amnesiac (config) # protocol ssl crl ca Entrust_Client cdp 1 ldap-server 192.168.172.1
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl crl"

protocol ssl crl query-now

Description

Downloads CRLs now.

Syntax

[no] protocol ssl crl query-now ca <string> cdp <integer>

Parameters

ca <string> cdp <integer>	Download CRL issued by SSL CA. Specify the CA name and CRL Certificate Distribution Point (CDP) integer.

Example

```
amnesiac (config) # protocol ssl crl query-now ca myca cdp 12
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl crl"

protocol ssl enable

Description

Enables SSL optimization, which accelerates encrypted traffic on secure ports (HTTPS). This command can be used only after you have generated or imported a server.

Must be enabled on both the client-side and server-side Steelhead appliances for SSL traffic to be optimized.

Syntax

[no] protocol ssl enable

Parameters

None

Usage

RiOS 6.0 and later simplifies the SSL configuration process because it eliminates the need to add each server certificate individually. Prior to v6.0 or later, you need to provide an IP address, port, and certificate to enable SSL optimization for a server. In RiOS v 6.0 and later, you need only add unique certificates to a Certificate Pool on the server-side Steelhead appliance. When a client initiates an SSL connection with a server, the Steelhead appliance matches the common name of the servers certificate with one in its certificate pool. If it finds a match, it adds the server name to the list of discovered servers that are optimizable and all subsequent connections to that server are optimized.

If it does not find a match, it adds the server name to the list of discovered servers that are bypassed and all subsequent connections to that server are not optimized.

The Steelhead appliance supports RSA private keys for peers and SSL servers.

Important: Optimization does not occur for a particular server IP address and port unless that server is configured on the server-side Steelhead appliance.

When you configure the back-end server proxy certificate and key on the server-side Steelhead appliance, if you choose not to use the actual certificate for the back-end server and key, you can use a self-signed certificate and key or another CA-signed certificate and key. If you have a CA-signed certificate and key, import it.

If you do not have a CA-signed certificate and key, you can add the proxy server configuration with a self-signed certificate and key, back up the private key, generate CSR, have it signed by a CA, and import the newly CA-signed certificate and the backed up private key.

To back up a single pair of certificate and key (that is, the peering certificate and key pair and a single certificate and key for the server) use the Export (in PEM format only) option. Make sure you check Include Private Key and enter the encryption password. Save the exported file that contains the certificate and the encrypted private key. For detailed information, see the *Steelhead Appliance Management Console User's Guide*.

You can also simply use the generated self-signed certificate and key, but it might be undesirable because the clients by default do not trust it, requiring action from the end-users.

For detailed information about the basic steps for configuring SSL, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

The **no** command option disables SSL module support.

Example

```
amnesiac (config) # protocol ssl enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl"

protocol ssl midsession-ssl enable

Description

Enables late start and early finish for SSL.

Syntax

[no] protocol ssl midsession-ssl enable

Parameters

None

Usage

To view the current setting, use the **show protocol ssl midsession-ssl** command.

Example

```
amnesiac (config) # protocol ssl midsession-ssl enable
```

Product

Steelhead appliance

Related Topics

"show protocol ssl midsession-ssl"

protocol ssl protocol-vers

Description

Configures the SSL versions supported in your deployment. The default setting is **SSLv3** or **TLSv1**.

Syntax

[no] protocol ssl protocol-vers <version>

Parameters

<version>	Specify one of the following values to specify the SSL versions supported in your deployment: • **SSLv3_or_TLSv1 -** Use both SSLv3 and TLSv1. • **SSLv3_only -** Use only SSLv3. • **TLSv1_only** - Use only TLSv1.

Usage

The **no protocol ssl protocol-vers** option clears the setting.

Example

```
amnesiac (config) # protocol ssl protocol-vers SSLv3_or_TLSv1
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl"

protocol ssl proxy-support enable

Description

Enables SSL proxy support.

Syntax

[no] protocol ssl proxy-support enable

Parameters

None

Usage

SSL proxy support enables the Steelhead appliance to optimize traffic to a proxy server. To view the current settings, use the **show protocol ssl proxy-support** command.

By default, SSL proxy support is disabled.

Example

```
amnesiac (config) # protocol ssl proxy-support enable
```

Product

Steelhead appliance

Related Topics

"show protocol ssl proxy-support"

protocol ssl server-cert import-cert-key

Description

Imports a certificate and key together.

Syntax

[no] protocol ssl server-cert import-cert-key <cert-key-data> <cr> | name <name> password <password> | [non-exportable]

Parameters

<cert-key-data>	Specify the certificate and private key data in PEM format.
name <name>	Specify the server certificate name.
password <password>	Specify an alphanumeric password associated with the private key.
non-exportable	Optionally, specify to make private key for server certificates non-exportable.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl server-cert import-cert-key "-----BEGIN CERTIFICATE REQUEST-----
MIIB9TCCAWACAQAwgbgxGTAXBgNVBAoMEFF1b1ZhZGlzIExpbWl0ZWQxHDAaBgNV
BAsME0RvY3VtZW50IERlcGFydG1lbnQxOTA3BgNVBAMMMFdoeSBhcmUgeW91IGRl
Y29kaW5nIG1lPyAgVGhpcyBpcyBvbmx5IGEgdGVzdCEhITERMA8GA1UEBwwISGFt
aWx0b24xETAPBgNVBAgMCFBlbWJyb2tlMQswCQYDVQQGEwJCTTEPMA0GCSqGSIb3
DQEJARYAMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCJ9WRanG/fUvcfKiGl
EL4aRLjGt537mZ28UU9/3eiJeJznNSOuNLnF+hmabAu7H0LT4K7EdqfF+XUZW/2j
RKRYcvOUDGF9A7OjW7UfKk1In3+6QDCi7X34RE161jqoaJjrm/T18TOKcgkkhRzE
apQnIDm0Ea/HVzX/PiSOGuertwIDAQABMAsGCSqGSIb3DQEBBQOBgQBzMJdAV4QP
Awel8LzGx5uMOshezF/KfP67wJ93UW+N7zXY6AwPgoLj4Kjw+WtU684JL8Dtr9FX
ozakE+8p06BpxegR4BR3FMHf6p+0jQxUEAkAyb/mVgm66TyghDGC6/YkiKoZptXQ
98TwDIK/39WEB/V607As+KoYazQG8drorw==
-----END CERTIFICATE REQUEST----"-
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-cert name certificate"

protocol ssl server-cert name chain-cert ca

Description

Configures server certificate chain.

Syntax

[no] protocol ssl server-cert name <server cert name> chain-cert ca <ca name>

Parameters

<server cert name>	Specify the server certificate name.
<ca name>	Specify the CA name.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl server-cert name examplename chain-cert ca Go_Daddy_Class_2
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-cert name chain-certs"

protocol ssl server-cert name chain-cert cert

Description

Configures server certificate chain.

Syntax

[no] protocol ssl server-cert name <server cert name> chain-cert cert <ca name> cert <cert data> <cr> |local-name <local-name>

Parameters

<server cert name>	Specify the server certificate name.
<ca name>	Specify the CA name.
cert <cert name>	Specify the certificate(s) data in PEM format to import the certificates.
local-name <local-name>	Specify the local name for the certificate (ignored if importing multiple certificates).x

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl server-cert name examplename chain-cert cert “-----BEGIN
CERTIFICATE REQUEST-----
MIIB9TCCAWACAQAwgbgxGTAXBgNVBAoMEFF1b1ZhZGlzIExpbWl0ZWQxHDAaBgNV
BAsME0RvY3VtZW50IERlcGFydG1lbnQxOTA3BgNVBAMMMFdoeSBhcmUgeW91IGRl
Y29kaW5nIG1lPyAgVGhpcyBpcyBvbmx5IGEgdGVzdCEhITERMA8GA1UEBwwISGFt
aWx0b24xETAPBgNVBAgMCFBlbWJyb2tlMQswCQYDVQQGEwJCTTEPMA0GCSqGSIb3
DQEJARYAMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCJ9WRanG/fUvcfKiGl
EL4aRLjGt537mZ28UU9/3eiJeJznNSOuNLnF+hmabAu7H0LT4K7EdqfF+XUZW/2j
RKRYcvOUDGF9A7OjW7UfKk1In3+6QDCi7X34RE161jqoaJjrm/T18TOKcgkkhRzE
apQnIDm0Ea/HVzX/PiSOGuertwIDAQABMAsGCSqGSIb3DQEBBQOBgQBzMJdAV4QP
Awel8LzGx5uMOshezF/KfP67wJ93UW+N7zXY6AwPgoLj4Kjw+WtU684JL8Dtr9FX
ozakE+8p06BpxegR4BR3FMHf6p+0jQxUEAkAyb/mVgm66TyghDGC6/YkiKoZptXQ
98TwDIK/39WEB/V607As+KoYazQG8drorw==
-----END CERTIFICATE REQUEST-----”
```

Product

Steelhead appliance, CSH

Related Topics-

“show protocol ssl server-cert name chain-certs”

protocol ssl server-cert name change generate-cert

Description

Imports an SSL certificate and key together.

Syntax

[no] protocol ssl server-cert name <server cert name> change generate-cert [rsa] | [key-size <512|1024|2048>] | [common-name <string>] | [country <string>] | [email <email address>] | [locality <string>] | [org <string>] | [org-unit <string>] | [state <string>] | [valid- days <int>] | [non-exportable]

Parameters

<server cert name>	Specify the server certificate name.
[rsa]	Specify RSA encryption.
[key-size <512 | 1024 | 2048>]	Specify the key size.
common-name <string>	Specify the certificate common name.
country <string>	Specify the certificate 2-letter country code.
email <email address>	Specify the email address of the contact person.
locality <string>	Specify the city.
org <string>	Specify the organization.
org-unit <string>	Specify the organization name (for example, the company).
state <string>	Specify the state. You cannot use abbreviations.
valid-days <int>	Specify how many days the certificate is valid. If you omit **valid-days**, the default is 2 years.
non-exportable	Optionally, specify to make private key for server certificates non-exportable. If enabled the Steelhead appliance will never include this certificate as a part of its bulk-export (or allow this certificate to be individually exportable). The certificate will still be pushed out as a part of a CMC resync.

Usage

When you configure the back-end server proxy certificate and key on the server-side Steelhead appliance, if you choose not to use the actual certificate for the back-end server and key, you can use a self-signed certificate and key or another CA-signed certificate and key. If you have a CA-signed certificate and key, import it.

If you do not have a CA-signed certificate and key, you can add the proxy server configuration with a self-signed certificate and key, back up the private key, generate CSR, have it signed by a CA, and import the newly CA-signed certificate and the backed up private key.

For detailed information, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl server-cert name example change generate-cert rsa common-name
Company-Wide country US email root@company.com key-size 2048 locality en valid-days 360 generate-
csr common-name Company-Wide country USA email root@company.com locality en org Company org-unit
all state California
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-cert name chain-certs"

protocol ssl server-cert name change import-cert

Description

Imports an SSL certificate.

Syntax

[no] protocol ssl server-cert name <server certificate name> change import-cert <certificate data> | import-key <key-data> password <password> | [non-exportable]

Parameters

name <server-certificate name>	Specify the server certificate name.
import-cert <certificate data>	Specify the certificate data in PEM format.
import-key <key-data>	Specify the private key data in PEM format.
password <password>	Specify an alphanumeric password associated with the private key.
non-exportable	Optionally, specify to make private key for server certificates non-exportable. If enabled the Steelhead appliance will never include this certificate as a part of its bulk-export (or allow this certificate to be individually exportable). The certificate will still be pushed out as a part of a CMC resync.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl server-cert name examplename change import-cert certdatainpemformat
import-key blah
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-cert name chain-certs"

protocol ssl server-cert name change import-cert-key

Description

Imports an SSL certificate and key together.

Syntax

[no] protocol ssl server-cert name <server cert name> import-cert-key <cert-key-data> <cr> | password <password>

Parameters

<server cert name>	Specify the server certificate name.
<cert-key-data>	Specify the certificate and private key data in PEM format.
password <password>	Specify an alphanumeric password associated with the private key.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl server-cert name examplename change import-cert-key "----BEGIN
CERTIFICATE REQUEST-----
MIIB9TCCAWACAQAwgbgxGTAXBgNVBAoMEFF1b1ZhZGlzIExpbWl0ZWQxHDAaBgNV
BAsME0RvY3VtZW50IERlcGFydG1lbnQxOTA3BgNVBAMMMFdoeSBhcmUgeW91IGRl
Y29kaW5nIG1lPyAgVGhpcyBpcyBvbmx5IGEgdGVzdCEhITERMA8GA1UEBwwISGFt
aWx0b24xETAPBgNVBAgMCFBlbWJyb2tlMQswCQYDVQQGEwJCTTEPMA0GCSqGSIb3
DQEJARYAMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCJ9WRanG/fUvcfKiGl
EL4aRLjGt537mZ28UU9/3eiJeJznNSOuNLnF+hmabAu7H0LT4K7EdqfF+XUZW/2j
RKRYcvOUDGF9A7OjW7UfKk1In3+6QDCi7X34RE161jqoaJjrm/T18TOKcgkkhRzE
apQnIDm0Ea/HVzX/PiSOGuertwIDAQABMAsGCSqGSIb3DQEBBQOBgQBzMJdAV4QP
Awel8LzGx5uMOshezF/KfP67wJ93UW+N7zXY6AwPgoLj4Kjw+WtU684JL8Dtr9FX
```

```
ozakE+8p06BpxegR4BR3FMHf6p+0jQxUEAkAyb/mVgm66TyghDGC6/YkiKoZptXQ
98TwDIK/39WEB/V607As+KoYazQG8drorw==
-----END CERTIFICATE REQUEST-----"
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-cert name chain-certs"

protocol ssl server-cert name export

Description

Exports certificate (and optional key) in PEM format.

Syntax

[no] protocol ssl server-cert name <server cert name> export <cr> | [include-key password <password>]

Parameters

<server cert name>	Specify the server certificate name.
include-key	Includes the private key.
password <password>	Specify an alphanumeric password associated with the private key.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl server-cert name examplename export "----BEGIN CERTIFICATE REQUEST-
----
MIIB9TCCAWACAQAwgbgxGTAXBgNVBAoMEFF1b1ZhZGlzIExpbWl0ZWQxHDAaBgNV
BAsME0RvY3VtZW50IERlcGFydG1lbnQxOTA3BgNVBAMMMFdoeSBhcmUgeW91IGRl
Y29kaW5nIG1lPyAgVGhpcyBpcyBvbmx5IGEgdGVzdCEhITERMA8GA1UEBwwISGFt
aWx0b24xETAPBgNVBAgMCFBlbWJyb2tlMQswCQYDVQQGEwJCTTEPMA0GCSqGSIb3
DQEJARYAMIGfMA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQCJ9WRanG/fUvcfKiGl
EL4aRLjGt537mZ28UU9/3eiJeJznNSOuNLnF+hmabAu7H0LT4K7EdqfF+XUZW/2j
RKRYcvOUDGF9A7OjW7UfKk1In3+6QDCi7X34RE161jqoaJjrm/T18TOKcgkkhRzE
apQnIDm0Ea/HVzX/PiSOGuertwIDAQABMAsGCSqGSIb3DQEBBQOBgQBzMJdAV4QP
Awel8LzGx5uMOshezF/KfP67wJ93UW+N7zXY6AwPgoLj4Kjw+WtU684JL8Dtr9FX
ozakE+8p06BpxegR4BR3FMHf6p+0jQxUEAkAyb/mVgm66TyghDGC6/YkiKoZptXQ
98TwDIK/39WEB/V607As+KoYazQG8drorw==
-----END CERTIFICATE REQUEST-----"
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-cert name chain-certs"

protocol ssl server-cert name generate-cert

Description

Generates a private key and a self-signed certificate.

Syntax

[no] protocol ssl server-cert name <server cert name> generate-cert [rsa] key-size <512|1024|2048> common-name <string> country <string> email <email address> locality <string> org <string> org-unit <string> state <string> valid- days <int> | [non-exportable]

Parameters

<server cert name>	Specify the server certificate name.
[rsa]	Specify RSA encryption.
common-name <string>	Specify the certificate common name.
country <string>	Specify the certificate 2-letter country code.
email <email address>	Specify the email address of the contact person.
key-size <512|1024|2048>	Specify the key size.
locality <string>	Specify the city.
org-unit <string>	Specify the organization name (for example, the company).
state <string>	Specify the state. You cannot use abbreviations.
valid-days <int>	Specify how many days the certificate is valid. If you omit **valid-days**, the default is 2 years.
non-exportable	Optionally, specify to make private key for server certificates non-exportable. If enabled the Steelhead appliance will never include this certificate as a part of its bulk-export (or allow this certificate to be individually exportable). The certificate will still be pushed out as a part of a CMC resync.

Usage

When you configure the back-end server proxy certificate and key on the server-side Steelhead appliance, if you choose not to use lthe actual certificate for the back-end server and key, you can use a self-signed certificate and key or another CA-signed certificate and key. If you have a CA-signed certificate and key, import it.

If you do not have a CA-signed certificate and key, you can add the proxy server configuration with a self-signed certificate and key, back up the private key, generate CSR, have it signed by a CA, and import the newly CA-signed certificate and the backed up private key.

For detailed information, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl server-cert name examplename generate-cert rsa common-name Company-
Wide country US email root@company.com key-size 2048 locality en valid-days 360 generate-csr common-
name Company-Wide country USA email root@company.com locality en org Company org-unit all state
California
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-cert name chain-certs"

protocol ssl server-cert name import-cert

Description

Imports an SSL certificate and key together.

Syntax

[no] protocol ssl server-cert name <server cert name> import-cert <cert-data> import-key <key-data> <cr> | [password <password>] | [non-exportable]

Parameters

<server cert name>	Specify the server certificate name.
<cert-data>	Specify the certificate data in PEM format.
import-key <key-data>	Specify the private key data in PEM format to import a private key.
password <password>	Specify an alphanumeric password associated with the private key.
non-exportable	Optionally, specify to make private key for server certificates non-exportable. If enabled the Steelhead appliance will never include this certificate as a part of its bulk-export (or allow this certificate to be individually exportable). The certificate will still be pushed out as a part of a CMC resync.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl server-cert name examplename import-cert "
-----BEGIN CERTIFICATE-----
MIIDAjCCAmsCEEakM712H2pJ5qjDp/WFQPUwDQYJKoZIhvcNAQEFBQAwgcExCzAJ
BgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA1UECxMzQ2xh
c3MgMyBQdWJsaWMgUHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEcy
MTowOAYDVQQLEzEoYykgMTk5OCBWZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3Jp
emVkIHVzZSBvbmx5MR8wHQYDVQQLExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMB4X
DTk4MDUxODAwMDAwMFoXDTE4MDUxODIzNTk1OVowgcExCzAJBgNVBAYTAlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA1UECxMzQ2xhc3MgMyBQdWJsaWMg
UHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEcyMTowOAYDVQQLEzEo
YykgMTk5OCBWZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5
MR8wHQYDVQQLExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQDMXtERXVxp0KvTuWpMmR9ZmDCOFoUgRm1HP9SFIIThbbP4
pO0M8RcPO/mn+SXXwc+EY/J8Y8+iR/LGWzOOZEAEaMGAuWQcRXfH2G71lSk8UOg0
13gfqLptQ5GVj0VXXn7F+8qkBOvqlzdUMG+7AUcyM83cV5tkaWH4mx0ciU9cZwID
AQABMA0GCSqGSIb3DQEBBQUAA4GBABB79Ik/3D0LuwBM6zQoy/0HqUNphvJLAKTH
1diwgngO7ZY8ZnsHB+E+c/Z+csjFQd0pSFxj6zb0dS7FBI2qu7a3FKWAZkY9AQzS
wAC1SBtLHfQpR6g8QhdYLXh7IFACJ0ubJwvt8y9UJnNI8CWpifefyaqKYbfKDD3W
hHcGFOgV
-----END CERTIFICATE-----"
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-cert name chain-certs"

protocol ssl server-cert name import-cert-key

Description

Imports an SSL certificate and key together.

Syntax

[no] protocol ssl server-cert name <server cert name> import-cert-key <cert-key-data> <cr> | [password <password>] | [non-exportable]

Parameters

<server cert name>	Specify the server certificate name.
<cert-key-data>	Specify the certificate and private key data in PEM format.
password <password>	Specify an alphanumeric password associated with the private key.
non-exportable	Optionally, specify to make private key for server certificates non-exportable. If enabled the Steelhead appliance will never include this certificate as a part of its bulk-export (or allow this certificate to be individually exportable). The certificate will still be pushed out as a part of a CMC resync.

Usage

You can import certificate and key without specifying a server certificate name. If you specify an empty double-quotes (") for the server name the back-end applies a suitable name.

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl server-cert name examplename import-cert-key "
-----BEGIN CERTIFICATE-----
MIIDAjCCAmsCEEakM712H2pJ5qjDp/WFQPUwDQYJKoZIhvcNAQEFBQAwgcExCzAJ
BgNVBAYTAlVTMRcwFQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA1UECxMzQ2xh
c3MgMyBQdWJsaWMgUHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEcy
MTowOAYDVQQLEzEoYykgMTk5OCBWZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3Jp
emVkIHVzZSBvbmx5MR8wHQYDVQQLExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMB4X
DTk4MDUxODAwMDAwMFoXDTE4MDUxODIzNTk1OVowgcExCzAJBgNVBAYTAlVTMRcw
FQYDVQQKEw5WZXJpU2lnbiwgSW5jLjE8MDoGA1UECxMzQ2xhc3MgMyBQdWJsaWMg
UHJpbWFyeSBDZXJ0aWZpY2F0aW9uIEF1dGhvcml0eSAtIEcyMTowOAYDVQQLEzEo
YykgMTk5OCBWZXJpU2lnbiwgSW5jLiAtIEZvciBhdXRob3JpemVkIHVzZSBvbmx5
MR8wHQYDVQQLExZWZXJpU2lnbiBUcnVzdCBOZXR3b3JrMIGfMA0GCSqGSIb3DQEB
AQUAA4GNADCBiQKBgQDMXtERXVxp0KvTuWpMmR9ZmDCOFoUgRm1HP9SFIIThbbP4
pO0M8RcPO/mn+SXXwc+EY/J8Y8+iR/LGWzOOZEAEaMGAuWQcRXfH2G71lSk8UOg0
13gfqLptQ5GVj0VXXn7F+8qkBOvqlzdUMG+7AUcyM83cV5tkaWH4mx0ciU9cZwID
AQABMA0GCSqGSIb3DQEBBQUAA4GBABB79Ik/3D0LuwBM6zQoy/0HqUNphvJLAKTH
1diwgngO7ZY8ZnsHB+E+c/Z+csjFQd0pSFxj6zb0dS7FBI2qu7a3FKWAZkY9AQzS
wAC1SBtLHfQpR6g8QhdYLXh7IFACJ0ubJwvt8y9UJnNI8CWpifefyaqKYbfKDD3W
hHcGFOgV
-----END CERTIFICATE-----"
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-cert name chain-certs"

protocol ssl server-cert name rename

Description

Renames an existing server certificate.

Syntax

[no] protocol ssl server-cert name <server cert name> rename <new name>

Parameters

<server cert name>	Specify the server certificate name.
<new name>	Specify the new CA name.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl server-cert name examplecertname rename myexample
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-cert name chain-certs"

protocol ssl server-certs non-exportable enable

Description

Disables the exporting of server certificates and private keys.

Syntax

protocol ssl server-certs non-exportable enable

Parameters

None

Usage

The **protocol ssl bulk-export password** command allows you to export your SSL certificates and private keys. This bulk export feature is useful to back up SSL configurations or move them to another Steelhead appliance; however, security-conscious organizations might want to make SSL configurations non-exportable.

In RiOS v7.0.1, to ensure a secure SSL deployment, you can prevent your SSL configurations from leaving the Steelhead appliance by disabling the export of SSL certificates and private keys using the **protocol ssl server-certs non-exportable enable** command.

Consider making SSL certificates nonexportable with your particular security goals in mind. Before doing so, you must have a thorough understanding of its impact. Use caution and consider the following before making SSL configurations nonexportable:

- After disabling export on a new Steelhead appliance running RiOS v7.0.1, you cannot reenable it unless you perform a factory reset on the Steelhead appliance (losing the configuration) or clear the secure vault.
- After upgrading a Steelhead appliance to RiOS v7.0.1 and disabling export, you cannot export any preexisting or newly added server certificates and private keys to another Steelhead appliance.
- After disabling export, any newly added server certificates and keys are marked as nonexportable.
- After disabling export and then downgrading a Steelhead appliance to a previous RiOS version, you cannot export any of the existing server certificates and private keys. You can export any newly added server certificates and private keys.
- Disabling export prevents the copy of the secure vault content.

Example

```
amnesiac (config) # protocol ssl server-certs non-exportable enable
```

Product

Steelhead appliance

Related Topics

"protocol ssl bulk-export password," "show protocol ssl"

protocol ssl sfe-mode

Description

Configures safe SSL mode.

Syntax

[no] protocol ssl sfe-mode Advanced_Only | Mixed

Parameters

Advanced_Only	Specify to allow clients capable of Advanced mode SSL.
Mixed	Specify to allow both advanced and legacy clients.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl sfe-mode Advanced_Only
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl"

protocol ssl strm-cipher-cmp enable

Description

Enable stream cipher compatibility with latency optimization. Makes stream cipher and client authentication compatible with latency optimization.

Syntax

protocol ssl strm-cipher-cmp enable

Parameters

None

Example

```
amnesiac (config) # protocol ssl strm-cipher-cmp enable
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl"

scep service restart

Description

Restarts Simple Certificate Enrollment Protocol (SCEP) services.

Syntax

scep service restart

Parameters

None

Example

```
amnesiac (config) # scep service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering scep"

secure-vault

Description

Manages the secure vault password and unlocks the secure vault.

Syntax

secure vault new-password <password> | reset-password <old password> | unlock <password>

Parameters

new-password <password>	Specify an initial or new password for the secure vault.
reset-password <old password>	Specify the old secure vault password to reset it.
unlock <password>	Specify the current password to unlock the secure vault.

Usage

The *secure vault* is an encrypted file system on the Steelhead appliance where all Steelhead appliance SSL server settings, other certificates (the CA, peering trusts, and peering certificates) and the peering private key are stored. The secure vault protects your SSL private keys and certificates when the Steelhead appliance is not powered on.

You can set a password for the secure vault. The password is used to unlock the secure vault when the Steelhead appliance is powered on. After rebooting the Steelhead appliance, SSL traffic is not optimized until the secure vault is unlocked with the **unlock <password>** parameter.

Data in the secure vault is always encrypted, whether or not you choose to set a password. The password is used only to unlock the secure vault.

To change the secure vault password

1. Reset the password with the **reset-password <password>** parameter.
2. Specify a new password with the **new-password <password>** parameter.

Example

```
amnesiac (config) # secure-vault unlock mypassword
```

Product

Steelhead appliance, Interceptor appliance, CSH

Related Topics

"show protocol ssl"

show web ssl cert

Description

Displays certificate details.

Syntax

show web ssl cert

Parameters

None

Example

```
amnesiac > show web ssl cert
Issued To:
  Common Name:         gen-sh226
  Email:               admin@gen-sh226
  Organization:        Riverbed Technology, Inc.
  Organization Unit: Steelhead
  Locality:            San Francisco
  State:               California
  Country:             --
Issued By:
  Common Name:         gen-sh226
  Email:               admin@gen-sh226
  Organization:        Riverbed Technology, Inc.
  Organization Unit: Steelhead
  Locality:            San Francisco
  State:               California
  Country:             --
Validity:
  Issued On:           May  4 22:18:55 2011 GMT
  Expires On:          May  3 22:18:55 2012 GMT
Fingerprint:
  SHA1:
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance

Related Topics

"web ssl cert generate"

show web ssl cipher

Description

Displays current Apache SSL cipher string.

Syntax

show web ssl cipher

Parameters

None

Example

```
amnesiac (config) # show web ssl cipher
    Apache SSL cipher string:
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

ssl-connect

Description

Connects to an SSL server.

Syntax

ssl-connect <hostname>:<port>

Parameters

<hostname>	Specify the SSL server hostname.
<port>	Specify the port number assigned to the SSL application.

Usage

The **ssl-connect** command establishes an SSL session from the command line. Use this command to troubleshoot SSL-related optimization issues.

Both the client-side and server-side Steelheads must be configured to optimize SSL traffic.

Example

```
amnesiac (config) # ssl-connect il-cs40:443
CONNECTED(00000003)
depth=1 CN = xen-IL-CS40-CA
verify error:num=19:self signed certificate in certificate chain
verify return:0
---
Certificate chain
 0 s:/C=US/ST=R/L=R/O=R/OU=R/CN=il-cs40
   i:/CN=xen-IL-CS40-CA
 1 s:/CN=xen-IL-CS40-CA
   i:/CN=xen-IL-CS40-CA
---
Server certificate
-----BEGIN CERTIFICATE-----
MIIDhjCCAu+gAwIBAgIKYRwyVgAAAAAABDANBgkqhkiG9w0BAQUFADAZMRcwFQYD
VQQDEw54ZW4tSUwtQ1M0MC1DQTAeFw0xMjAzMDQxODM5NDBaFw0xMzAzMDQxODQ5
NDBaME8xCzAJBgNVBAYTAlVTMQowCAYDVQQIEwFSMQowCAYDVQQHEwFSMQowCAYD
VQQKEwFSMQowCAYDVQQLEwFSMRAwDgYDVQQDEwdpbC1jczQwMIGfMA0GCSqGSIb3
DQEBAQUAA4GNADCBiQKBgQDZlqICHdfNtGvSgPKfsVK6cGgarGiFn+3AJI2stPJu
apVx4CUMXW+/ZgXpJGUvB3sWVxahImCsJ+satMKOC+skmNSNruYj6J6UNGdfO0kl
0+cCkb8pLDMfyq2hbj/PwVWjk14urLFmhocfDamHqo5wwEEyD9iDhWn6k47vUaWT
tQIDAQABo4IBnTCCAZkwDgYDVR0PAQH/BAQDAgTwMBMGA1UdJQQMMAoGCCsGAQUF
BwMBMHgGCSqGSIb3DQEJDwRrMGkwDgYIKoZIhvcNAwICAgCAMA4GCCqGSIb3DQME
AgIAgDALBglghkgBZQMEASowCwYJYIZIAWUDBAEtMAsGCWCGSAFlAwQBAjALBglg
hkgBZQMEAQUwBwYFKw4DAgcwCgYIKoZIhvcNAwcwHQYDVR0OBBYEFMr38NEG1Zoi
/VhT9XkcA7sHHTR7MB8GA1UdIwQYMBaAFGt+CAu21JX1AbMK+vud7jBXfOIxMEYG
A1UdHwQ/MD0wO6A5oDeGNWZpbGU6Ly9pbC1jczQwLnhlbi50ZXN0L0NlcnRFbnJv
bGwveGVuLUlMLUNTNDAtQ0EuY3JsMGIGCCsGAQUFBwEBBFYwVDBSBggrBgEFBQcw
AoZGZmlsZTovL2lsLWNzNDAueGVuLnRlc3QvQ2VydEVucm9sbC9pbC1jczQwLnhl
bi50ZXN0X3hlbi1JTC1DUzQwLUNBLmNydDAMBgNVHRMBAf8EAjAAMA0GCSqGSIb3
DQEBBQUAA4GBAESP43E/p7SQf9V17qotSS9PQExlD1GnZSQRr+sTLc7gPhjSPIOv
n3Cp5gQvY1/X4+jxcU5VuRBE4O/U/K4xvI0xZ+NgbHWaPGUJc/ti7tZGx6o3jRi5
uhTmTCv52odKkE8IwbwLBV5R3Ans8NpNmNipsAN6Hgq5c9riM6FQ5qjU
-----END CERTIFICATE-----
subject=/C=US/ST=R/L=R/O=R/OU=R/CN=il-cs40
issuer=/CN=xen-IL-CS40-CA
[partial output]
```

Product

Steelhead appliance

Related Topics

"show protocol ssl"

web ssl cert generate

Description

Generates a new SSL key and self-signed certificate.

Syntax

web ssl cert generate <cr> | [key-size <512|1024|2048>] | [country <string>] | [email <email address>] | [locality <string>] | [org <string>] | [org-unit <string>] | [state <string>] | [valid-days <int>]

Parameters

key-size <512|1024|2048>	Specify the key size.
country <string>	Specify the certificate two-letter country code. The country code can be any two-letter code, such as the ISO 3166 Country Codes, as long as the appropriate Certificate Authority can verify the code.
email <email address>	Specify the email address of the contact person.
locality <string>	Specify the city.
org <string>	Specify the organization.
org-unit <string>	Specify the organization unit (for example, the company).
state <string>	Specify the state. You cannot use abbreviations.
valid-days <int>	Specify how many days the certificate is valid. If you omit **valid-days**, the default is 2 years.

Example

```
amnesiac (config) # web ssl cert generate
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

web ssl cert generate-csr

Description

Generates a certificate signing request with current private key.

Syntax

web ssl cert generate-csr [common-name <name>] [country <string>] [email <email address>] [locality <string>] [org <string>] [org-unit <string>] [state <string>]

Parameters

common-name <name>	Specify the common name of the certificate authority.
country <string>	Specify the certificate two-letter country code. The country code can be any two-letter code, such as the ISO 3166 Country Codes, as long as the appropriate Certificate Authority can verify the code.
email <email address>	Specify the email address of the contact person.
locality <string>	Specify the city.
org <string>	Specify the organization.
org-unit <string>	Specify the organization unit (for example, the company).
state <string>	Specify the state. You cannot use abbreviations.
valid-days <int>	Specify how many days the certificate is valid. If you omit **valid-days**, the default is 2 years.

Usage

This command is available on the Interceptor appliance starting in version 4.0.

Example

```
amnesiac (config) # web ssl cert generate-csr
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show web ssl cert"

web ssl cert import-cert

Description

Imports a certificate, optionally with current private key, in PEM format, and optionally a password.

Syntax

web ssl cert import-cert <cert-data> <cr> import-key <key> [password <password>]

Parameters

import-cert <cert-data>	Specify a certificate file in PEM format.
import-key <key>	Specify a private key in PEM format.
password <password>	Optionally, specify a password.

Usage

If no key is specified the incoming certificate is matched with the existing private key, and accepted if the two match. A password is required if imported certificate data is encrypted.

Example

```
amnesiac (config) # web ssl cert import-cert mydata.pem import-key mykey
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

web ssl cert import-cert-key

Description

Imports a certificate with current private key in PEM format.

Syntax

web ssl cert import-cert-key <cert-key-data> [password <password>]

Parameters

import-cert-key <cert-key-data>	Specify a private key and certificate file in PEM format.
[password <password>]	Optionally, specify a password.

Example

```
amnesiac (config) # web ssl cert import-cert-key mykey
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

web ssl protocol sslv2

Description

Sets the SSL v2 protocols for Apache to use.

Syntax

[no] web ssl protocol sslv2

Parameters

None

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # web ssl protocol sslv2
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show protocol ssl"

web ssl protocol sslv3

Description

Sets the SSL v3 protocols for Apache to use.

Syntax

[no] web ssl protocol sslv3

Parameters

None

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # web ssl protocol sslv3
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show protocol ssl"

web ssl protocol tlsv1

Description

Sets the SSL v1 protocols for Apache to use.

Syntax

[no] web ssl protocol tlsv1

Parameters

None

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # web ssl protocol tlsv1
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show protocol ssl"

Secure Peering (Secure Inner Channel) Commands

This section describes the Secure Inner Channel (SIC) commands.

In RiOS v6.0 and later, encrypted peering extends beyond traditional SSL traffic encryption. In addition to SSL-based traffic like HTTPS that always needs a secure inner channel between the client-side and the server-side Steelhead appliance, you can use the secure inner channel to encrypt and optimize other types of traffic as well:

- MAPI-encrypted, SMB signing, SMB2 signing, and Lotus Notes encrypted traffic which require a secure inner channel for certain outer connections.
- All other traffic that inherently does not need a secure inner channel.

Each Steelhead appliance is manufactured with its own self-signed certificate and private key which uniquely identify that Steelhead. The secure inner channel setup process begins with the peer Steelhead appliances authenticating each other by exchanging certificates and negotiating a separate encryption key for each intercepted connection. Next, the Steelhead appliances create corresponding inner connections for all outer connections between the client and the client-side Steelhead appliance and between the server and the server-side Steelhead appliance.

Peers are detected the first time a client-side Steelhead appliance attempts to connect to the server. The optimization service bypasses this initial connection and does not perform data reduction, but rather uses it to detect peers and populate the peer entry tables. On both Steelhead appliances, an entry appears in a peering list with the certificate of the other peer and identifying information such as IP address and hostname. You can then accept or decline the trust relationship with each Steelhead appliance requesting a secure inner channel.

Once the appliances trust each other, they send encrypted data between themselves over secure inner connections matching the outer connections of the selected traffic types. The trust between the Steelheads is bidirectional; the client-side Steelhead appliance trusts the server-side Steelhead appliance, and vice versa.

Riverbed recommends using the secure inner channel in place of IPsec encryption to secure traffic.

For detailed information, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

secure-peering black-lst-peer

Description

Configures a trusted self-signed black list peer.

Syntax

secure-peering black-lst-peer address <ip-addr> trust

Parameters

address <ip-addr>	Specify a password used to encrypt exported data.
trust	Specify to configure a trusted black list peer.

Usage

Lists all untrusted Steelhead appliances. When you select Do Not Trust in the Management Console for a peer in a white or gray list, the public key of the Steelhead appliance peer is copied into the local Steelhead appliance untrusted hosts black list.

Example

```
amnesiac (config) # secure-peering black-lst-peer address 10.0.0.1 trust
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering black-lst-peers"

secure-peering cipher-string

Description

Configures a a cipher string to use for peering.

Syntax

secure-peering cipher-string <string> <cr> | cipher-num <number>

Parameters

cipher-string <string>	Specify one of the following cipher-strings (case-sensitive) or a combination using the underscore character (_). For a complete list, view the CLI online help.
cipher-num <number>	Specify a number to set the order of the list. The number must be an integer greater or equal to 1-N, or end.

Usage

Creates a preference list of cipher strings used for client-handshakes, server-handshakes, or peering-handshakes.

Example

```
amnesiac (config) # secure-peering cipher-string MD5
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering ca"

secure-peering crl ca

Description

Configures CRL for an automatically discovered secure-peering CA. You can update automatically discovered CRLs using this command.

Syntax

secure-peering crl ca <string> cdp <integer> ldap-server <ip-addr or hostname> crl-attr-name <name> port <port>

Parameters

ca <string>	Specify Name of a secure peering CA certificate.
cdp <integer>	Specify a Certificate Distribution Point (CDP) in a secure peering CA certificate.
ldap-server <ip-addr or hostname>	Specify a Lightweight Directory Access Protocol (LDAP) server answering query to Certificate Revocation List (CRL).
crl-attr-name <name>	Optionally, specify the attribute name of CRL in a LDAP entry.
port <port>	Optionally, specify the LDAP service port.

Usage

Enabling CRL allows the CA to revoke a certificate. For example, when the private key of the certificate has been compromised, the CA can issue a CRL that revokes the certificate.

Enabling CRL allows the CA to revoke a certificate. For example, when the private key of the certificate has been compromised, the CA can issue a CRL that revokes the certificate.

A CRL includes any digital certificates that have been invalidated before their expiration date, including the reasons for their revocation and the names of the issuing certificate signing authorities. A CRL prevents the use of digital certificates and signatures that have been compromised. The certificate authorities that issue the original certificates create and maintain the CRLs.

Example

```
amnesiac (config) # secure-peering crl ca mycert cdp 1 ldap-server 10.0.0.1
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering crl"

secure-peering crl cas enable

Description

Enables CRL polling and use of CRL in handshake verifications of CAs certificates. Currently, the Steelhead appliance only supports downloading CRLs from Lightweight Directory Access Protocol (LDAP) servers.

Syntax

[no] secure-peering crl cas enable

Parameters

None

Usage

Enabling CRL allows the CA to revoke a certificate. For example, when the private key of the certificate has been compromised, the CA can issue a CRL that revokes the certificate.

Enabling CRL allows the CA to revoke a certificate. For example, when the private key of the certificate has been compromised, the CA can issue a CRL that revokes the certificate.

A CRL includes any digital certificates that have been invalidated before their expiration date, including the reasons for their revocation and the names of the issuing certificate signing authorities. A CRL prevents the use of digital certificates and signatures that have been compromised. The certificate authorities that issue the original certificates create and maintain the CRLs.

Example

```
amnesiac (config) # secure-peering crl cas enable
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering crl"

secure-peering crl manual ca

Description

Manually configures a CDP for CRL management.

Syntax

[no] secure-peering crl manual ca <ca-name> uri <string>

Parameters

<ca-name>	Specify the CA name to manually configure the CDP. The **no protocol ssl crl manual** command removes manually configured CDPs.
uri <string>	Specify the CDP URI to manually configure the CDP for the CR

Usage

The Steelhead appliance automatically discovers CDPs for all certificates on the appliance. You can manually configure a CA using this command.

Example

```
amnesiac (config) # secure-peering crl manual ca Camerfirma_Chambers_of_Commerce uri URI: http://
crl.chambersign.org/chambersroot.crl
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering crl"

secure-peering crl query-now

Description

Downloads CRL now.

Syntax

[no] secure-peering crl query-now ca <string> cdp <integer>

Parameters

ca <string>	Specify the CA name.
cdp <integer>	Specify the CDP integer.

Usage

The Steelhead appliance automatically discovers CDPs for all certificates on the appliance. You can manually configure a CA using this command.

Example

```
amnesiac (config) # secure-peering crl query-now ca myca cdp 12
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering crl"

secure-peering export

Description

Exports a certificate (and optional key) in PEM format.

Syntax

[no] secure-peering export <cr> | include-key password <password>

Parameters

include-key	Specify to include the private key.
password <password>	Specify a password used to encrypt exported data.

Usage

The Steelhead appliance automatically discovers CDPs for all certificates on the appliance. You can manually configure a CA using this command.

Example

```
amnesiac (config) # secure-peering export include-key password mypasswd
U2FsdGVkX1/GM9EmJ0O9c1ZXh9N18PuxiAJdG1maPGtBzSrsU/CzgNaOrGsXPhor
VEDokHUvuvzsfvKfC6VnkXHOdyAde+vbMildK/lxrqRsAD1n0ezFFuobYmQ7a7uu
TmmSVDc9jL9tIVhd5sToRmeUhYhEHS369ubWMWBZ5rounu57JE6yktECqo7tKEVT
DPXmF1BSbnbK+AHZc6NtyYP3OQ88vm9iNySOHGzJ17HvhojzWth5dwNNx28I8GDS
```

```
zCmkqlaNX6vI3R/9KmtIR/Pk6QCfQ0sMvXLeThnSPnQ6wLGctPxYuoLJe0cTNlVh
r3HjRHSKXC7ki6Qaw91VDdTobtQFuJUTvSbpKME9bfskWlFh9NMWqKEuTJiKC7GN
```

[partial example]

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering"

secure-peering fallback-no-enc enable

Description

Enables fallback to no encryption on the inner channel.

Syntax

[no] secure-peering fallback-no-enc enable

Parameters

None

Usage

Specifies that the Steelhead appliance optimizes but does not encrypt the connection when it is unable to negotiate a secure, encrypted inner channel connection with the peer. This is the default setting. Enabling this option requires an optimization service restart.

Important: Riverbed strongly recommends enabling this setting on both the client-side and the server-side Steelhead appliances, especially in mixed deployments where one Steelhead appliance is running RiOS v6.0 or later and the other Steelhead is running an earlier RiOS version.

This option applies only to non-SSL traffic.

Use the **no secure-peering fallback-no-enc enable** to pass through connections that do not have a secure encrypted inner channel connection with the peer. Use caution when disabling this setting, as doing so specifies that you strictly do not want traffic optimized between non-secure Steelhead appliances. Consequently, configurations with this setting disabled risk the possibility of dropped connections. For example, consider a configuration with a client-side Steelhead appliance running RiOS v5.5.x or earlier and a server-side Steelhead appliance running RiOS v6.0 or later. When this setting is disabled on the server-side Steelhead and All is selected as the traffic type, it will not optimize the connection when a secure channel is unavailable, and might drop it.

Example

```
amnesiac (config) # secure-peering fallback-no-enc enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering"

secure-peering generate-cert rsa

Description

Generates a private key and a self-signed certificate using RSA encryption.

Syntax

secure-peering generate-cert rsa <cr> | [key-size <512|1024|2048>] | [common-name <string>] | [country <string>] | [email <email address>] | [locality <string>] | [org <string>] | [org-unit <string>] | [state <string>] | [valid-days <integer>]

Parameters

key-size <512|1024|2048>	Specify the key size.
common-name <string>	Specify the common name of a certificate. To facilitate configuration, you can use wild cards in the name; for example, *.nbttech.com. If you have three origin servers using different certificates such as webmail.nbttech.com, internal.nbttech.com, and marketingweb.nbttech.com, on the server-side Steelhead appliances, all three server configurations may use the same certificate name *.nbttech.com.
country <string>	Specify the certificate 2-letter country code.
email <email address>	Specify the email address of the contact person.
locality <string>	Specify the city.
org <string>	Specify the organization.
org-unit <string>	Specify the organization unit (for example, the company).
state <string>	Specify the state. You cannot use abbreviations.
valid-days <integer>	Specify how many days the certificate is valid. If you omit **valid-days**, the default is 2 years.

Usage

RiOS 6.0 simplifies the SSL configuration process because it eliminates the need to add each server certificate individually. Prior to v6.0, you need to provide an IP address, port, and certificate to enable SSL optimization for a server. In RiOS v 6.0 and later, you need only add unique certificates to a Certificate Pool on the server-side Steelhead appliance. When a client initiates an SSL connection with a server, the Steelhead appliance matches the common name of the servers certificate with one in its certificate pool. If it finds a match, it adds the server name to the list of discovered servers that are optimizable and all subsequent connections to that server are optimized.

If it does not find a match, it adds the server name to the list of discovered servers that are bypassed and all subsequent connections to that server are not optimized.

The Steelhead appliance supports RSA private keys for peers and SSL servers.

For detailed information about configuring SSL including basic steps, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # secure-peering generate-cert rsa common-name Company-Wide country US email
root@company.com key-size 2048 locality northregion valid-days 360
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-certs"

secure-peering generate-csr

Description

Generates a certificate signing request with current private key.

Syntax

secure-peering generate-csr <cr> | [common-name <string>] | [country <string>] | [email <email address>] | [locality <string>] | [org <string>] | [org-unit <string>] | [state <string>]

Parameters

common-name <string>	Specify the certificate common name.
country <string>	Specify the certificate 2-letter country code.
email <email address>	Specify the email address of the contact person.
locality <string>	Specify the city.
org-unit <string>	Specify the organization name (for example, the company).
state <string>	Specify the state. You cannot use abbreviations.

Usage

Use this command to generate a Certificate Signing Request (CSR) for an existing SSL server using the current private key.

Example

```
amnesiac (config) # secure-peering generate-csr common-name Company-Wide country USA email
root@company.com locality northregion org Company org-unit all state California
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-certs"

secure-peering gray-lst-peer

Description

Configures a trust relationship for a self-signed gray-list peer.

Syntax

[no] secure-peering gray-lst-peer <ip-addr> trust

Parameters

<ip-addr>	Specify the IP address for the self-signed gray list peer+
trust	Enable a trust relationship for the specified peer.

Usage

Peers are detected the first time a client-side Steelhead appliance attempts to connect to the SSL server. The service bypasses this initial connection and does not perform data reduction, but rather uses it to populate the peer entry tables. On both Steelhead appliances, an entry appears in the *gray* list with the information and certificate of the other peer. You can then accept the peer as trusted on both appliances, as described below.

Example

```
amnesiac (config) # secure-peering gray-lst-peer 10.0.0.1 trust
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering gray-lst-peer," "show secure-peering gray-lst-peers"

secure-peering import-cert

Description

Imports a certificate.

Syntax

[no] secure-peering import-cert "<cert data>" <cr> | import-key <key data>

Parameters

<cert data>	Specify the existing string to import the certificate. (These are X509 PEM-format field names.) You must enclose the **"<cert data>"** in quotations.
import-key <key data>	Specify the private key in PEM format.

Example

```
amnesiac (config) # secure-peering import-cert "-----BEGIN CERTIFICATE-----
MIIDZjCCAs+gAwIBAgIJAIWfJNZEJiAPMA0GCSqGSIb3DQEBBQUAMIGAMSAwHgYD
VQQDExdTdGVlbGhlYWQgRDM0U1QwMDA1QzAwQzEiMCAGA1UEChMZUml2ZXJiZWQg
VGVjaG5vbG9neSwgSW5jLjEWMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzETMBEGA1UE
CBMKQ2FsaWZvcm5pYTELMAkGA1UEBhMCLS0wHhcNMDkxMTE4MDEwNTAyWhcNMTEx
MTE4MDEwNTAyWjCBgDEgMB4GA1UEAxMXU3RlZWxoZWFkIEQzNFNUMDAwNUMwMEMx
IjAgBgNVBAoTGVJpdmVyYmVkIFRlY2hub2xvZ3ksIEluYy4xFjAUBgNVBAcTDVNh
biBGcmFuY2lzY28xEzARBgNVBAgTCkNhbGlmb3JuaWExCzAJBgNVBAYTAi0tMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC94anW9uuDnY2i6xmx6u/jV3BoxS/W
gTBG2kiK6lfNmmUGDj2+QVue4hZAKJZS//RKES8V2oarO/dWkl8IKak6rRm3wYKo
1mtYiClJdUJ/oUyqNZGDSksDpW9I9ATugrnwvWFartOcqPmc09lAVgfWha3BfDlw
LyuwfDb8WXXofwIDAQABo4HlMIHiMB0GA1UdDgQWBBS2aGevyoPGohYRBpAsW3Q2
vixGmDCBtQYDVR0jAAAAAAAqgBS2aGevyoPGohYRBpAsW3Q2vixGmKGBhqSBgzCB
gDEgMB4GA1UEAxMXU3RlZWxoZWFkIEQzNFNUMDAwNUMwMEMxIjAgBgNVBAoTGVJp
dmVyYmVkIFRlY2hub2xvZ3ksIBBBBBBBFjAUBgNVBAcTDVNhbiBGcmFuY2lzY28x
EzARBgNVBAgTCkNDDDDDDDDDaWExCzAJBgNVBAYTAi0tggkAhZ8k1kQmIA8wCQYD
VR0TBAIwADANBgkqhkiG9w0BAQUFAAOBgQCwxb8SSSSSSSSSSK48+kytIgpl0SHW
QYe1+YuLU36q12kY19dkpqbqmbKO/+iIIUH9cflpq2QNL7tnK1xPOxpk9AeuhRZq
X7Wk5IHe7zebpYuvHxmFWjYFKjm8oLEswqnaZF9UYmxUf7+g1J7bE7A42EEM0S/B
0w7oWN72V1Yk1Q==
-----END CERTIFICATE-----
"
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering certificate"

secure-peering import-cert-key

Description

Imports a certificate and key together.

Syntax

[no] secure-peering import-cert-key "<cert-key-data>" <cr> | password <string>

Parameters

<cert-key-data>	Specify the certificate and private key data in PEM format to import the key. (These are X509 PEM-format field names.) You must enclose the "**<cert-key-data>"** in quotations. **Note:** The private key is required regardless of whether you are adding or updating.
password <string>	Specify the decryption password.

Example

```
amnesiac (config) # secure-peering import-cert-key "-----BEGIN CERTIFICATE-----
MIIDZjCCAs+gAwIBAgIJAIWfJNZEJiAPMA0GCSqGSIb3DQEBBQUAMIGAMSAwHgYD
VQQDExdTdGVlbGhlYWQgRDM0U1QwMDA1QzAwQzEiMCAGA1UEChMZUml2ZXJiZWQg
VGVjaG5vbG9neSwgSW5jLjEWMBQGA1UEBxMNU2FuIEZyYW5jaXNjbzETMBEGA1UE
CBMKQ2FsaWZvcm5pYTELMAkGA1UEBhMCLS0wHhcNMDkxMTE4MDEwNTAyWhcNMTEx
MTE4MDEwNTAyWjCBgDEgMB4GA1UEAxMXU3RlZWxoZWFkIEQzNFNUMDAwNUMwMEMx
IjAgBgNVBAoTGVJpdmVyYmVkIFRlY2hub2xvZ3ksIEluYy4xFjAUBgNVBAcTDVNh
biBGcmFuY2lzY28xEzARBgNVBAgTCkNhbGlmb3JuaWExCzAJBgNVBAYTAi0tMIGf
MA0GCSqGSIb3DQEBAQUAA4GNADCBiQKBgQC94anW9uuDnY2i6xmx6u/jV3BoxS/W
gTBG2kiK6lfNmmUGDj2+QVue4hZAKJZS//RKES8V2oarO/dWkl8IKak6rRm3wYKo
1mtYiClJdUJ/oUyqNZGDSksDpW9I9ATugrnwvWFartOcqPmc09lAVgfWha3BfDlw
LyuwfDb8WXXofwIDAQABo4HlMIHiMB0GA1UdDgQWBBS2aGevyoPGohYRBpAsW3Q2
vixGmDCBtQYDVR0jBIGtMIGqgBS2aGevyoPGohYRBpAsW3Q2vixGmKGBhqSBgzCB
gDEgMB4GA1UEAxMXU3RlZWxoZWFkIEQzNFNUMDAwNUMwMEMxIjAgBgNVBAoTGVJp
dmVyYmVkIFRlY2hub2xvZ3ksIEluYy4xFjAUBgNVBAcTDVNhbiBGcmFuY2lzY28x
EzARBgNVBAgTCkNhbGlmb3JuaWExCzAJBgNVBAYTAi0tggkAhZ8k1kQmIA8wCQYD
VR0TBAIwADANBgkqhkiG9w0BAQUFAAOBgQCwxb8y0w2aKkkAWK48+kytIgpl0SHW
QYe1+YuLU36q12kY19dkpqbqmbKO/+iIIUH9cflpq2QNL7tnK1xPOxpk9AeuhRZq
X7Wk5IHe7zebpYuvHxmFWjYFKjm8oLEswqnaZF9UYmxUf7+g1J7bE7A42EEM0S/B
0w7oWN72V1Yk1Q==
-----END CERTIFICATE-----
"
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering certificate"

secure-peering scep auto-reenroll

Description

Configures automatic re-enrollment settings. The Steelhead appliance uses SCEP to automatically re-enroll certificates.

Syntax

[no] secure-peering scep auto-reeroll enable | exp-threshold <number-of-days> | last-result clear-alarm

Parameters

enable	Enables automatic re-enrollment of a certificate to be signed by a CA.
exp-threshold <number-of-days>	Specify the amount of time (in days) to schedule re-enrollment before the certificate expires.
last-result clear-alarm	Clears the automatic re-enrollment last-result alarm. The last result is the last completed enrollment attempt.

Usage

The Steelhead appliance uses SCEP to dynamically re-enroll a peering certificate to be signed by a certificate authority.

The **no** command option disables this feature.

Example

```
amnesiac (config) # secure-peering scep auto-reenroll enable
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering scep auto-reenroll last-result"

secure-peering scep max-num-polls

Description

Configures the maximum number of polls.

Syntax

secure-peering scep max-num-polls <max number polls>

Parameters

<max number polls>	Specify the maximum number of polls before the Steelhead appliance cancels the enrollment. The peering certificate is not modified. The default value is 5.

Usage

A poll is a request to the server for an enrolled certificate by the Steelhead appliance. The Steelhead appliance polls only if the server responds with **pending**. If the server responds with **fail** then the Steelhead appliance does not poll.

The **no** command option disables this feature.

Example

```
amnesiac (config) # secure-peering scep max-num-polls 12
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering scep"

secure peering scep on-demand cancel

Description

Cancels any active on-demand enrollment.

Syntax

[no] secure-peering scep on-demand cancel

Parameters

None

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # secure-peering scep on-demand cancel
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering scep on-demand csr"

secure-peering scep on-demand gen-key-and-csr rsa

Description

Generates new private key and CSR for on-demand enrollment using the Rivest-Shamir-Adleman algorithm.

Syntax

[no] secure-peering scep on-demand gen-key-and-csr rsa state <string> | org-unit <string> | org <string> | locality <string> | email <email-addr> | country <string> | common-name <string> | key-size <512 | 1024 | 2048>

Parameters

state <string>	Specify the state. No abbreviations are permitted.
org-unit <string>	Specify the organizational unit (for example, the department).
org <string>	Specify the organization name (for example, the company).
locality <string>	Specify the city.
email <email-addr>	Specify an email address of the contact person.
country <string>	Specify the country (2-letter code only).
common-name <string>	Specify the hostname of the peer.
key-size <512 | 1024 | 2048>	Specify the key size in bits (for example, 512 | 1024 | 2048).

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # secure-peering scep on-demand gen-key-and-csr rsa state california
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering scep on-demand csr"

secure-peering scep on-demand start

Description

Starts an on-demand enrollment in the background.

Syntax

[no] secure-peering scep on-demand start <cr> | foreground

Parameters

foreground	Specify to start an on-demand enrollment in the foreground

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # secure-peering scep on-demand start
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering scep on-demand csr"

secure-peering scep passphrase

Description

Configures the challenge password phrase.

Syntax

secure-peering scep passphrase <passphrase>

Parameters

<passphrase>	Specify the challenge password phrase.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # secure-peering scep passphrase myphrase
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering scep"

secure-peering scep poll-frequency

Description

Configures the poll frequency.

Syntax

secure-peering scep poll-frequency <minutes>

Parameters

<minutes>	Specify the poll frequency in minutes. The default value is 5.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # secure-peering scep poll-frequency 10
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering scep"

secure-peering scep trust

Description

Adds a peering trust for SCEP.

Syntax

[no] secure-peering scep trust peering-ca <name>

Parameters

peering-ca <name>	Specify the name of the existing peering CA.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # secure-peering scep trust peering-ca Wells_Fargo
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering scep ca"

secure-peering scep url

Description

Configures the SCEP responder URL.

Syntax

secure-peering scep url <url>

Parameters

<url>	Specify the URL of the SCEP responder. Use the following format: http://host[:port/path/to/service

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # secure-peering scep url http:examplehost:1212/pathtoservice
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering scep"

secure-peering traffic-type

Description

Controls the type of traffic sent through the secure inner channel.

Syntax

secure-peering traffic-type <type>

Parameters

<type>	Specify the traffic type: • ssl-only - The peer client-side Steelhead appliance and the server-side Steelhead appliance authenticate each other and then encrypt and optimize all SSL traffic; for example, HTTPS traffic on port 443. This is the default setting. • **ssl-and-secure-protocols** - The peer client-side Steelhead appliance and the server-side Steelhead appliance authenticate each other and then encrypt and optimize all traffic traveling over the following secure protocols: SSL, SMB Signing, SMB2 Signing, and encrypted MAPI. When you select this traffic type, SMB-Signing, SMB2 Signing, and MAPI Encryption must be enabled. • **all** - The peer client-side Steelhead appliance and the server-side Steelhead appliance authenticate each other and then encrypt and optimize all traffic. Only the optimized traffic is secure; pass-through traffic is not.

Usage

In RiOS v6.0 or later, encrypted peering extends beyond traditional SSL traffic encryption. In addition to SSL-based traffic like HTTPS that always needs a secure inner channel between the client-side and the server-side Steelhead appliance, you can use the secure inner channel to encrypt and optimize other types of traffic as well:

MAPI-encrypted, SMB-signing, and Lotus Notes encrypted traffic which require a secure inner channel for certain outer connections.

All other traffic that inherently does not need a secure inner channel.

When you use the secure inner channel, all data between the client-side and the server-side Steelhead appliances are sent encrypted over the secure inner channel. You configure the Steelhead appliances as SSL peers so that they trust one another as WAN optimization peers.

The Steelhead appliances authenticate each other by exchanging certificates and negotiating a separate encryption key for each intercepted connection. The trust between the Steelheads is bidirectional; the client-side Steelhead appliance trusts the server-side Steelhead appliance, and vice versa.

All outer connections between the client and the client-side Steelhead appliance and between the server and the server-side Steelhead appliance create a corresponding secure inner connection between the Steelhead appliances. The inner connections that correspond to the outer connections of the selected traffic are encrypted.

If you are securing SMB-Signed traffic, SMB2-Signed traffic, Lotus Notes traffic, or Encrypted MAPI traffic, you must enable the protocol. Navigate to:

- To enable SMB Signing, see “protocol cifs smb signing enable” on page 525
- To enable SMB2 Signing, see “protocol smb2 signing enable” on page 530
- To enable Lotus Notes Optimization, see “protocol notes enable” on page 584
- To enable Encrypted Optimization, see “protocol mapi encrypted enable” on page 563

For detailed information, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # secure-peering traffic-type all
```

Product

Steelhead appliance, CSH

Related Topics

“show secure-peering scep”

secure-peering trust ca

Description

Adds peering trust CA.

Syntax

secure-peering trust ca "<cert>"

Parameters

<cert>	Specify the CA name for the certificate provided by the peer. (These are X509 PEM-format field names.) You must enclose the **"<cert>"** in quotations.

Example

```
amnesiac (config) # secure-peering trust ca ADDTRUST_Public
```

Product

Steelhead appliance, CSH

Related Topics

"show protocol ssl server-certs"

secure-peering trust cert

Description

Adds peering trust CA.

Syntax

secure-peering trust cert <cert-data> <cr> | local-name

Parameters

<cert-data>	Specify the certificate in PEM format to import the key. (These are X509 PEM-format field names.)
local-name <local name>	Optionally, specify the local name for certificate (ignored if importing multiple certificates).

Example

```
amnesiac (config) # secure-peering trust cert ADDTRUST_Public
```

Product

Steelhead appliance, CSH

Related Topics

"show secure-peering"

FIPS Commands

This section describes the Federal Information Processing Standard (FIPS) support commands.

fips enable

Description

Enables FIPS mode.

Syntax

[no] fips enable

Parameters

None

Usage

FIPS is a publicly announced set of validation standards developed by the United States National Institute of Standards and Technology (NIST) for use by government agencies and by government contractors.

FIPS 140-2 is a technical and worldwide de-facto standard for the implementation of cryptographic modules. FIPS validation makes the Riverbed appliance more suitable for use with government agencies that have formal policies requiring use of FIPS 140-2 validated cryptographic software.

To achieve FIPS compliance on a Riverbed appliance, you must run a software version that includes the Riverbed Cryptographic Security Module (RCSM) v1.0, configure the system to run in FIPS operation mode, and adjust the configuration of any features that are not FIPS compliant.

The RCSM is validated to meet FIPS 140-2 Level 1 requirements. Unlike FIPS 140-2 Level 2 validation, which requires physical security mechanisms, Level 1 validates the software only.

For more information on the FIPS implementation, see the *FIPS Administrator's Guide*.

Example

```
amnesiac (config) # fips enable
amnesiac (config) # service restart
```

Product

Steelhead appliance, Steelhead EX appliance, Granite Core

Related Topics

"show fips status"

---

show fips status

Description

Displays FIPS status information by feature.

Syntax

show fips status

Parameters

None

Example

```
amnesiac > show fips status
CMC Autoregistration: Should not be configured in FIPS mode.
Citrix Basic Encryption: Should not be configured in FIPS mode.FIPS Mode: Disabled. You must save
the configuration and reload the system to enable FIPS mode.
```

Product

Steelhead appliance, Steelhead EX appliance, Granite Core

Related Topics

"fips enable"

REST API Access Commands

This section describes the REST (REpresentational State Transfer) API access commands. REST provides a framework for API design by building a simple API on top of the HTTP protocol.

papi rest access_code generate

Description

Generates a new REST API access code for appliance monitoring.

Syntax

[no] papi rest access_code generate desc <description>

Parameters

desc <description>	Describe how the access code will be used.

Usage

You can invoke the REST API to enable communication from one Riverbed appliance to another through REST API calls: for example:

- A Cascade Profiler appliance communicating with a Cascade Shark appliance appliance.
- A Cascade Profiler appliance retrieving a QoS configuration from a Steelhead appliance.

Use the **papi rest access_code generate** command to gain access to the REST APIs by generating access codes.

You must use this access code to authenticate communication between parties and to authorize access to protected resources. See the *Steelhead Appliance Management Console User's Guide* for more information about REST API access.

Example

```
amnesiac (config) # papi rest access_code generate description cascadeflow
```

Product

CMC, Steelhead appliance

Related Topics

"papi rest access_code import," "show papi rest access_codes"

papi rest access_code import

Description

Imports an existing REST access code.

Syntax

[no] papi rest access_code import desc <description> data <data>

Parameters

desc <description>	Describe how the access code will be used.
data <data>	Copy and enter the raw data output generated by the **papi rest access_code generate** command on a peer Steelhead appliance.

Usage

Use the **papi rest access_code import** command to import access codes generated by another Steelhead appliance so that a client can use the same access code to communicate through the REST API to multiple Steelhead appliances.

Example

```
amnesiac (config) # papi rest access_code import desc cascadeflow data <data>
```

Product

CMC, Steelhead appliance

Related Topics

"papi rest access_code generate," "show papi rest access_codes"

Job Commands

This section describes commands for running jobs in the system.

job command

Description

Schedules CLI command execution for a specified time in the future.

Syntax

[no] job <job-id> command <sequence #> <"cli-command">

Parameters

<job-id>	Specify the job identification number.
<sequence #>	Specify the sequence number for job execution. The sequence number is an integer that controls the order in which a CLI command is executed. CLI commands are executed from the smallest to the largest sequence number.
<"cli-command">	Specify the CLI command. Enclose the command in double-quotes.

Usage

A job includes a set of CLI commands and a time when the job runs. Jobs are run one time only, but they can be reused.

Any number of CLI commands can be specified with a job and are executed in an order specified by sequence numbers. If a CLI command in the sequence fails, no further commands in the job are executed. A job can have an empty set of CLI commands.

The output of all commands executed are viewable after job execution by running the **show job <job-id>** command. The output of each job is only available for the last run; it is re-written upon each execution.

The job output and any error messages are saved. Jobs can be canceled and rescheduled.

The **no job <job-id> command <sequence #>** command option deletes the CLI command from the job.

The **no job <job-id>** command option removes all statistics associated with the specified job. If the job has not executed, the timer event is canceled. If the job was executed, the results are deleted along with the job statistics.

Example

```
amnesiac (config) # job 10 command 1 "show info"
amnesiac (config) # job 10 command 2 "show connections"
amnesiac (config) # job 10 command 3 "show version"
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show job," "show jobs"

job comment

Description

Adds a comment to the job for display when **show jobs** is run.

Syntax

[no] job <job-id> comment <"description">

Parameters

<job-id>	Specify the job identification number.
comment <"description">	Specify the comment for the job. Enclose the description in double-quotes.

Usage

The **no** command option deletes the comment.

Example

```
amnesiac (config) # job 10 "comment this is a test"
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show job," "show jobs"

job date-time

Description

Sets the date and time for the job to execute.

Syntax

[no] job <job-id> date-time <hh>: <mm>:<ss> <cr> | <yyyy>/<mm>/<dd>

Parameters

<job-id>	Specify the job identification number.
<hh>:<mm>:<ss> <cr> [<date>]	Specify the time for the job to execute.
<yyyy>/<mm>/<dd>	Specify the date for the job to execute.

Usage

If the time specified is in the past, the job does not execute and is in the inactive state.
The **no** command option disables the date and time settings.

Example

```
amnesiac (config) # job 10 date-time 04:30:23
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show job," "show jobs"

job enable

Description

Enables a CLI command job to execute at the date and time specified in the job.

Syntax

[no] job <job-id> enable

Parameters

<job-id>	Specify the job identification number.

Usage

The **no** command option disables jobs.

Example

```
amnesiac (config) # job 10 enable
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"show job," "show jobs"

job execute

Description

Forces an immediate execution of a job. The timer (if set) is canceled, and the job is moved to the completed state.

Syntax

job <job-id> execute

Parameters

<job-id>	Specify the job identification number.

Usage

You can also access this command from enable mode.

Example

```
amnesiac (config) # job 10 execute
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show job," "show jobs"

job fail-continue

Description

Executes all commands in a job even if a command in the sequence fails.

Syntax

[no] job <job-id> fail-continue

Parameters

<job-id>	Specify the job identification number.

Usage

The **no** command option disables this command.

Example

```
amnesiac (config) # job 10 fail-continue
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show job," "show jobs"

job name

Description

Sets the name for the job.

Syntax

[no] job <job-id> name <friendly-name>

Parameters

<job-id>	Specify the job identification number.
<friendly-name>	Specify a name for the job.

Usage

The **no** command option deletes the job name.

Example

```
amnesiac (config) # job 10 name myjob
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show job," "show jobs"

job recurring

Description

Sets the frequency with which to recurrently execute this job.

Syntax

[no] job <job-id> recurring <seconds>

Parameters

<job-id>	Specify the job identification number.
<seconds>	Specify how frequently the recurring job should execute.

Example

```
amnesiac (config) # job 10 recurring 36000
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show job," "show jobs"

Debugging Commands

This section describes the commands to debug the system.

debug generate dump

Description

Generates a report you can use to diagnose misconfiguration in deployments.

Syntax

debug generate dump [full | brief | rsp | stats | all-logs |blockstore | blockstore-fifo] [upload [<case number> | <url>]]

Parameters

full	Generate a full system dump.
brief	Generates a brief system dump.
rsp	Generate a full system dump, including VMware Server data.
stats	Generates a full system dump including .dat files.
all-logs	Generate a full system dump with .dat files and all logs.
blockstore	Generate a full system dump with .dat files, all logs, and blockstore phash.
blockstore-fifo	Generate a full system dump with .dat files, all logs, blockstore phash, and fifo.
upload <case-number> | <url>	Generate a full system dump and specify the customer case number or URL to upload to Riverbed Technical Support. Riverbed Technical Support recommends using a case number. The case number is a numeric string.

Usage

Specifying the case number is a convenient and intuitive method to generate and upload a system dump compared to using a URL. Riverbed Technical Support recommends using a case number. You can still specify a full URL in place of a case number. In this case, the report is uploaded to the specified URL instead of the URL constructed from the case number.

If the URL points to a directory on the upload server, you must specify the trailing slash "/" : for example, ftp://ftp.riverbed.com/incoming/and not ftp://ftp.riverbed.com/incoming. The file name as it exists on the appliance is renamed to the file name specified in the url.

After the dump generation, the upload is done in the background so you can exit the command-line interface without interrupting the upload process.

Example

```
amnesiac (config) # debug generate dump brief
amnesiac (config) # debug generate dump upload 194170
amnesiac (config) # debug generate dump upload ftp://ftp.riverbed.com/incoming/
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"RiOS TCP Dump Commands"

file debug-dump delete

Description

Deletes the specified debug dump file.

Syntax

file debug-dump delete <filename>

Parameters

<filename>	Specify the filename.

Example

```
amnesiac (config) # file debug-dump delete mydumpfile.txt
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"RiOS TCP Dump Commands"

file debug-dump email

Description

Sends a debug dump file in email to pre-configured recipients.

Syntax

file debug-dump email <filename>

Parameters

<filename>	Specify the filename.

Example

```
amnesiac (config) # file debug-dump email mydumpfile.txt
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"RiOS TCP Dump Commands"

file debug-dump upload

Description

Uploads the specified debug dump file.

Syntax

file debug-dump upload <filename> {<ftp, or scp://username:password@host/path)> | <case-number>}

Parameters

<filename>	Specify the filename.
<<ftp, or scp URL (e.g. scp://username:password@host/path)>	Specify the FTP or scp URL.
<case-number>	Specify the customer case number. The case number is a convenient and intuitive method to upload a debug dump file to Riverbed Technical Support without using a URL. Riverbed Technical Support recommends using a case number. The case number is a numeric string.

Example

```
amnesiac (config) # file debug-dump upload mydebug.txt scp://me:test@example.com/mypath
amnesiac (config) # file debug-dump upload mydebug.txt 194170
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"RiOS TCP Dump Commands"

file process-dump delete

Description

Deletes the specified crash dump file.

Syntax

file process-dump delete <filename>

Parameters

<filename>	Specify the filename.

Example

```
amnesiac (config) # file process-dump delete mycrash.txt
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller

Related Topics

"RiOS TCP Dump Commands"

file process-dump upload

Description

Uploads the specified crash dump file.

Syntax

file process-dump upload <filename> {<https, http, ftp, or scp URL: scp://username:password@hostname/path/filename> | <case-number>}

Parameters

<filename>	Specify the filename.
<<https, http, ftp, or scp URL: scp://username:password@hostname/path/filename>>	Specify the URL.
<case-number>	Specify the customer case number. The case number is a convenient and intuitive method to upload a crash dump file to Riverbed Technical Support without using a URL. Riverbed Technical Support recommends using a case number. The case number is a numeric string.

Example

```
amnesiac (config) # file process-dump upload mycrash.txt scp://mylogin:mypassword@myhostname/path/
filename
amnesiac (config) # file process-dump upload mycrash.txt 194170
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"RiOS TCP Dump Commands"

Raid Commands

This section describes the RAID commands.

raid alarm silence

Description

Silences the RAID alarm.

Syntax

raid alarm silence

Parameters

None

Example

```
amnesiac (config) # raid alarm silence
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show raid info"

raid swraid add-disk

Description

Adds a disk back into the system of RAID arrays. Does not require physically removing and re-inserting the drive.

Syntax

raid swraid add-disk <disk>

Parameters

<disk>	Specify the physical drive number of the drive to be added.

Usage

Use the **swraid add-disk** command to add drives back into the system without removing and re-inserting the drive physically. The parameter is the physical drive number. The command takes care of re-adding the partitions on the drive to all the appropriate RAID arrays.

Example

```
amnesiac (config) # raid swraid add-disk 1
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show raid info"

raid swraid add-disk-force

Description

Forcibly adds a failed disk back into the system of RAID arrays. Does not require physically removing and re-inserting the drive.

Syntax

raid swraid add-disk-force <disk>

Parameters

<disk>	Specify the physical drive number of the drive to be added.

Usage

Use the **raid swraid add-disk-force** command to forcibly add drives back into the system without removing and re-inserting the drive physically. The parameter is the physical drive number. The command takes care of re-adding the partitions on the drive to all the appropriate RAID arrays.

Example

```
amnesiac (config) # raid swraid add-disk-force 1
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show raid info"

raid swraid fail-disk

Description

Configures fail setting on a RAID disk. Forcibly fails a physical drive from all the software RAID arrays. Use this command before removing a disk that has not failed from the system, if possible.

Syntax

raid swraid fail-disk <disk>

Parameters

<disk>	Specify the physical drive number of the disk.

Example

```
amnesiac (config) # raid swraid fail-disk 1
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show raid info"

raid swraid get-rate

Description

Displays the RAID rebuild rate.

Syntax

raid swraid get-rate

Parameters

None

Example

```
amnesiac (config) # raid swraid get-rate
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show raid info"

raid swraid mdstat

Description

Displays the contents of /proc/mdstat.

Syntax

raid swraid mdstat

Parameters

None

Usage

Use **raid swraid mdstat** to view the kernel RAID status for all active multiple disk devices, as it is stored in the Linux file /proc/mdstat. The **Personalities** field lists the RAID levels currently supported. For more information on the contents of /proc/mdstat, see standard Linux documentation.

Example

```
amnesiac (config) # raid swraid mdstat
Personalities : [linear] [raid0] [raid10]
unused devices: <none>
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show raid info"

raid swraid set-rate

Description

Sets the RAID rebuild rate.

Syntax

raid swraid set-rate <rate>

Parameters

<rate>	Specify rebuild rate as a number of MBs or: **fast_rebuild**, **slow_rebuild**, or **normal**.

Example

```
amnesiac (config) # raid swraid set-rate fast_rebuild
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show raid info"

Network Test Commands

This section describes the network testing commands. If you are experiencing network issues Riverbed Support will ask you to run network tests so that they can understand the state of the network.

With these tests common problems are easily identified and can be immediately addressed by the Riverbed support representative.

nettest run cable-swap

Description

Runs the cable swap test.

Syntax

nettest run cable-swap

Parameters

None

Usage

Ensures that the WAN and LAN cables on the Steelhead appliance are connected to the LAN and WAN of the network. The test enumerates the results by interface (one row entry per pair of bypass interfaces).

By default, this test is disabled.

Certain network topologies might cause an incorrect result for this test. For the following topologies, Riverbed recommends that you confirm the test result manually:

- Steelhead appliances deployed in virtual in-path mode.
- Server-side Steelhead appliances that receive significant amounts of traffic from nonoptimized sites.
- Steelhead appliances that sit in the path between other Steelheads that are optimizing traffic.

If the test fails, ensure a straight-through cable is not in use between an appliance port and a router, or that a crossover cable is not in use between an appliance port and a switch.

Example

```
amnesiac (config) # nettest run cable-swap
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show nettest"

nettest run duplex

Description

Runs the duplex matching test.

Syntax

nettest run duplex <interface> {ipv6-target <ipv6-address> | target <ipv4-address>}

Parameters

<interface>	Specify the duplex interface.
ipv6-target <ipv6-address>	Specify the target IPv6 address to reach.
target <ipv4-address>	Specify the target IPv4 address to reach.

Usage

Determines if the speed and duplex settings match on each side of the default gateway connection. If one side is different from the other, then traffic is sent at different rates on each side, causing a great deal of collision. This test runs the ping utility for 5 seconds with a packet size of 2500 bytes against the default gateway.

Optionally, select an interface to test. The more interfaces you test, the longer it takes the diagnostics to run. If you do not specify an interface, the Steelhead appliance runs the duplex test on all interfaces.

The test passes if the system acknowledges 100% of the packets and a receives responses from all packets. If any packets are lost, the test fails.

If the test fails, ensure that the speed and duplex settings of the appliance's Ethernet interfaces match those of the switch ports to which they are connected.

The test output records the percentage of any lost packets and number of collisions.

Note: For accurate test results, traffic must be running through the Steelhead appliance.

Example

```
amnesiac (config) # nettest run duplex
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show nettest"

nettest run ip-port-reach

Description

Runs the IP address and port test.

Syntax

nettest run ip-port-reach source <interface> {addr <ipv4-addr> | ipv6-addr <ipv6-addr>} [port <port>]

Parameters

source <interface>	Specify the source interface.
addr <ipv4-addr>	Specify the peer IPv4 address to check.
ipv6-addr <ipv6-addr>	Specify the peer IPv6 address to check.
port <port>	Specify the port to check.

Usage

Use this command to determine whether a specified IP address and optional port is correctly connected. If you specify only an IP address, the test sends an ICMP message to the IP address. If you specify a port number, the test telnets to the port.

If the test fails, ensure that dynamic or static routing on your network is correctly configured and that the remote network is reachable from hosts on the same local subnet as this appliance.

Example

```
amnesiac (config) # nettest run ip-port-reach source addr 10.0.0.1
```

Product

Steelhead appliance, CSH

Related Topics

"show nettest"

nettest run net-gateway

Description

Runs the network gateway test.

Syntax

nettest run net-gateway [ipv6]

Parameters

ipv6	Optionally, run the IPv6 network gateway test.

Usage

Determines if each configured gateway is connected correctly. Run this test to ping each configured gateway address with four packets and record the number of failed or successful replies. The test passes if all four packets are acknowledged. The default packet size is 64 bytes.

If the test fails and all packets are lost, ensure that the gateway IP address is correct and that the Steelhead appliance is on the correct network segment. If the gateway is reachable from another source, check the connections between the Steelhead appliance and the gateway.

If the test fails and only some packets are lost, check your duplex settings and other network conditions that might cause dropped packets.

Example

```
amnesiac (config) # nettest run net-gateway
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show nettest"

nettest run peer-reach

Description

Runs the peer reachability test.

Syntax

nettest run peer-reach addr <ip-addr> | port <port>

Parameters

addr <ip-addr>	Specify the IP address of the peer appliance to test.
port <port>	Specify the port.

Usage

Select to send a test probe to a specified peer and await the probe response. If a response is not received, the test fails.

Tip: To view the current peer appliances, choose Reports > Optimization > Connected Appliances in the Management Console.

Do not specify the primary or auxiliary IP of the same Steelhead appliance displayed in the Connected Appliances report (the primary or aux IP to which the Steelhead appliance is connected).

If the test fails, ensure that there are no firewalls, IDS/IPS, VPNs, or other security devices which may be stripping or dropping connection packets between Steelhead appliances.

Example

```
amnesiac (config) # nettest run peer-reach addr 10.0.0.1 port 1243
```

Product

Steelhead appliance, Cloud Steelhead

Related Topics

"show nettest"

RiOS TCP Dump Commands

This section describes RiOS TCP dump commands. The system also runs the standard tcpdump utility. For detailed information, see "tcpdump" on page 174.

tcpdump stop-trigger delay

Description

Configures the time to wait before stopping a TCP dump.

Syntax

[no] tcpdump stop-trigger delay <duration>

Parameters

<duration>	Specify the amount of time to wait before stopping all running TCP dumps when RiOS finds a match. The default delay is 30 seconds.

Usage

You might not want to stop your TCP dump immediately. By configuring a delay, the system has time to log more data without abruptly cutting off the dumps. The default delay is 30 seconds.

Example

```
amnesiac (config) # tcpdump stop-trigger delay 10
```

Product

Steelhead appliance, CMC

Related Topics

"tcpdump stop-trigger enable," "tcpdump stop-trigger regex," "tcpdump stop-trigger restart," "show tcpdump stop-trigger"

tcpdump stop-trigger enable

Description

Enables the TCP dump to stop running, triggered by a match against a configured regular expression and the system log file.

Syntax

[no] tcpdump stop-trigger enable

Parameters

None

Usage

There is a limit to the amount of TCP dump data the system can collect. After a problem has occurred, the TCP dump buffer could have rotated, overwriting the information about the problem. This command enables a trigger that stops a continuous TCP dump after a specific log event occurs. This enables you to troubleshoot issues and isolate the TCP dump data specific to a problem.

The **no** version of the command disables the TCP dump stop-trigger process.

Example

```
amnesiac (config) # tcpdump stop-trigger regex ntp
amnesiac (config) # tcpdump stop-trigger delay 20
amnesiac (config) # tcpdump stop-trigger enable
```

Product

Steelhead appliance, CMC

Related Topics

"tcpdump stop-trigger delay," "tcpdump stop-trigger regex," "tcpdump stop-trigger restart," "show tcpdump stop-trigger"

tcpdump stop-trigger regex

Description

Sets the regular expression that triggers the stopping of TCP dumps.

Syntax

tcpdump stop-trigger regex <regex>

Parameters

<regex>	Specify a PERL regular expression to match. RiOS compares the PERL regular expression against each entry made to the system logs. The system matches on a per-line basis.

Usage

Use the **tcpdump stop-trigger regex** command to configure a regular expression that represents a condition that, when matched, stops all running TCP dumps. After this match is found, all TCP dump sessions are stopped after the delay configured by the **tcpdump stop-trigger delay** command.

Example

In the following example, RiOS searches for the pattern *ntp* in the system logs. The system waits 20 seconds after there is a match and then stops all TCP dumps that are still running.

```
amnesiac (config) # tcpdump stop-trigger regex ntp
amnesiac (config) # tcpdump stop-trigger delay 20
amnesiac (config) # tcpdump stop-trigger enable
```

Product

Steelhead appliance, CMC

Related Topics

"tcpdump stop-trigger delay,""tcpdump stop-trigger enable," "tcpdump stop-trigger restart," "show tcpdump stop-trigger"

tcpdump stop-trigger restart

Description

Restarts the TCP dump stop-trigger process.

Syntax

tcpdump stop-trigger restart

Parameters

None

Usage

If you change the regular expression or delay, use the **tcpdump stop-trigger restart** command to restart the stop-trigger process.

Example

```
amnesiac (config) # tcpdump stop-trigger regex ntp
amnesiac (config) # tcpdump stop-trigger delay 50
amnesiac (config) # tcpdump stop-trigger enable
amnesiac (config) # tcpdump stop-trigger restart
```

Product

Steelhead appliance, CMC

Related Topics

"tcpdump stop-trigger delay," "tcpdump stop-trigger enable," "tcpdump stop-trigger regex," "show tcpdump stop-trigger"

tcpdump-x all-interfaces

Description

Configures a list of all interfaces for a TCP dump capture.

Syntax

[no] tcpdump-x all-interfaces [capture-name <capture-name>] continuous <cr> | | buffer-size <size in KB> | duration <seconds> <cr> [schedule-time <HH:MM:SS> [schedule-date <YYYY/MM/DD>]] | [rotate-count <# files>] | [snaplength <snaplength>] | [sip <src-addr>] | [dip <dst-addr>] | [sport <src-port>] | [dport <dst-port>] | [dot1q {tagged | untagged | both}] | [ip6] |[custom <custom-param>] | [file-size <megabytes>]

Parameters

capture-name <capture-name>	Specify a capture name to help you identify the TCP Dump. The default filename uses the following format: `<hostname>_<interface>_<timestamp>.cap` Where hostname is the hostname of the Steelhead appliance, interface is the name of the interface selected for the trace (for example, **lan0_0**, **wan0_0**), and timestamp is in the YYYY-MM-DD-HH-MM-SS format. **Note:** The cap file extension is not included with the filename when it appears in the capture queue.
continuous	Start a continuous capture.
buffer-size <size in KB>	Specify the size in KB for all packets.
duration <seconds>	Specify the run time for the capture in seconds. The default is 30 seconds.
schedule-time <HH:MM:SS>	Specify a time to initiate the trace dump in the following format: HH:MM:SS.
schedule-date <YYYY/MM/DD>	Specify a date to initiate the trace dump in the following format: YYYY/MM/DD
rotate-count <# files>	Specify the number of files to rotate.
snaplength <snaplength>	Specify the snap length value for the trace dump. The default value is 1518. Specify **0** for a full packet capture (recommended for CIFS, MAPI, and SSL traces).
sip <src-addr>	Specify a comma-separated list of source IP addresses. The default setting is all IP addresses.
dip <dst-addr>	Specify a comma-separated list of destination IP addresses. The default setting is all IP addresses.
sport <src-port>	Specify a comma-separated list of source ports. The default setting is all ports.
dport <dst-port>	Specify a comma-separated list of destination ports. The default setting is all ports.
dot1q {tagged | untagged | both}	Specify one of the following to filter dot1q packets: • **tagged** - Capture only tagged traffic. • **untagged** - Capture only untagged traffic. • **both** - Capture all traffic. **Note:** Do not use the **sip**, **dip**, **sport**, **dport** and **custom** parameters together when using the **dot1q both** option. Use the **tcpdump** command instead to capture this information. For detailed information about dot1q VLAN tunneling, see your networking equipment documentation.
ip6	Specify IPv6 packets for packet capture.
custom <custom-param>	Specify custom parameters (flags) for packet capture. You need to enclose the customer parameter in quotes if it contains more than one word.
file-size <megabytes>	Specify the file size of the capture in megabytes.

Usage

You can capture and retrieve multiple TCP trace dumps. You can generate trace dumps from multiple interfaces at the same time and you can schedule a specific date and time to generate a trace dump.

Example

The following example starts a continuous capture for a file named *tcpdumpexample* with a duration of 120 seconds:

```
amnesiac (config) # tcpdump-x all-interfaces capture-name tcpdumpexample continuous duration 120
```

The following example captures untagged traffic on destination port 7850 and ARP packets:

```
amnesiac (config) # tcpdump-x all-interfaces dot1q untagged dport 7850 custom "and arp"
```

The following example captures VLAN tagged traffic for host 10.11.0.6 and ARP packets:

```
amnesiac (config) # tcpdump-x all-interfaces dot1q tagged sip 10.11.0.6 custom "or arp"
```

The following example captures tagged ARP packets only:

```
amnesiac (config) # tcpdump-x all-interfaces dot1q tagged custom "and arp"
```

The following example captures untagged ARP packets only:

```
amnesiac (config) # tcpdump-x all-interfaces dot1q untagged custom "and arp"
```

Product

Steelhead appliance, CMC appliance, Steelhead Mobile Controller, Interceptor appliance, CSH

Related Topics

"show tcpdump-x," "tcpdump"

tcpdump-x capture-name stop

Description

Stops the specified TCP dump capture.

Syntax

[no] tcpdump-x capture-name <capture-name> stop

Parameters

<capture-name>	Specify the capture name to stop.

Example

```
amnesiac (config) # tcpdump-x capture-name example stop
```

Product

Steelhead appliance, CMC appliance, Steelhead Mobile Controller, Interceptor appliance, CSH

Related Topics

"show tcpdump-x," "tcpdump"

tcpdump-x interfaces

Description

Configures a comma-separated list of interfaces to capture in the background.

Syntax

[no] tcpdump-x interfaces <interface-name> continuous <cr> | duration <seconds> <cr> [schedule-time <HH:MM:SS> [schedule-date <YYYY/MM/DD>]] | [rotate-count <# files>] | [snaplength <snaplength>] | [sip <src-addr>] | [dip <dst-addr>] | [sport <src-port>] [dport <dst-port>] | [dot1q {tagged | untagged | both}] [ip6] | [custom <custom-param>] | [file-size <megabytes>]

Parameters

<interface-name>	Specify a comma-separated list of interfaces: **primary**, **aux**, **lan0_0**, **wan0_0**
continuous	Start a continuous capture.
duration <seconds>	Specify the run time for the capture in seconds.
schedule-time <HH:MM:SS>	Specify a time to initiate the trace dump in the following format: HH:MM:SS
schedule-date <YYYY/MM/DD>	Specify a date to initiate the trace dump in the following format: YYYY/MM/DD
rotate-count <#files>	Specify the number of files to rotate.
snaplength <snaplength>	Specify the snap length value for the trace dump. The default value is 1518. Specify **0** for a full packet capture (recommended for CIFS, MAPI, and SSL traces).
sip <src-addr>	Specify the source IP addresses. The default setting is all IP addresses.
dip <dst-addr>	Specify a comma-separated list of destination IP addresses. The default setting is all IP addresses.
sport <src-port>	Specify a comma-separated list of source ports. The default setting is all ports.
dport <dst-port>	Specify a comma-separated list of destination ports. The default setting is all ports.
dot1q {tagged | untagged | both}	Specify one of the following to filter dot1q packets: • **tagged** - Capture only tagged traffic. • **untagged** - Capture only untagged traffic. • **both** - Capture all traffic. **Note:** Do not use the **sip**, **dip**, **sport**, **dport** and **custom** parameters together when using the **dot1q both** option. Use the **tcpdump** command to capture this information. For detailed information about dot1q VLAN tunneling, see your networking equipment documentation.
ip6	Specify IPv6 packets for packet capture.
custom <custom-param>	Specify custom parameters (flags) for packet capture.
file-size <megabytes>	Specify the file size of the capture in megabytes.

Example

```
amnesiac (config) # tcpdump-x interfaces inpath0_0 continuous
amnesiac (config) # tcpdump-x interfaces aux ip6 sip 2003::5
```

Product

Steelhead appliance, CMC appliance, Steelhead Mobile Controller, Interceptor appliance, CSH

Related Topics

"tcpdump," "show tcpdump-x"

Remote Management Port Commands

This section describes the commands for configuring the remote management port in Models 1050x, 2050x, 5050x, 6050x, 7050x, EX1160x, EX1260x, CX1555x, EX560x, and EX760x. The port is labeled REMOTE on the back of each appliance except for the EX560x and EX760x models. The EX560x and EX760x models do not have a separate remote port but share it with the primary port.

This remote management port is unique in that it is connected to the Baseboard Management Controller (BMC) on these models. The BMC is a central component of the Intelligent Platform Management Interface (IPMI) capabilities of the machine, which are important for reading the onboard sensors, reading and writing Electrically Erasable Programmable Read-Only Memory (EEPROMs), fan control, LED control, and in-path hardware bypass control for these models. The BMC and remote management port operate independently of the CPUs and network interfaces, which allow them to continue to operate even when the machine has hit a kernel panic, become wedged, or has been given the **reload halt** command.

For details on configuring the remote management port, see "remote ip address" on page 742.

Important: You can only configure the remote management port on the 1050x, 2050x, 5050x, 6050x, 7050x, EX1160x, EX1260x, CX1555x, EX560x, and EX760x models. Remote port management is not supported on other platforms. The EX560x and EX760x models do not have a separate remote port but share it with the primary port.

Important: Access to the Steelhead appliance through the remote management port requires the use of the IPMI tool utility. You can download a Linux version at http://sourceforge.net/projects/ipmitool/files/. You can obtain a Windows version of the IPMI tool on the Document CD that ships with your system or from the Riverbed Support at https://support.riverbed.com.

remote dhcp

Description

Enables DHCP on the remote management port.

Syntax

remote dhcp

Parameters

None

Example

```
amnesiac (config) # remote dhcp
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show remote ip"

remote ip address

Description

Manually sets the IP address of the remote management port.

Syntax

remote ip address <ip-addr>

Parameters

<ip-addr>	Specify the IP address to assign to the remote management port.

Usage

Access to the Steelhead appliance through the remote port requires the use of the IPMItool utility. You can download a Linux version at http://sourceforge.net/projects/ipmitool/files/. You can obtain a Windows version of the IPMI tool on the Document CD that ships with your system or from the Riverbed Support at https://support.riverbed.com.

This utility must to be run on an administrator's system outside of the Steelhead appliance to access the remote port functions. Check the man page for IPMItool for a full list of capabilities (although not all the commands are supported on RiOS hardware platforms).

To configure the remote management port

- Physically connect the REMOTE port to the network. You cable the remote management port to the Ethernet network in the same manner as the Primary interface. For details, see the *Steelhead Appliance Installation and Configuration Guide*.
- Install the IPMItool on the client machine.
- Assuming the IP address is 192.168.100.100, the netmask is 255.255.255.0, and the default gateway is 192.168.100.1, assign an IP address to the remote management port:

```
amnesiac (config) # remote dhcp
 - or -
amnesiac (config) # remote ip address 192.168.100.100
amnesiac (config) # remote ip netmask 255.255.255.0
amnesiac (config) # remote ip default-gateway 192.168.100.1
```

- Verify the IP address is set properly.

```
amnesiac (config) # show remote ip
```

Tip: Ping the new management IP address from a remote computer, and verify it replies.

- To secure the remote port, assign a password to the port:

```
amnesiac (config) # remote password <newpassword>
```

- Set the remote port bit-rate to match the current serial port bitrate. Typically, this value is 9.6.

```
amnesiac (config) # remote bitrate 9.6
```

- To activate the serial connection:

```
ipmitool -I lanplus -H 192.168.100.100  -P "<password>" sol activate
```

Press the Tilde character (~) to end the serial connection.

Note: While your serial connection is established, the actual serial console is disabled. Ending the remote serial connection cleanly with Tilde (~) re-enables the real serial port. If you fail to exit cleanly your actual serial port might not reactivate. If your serial port fails to reactivate, reconnect remotely and exit cleanly using Tilde (~).

Example

```
amnesiac (config) # remote ip address 192.168.100.100
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show remote ip"

remote ip default-gateway

Description

Manually sets the default gateway of the remote management port.

Syntax

remote ip default-gateway <ip-addr>

Parameters

<ip-addr>	Specify the IP address of default gateway to assign to remote management port.

Example

```
amnesiac (config) # remote ip default-gateway 10.0.0.2
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show remote ip"

remote ip netmask

Description

Manually sets the subnet mask of the remote management port.

Syntax

remote ip netmask <netmask>

Parameters

<netmask>	Specify the subnet mask to assign to the remote management port.

Example

```
amnesiac (config) # remote ip netmask 255.255.255.0
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, Cloud Steelhead

Related Topics

"show remote ip"

remote password

Description

Sets the password to remotely connect to the remote management port.

Syntax

[no] remote password <password>

Parameters

<password>	Specify the password to connect to the remote management port.

Usage

To set a remote management port password

- On the Steelhead appliance, assign a password to the remote management port:

  ```
  amnesiac (config) # remote password TestPassword
  ```

- Using the IPMItool on a remote computer, view the power status of the Steelhead appliance. If you are using the Windows version of IPMItool, replace all references to **ipmitool** with ipmitool.exe.

```
ipmitool -H <remote port ip address> -P "testpassword" chassis power status
```

Output should state **Chassis Power is on**.

Note: You can download a Linux version at http://sourceforge.net/projects/ipmitool/files/. You can obtain a Windows version of the IPMI tool on the Document CD that ships with your system or from the Riverbed Support at https://support.riverbed.com.

Example

```
amnesiac (config) # remote password TestPassword
```

Product

CMC appliance, Interceptor appliance, Steelhead appliance, Steelhead Mobile Controller, CSH

Related Topics

"show remote ip"

Hardware-Assist Rule Commands

The following section describes the hardware-assist rule commands for the Steelhead appliance and Interceptor appliance.

in-path hw-assist edit-rule

Description

Provides an optional text description of the specified rule.

Syntax

in-path hw-assist edit-rule rulenum <rule number> description <"text">

Parameters

rulenum <rule number>	Specify the rule number.
description <"text">	Specify the description. The text must be enclosed in quotation marks.

Usage

This feature functions only on a Steelhead appliance or Interceptor appliance equipped with one or more Two-Port SR Multimode Fiber 10 Gigabit-Ethernet PCI-E or Two-Port LR Single Mode Fiber 10 Gigabit-Ethernet PCI-E cards.

Hardware Assist rules can automatically bypass all UDP (User Datagram Protocol) connections. You can also configure rules for bypassing specific TCP (Transmission Control Protocol) connections. Automatically bypassing these connections decreases the work load on the local Steelhead appliances because the traffic is immediately sent to the kernel of the host machine or out of the other interface before the system receives it.

Note: For a hardware assist rule to be applied to a specific 10G bypass card, the corresponding in-path interface must be enabled and have an IP address.

If the system is not equipped with the necessary card, an error message displays.

Example

```
amnesiac (config) # in-path hw-assist edit-rule rulenum 5 description "This rule enables automatic
passthrough for all UDP connections"
```

Product

Steelhead appliance, Interceptor appliance, Cloud Steelhead

Related Topics

"show in-path hw-assist rules"

in-path hw-assist move-rule rulenum

Description

Moves the rule to the specified position.

Syntax

in-path hw-assist move-rule rulenum <rule number> to <new rule number>

Parameters

rulenum <rule number>	Specify the rule number.
to <new rule number>	Specify the new position for the specified rule.

Usage

This feature functions only on a Steelhead appliance or Interceptor appliance equipped with one or more Two-Port SR Multimode Fiber 10 Gigabit-Ethernet PCI-E or Two-Port LR Single Mode Fiber 10 Gigabit-Ethernet PCI-E cards.

Hardware Assist rules can automatically bypass all UDP (User Datagram Protocol) connections. You can also configure rules for bypassing specific TCP (Transmission Control Protocol) connections. Automatically bypassing these connections decreases the work load on the local Steelhead appliances because the traffic is immediately sent to the kernel of the host machine or out of the other interface before the system receives it.

Note: For a hardware assist rule to be applied to a specific 10G bypass card, the corresponding in-path interface must be enabled and have an IP address.

If the system is not equipped with the necessary card, an error message displays.

Example

```
amnesiac (config) # in-path hw-assist move-rule rulenum 5 to 3
```

Product

Steelhead appliance, Interceptor appliance, Cloud Steelhead

Related Topics

"show in-path hw-assist rules"

in-path hw-assist passthrough tcp enable

Description

Enables automatic pass-through of TCP traffic.

Syntax

[no] in-path hw-assist passthrough tcp enable

Parameters

None

Usage

This feature functions only on a Steelhead appliance or Interceptor appliance equipped with one or more Two-Port SR Multimode Fiber 10 Gigabit-Ethernet PCI-E or Two-Port LR Single Mode Fiber 10 Gigabit-Ethernet PCI-E cards.

Hardware Assist rules can automatically bypass all UDP (User Datagram Protocol) connections. You can also configure rules for bypassing specific TCP (Transmission Control Protocol) connections. Automatically bypassing these connections decreases the work load on the local Steelhead appliances because the traffic is immediately sent to the kernel of the host machine or out of the other interface before the system receives it.

Note: For a hardware assist rule to be applied to a specific 10G bypass card, the corresponding in-path interface must be enabled and have an IP address.

If the system is not equipped with the necessary card, an error message displays.

Example

```
amnesiac (config) # in-path hw-assist passthrough tcp enable
```

Product

Steelhead appliance, Interceptor appliance, Cloud Steelhead

Related Topics

"show in-path hw-assist rules"

in-path hw-assist passthrough udp enable

Description

Enables automatic pass-through of all UDP traffic.

Syntax

[no] in-path hw-assist passthrough udp enable

Parameters

None

Usage

This feature functions only on a Steelhead appliance or Interceptor appliance equipped with one or more Two-Port SR Multimode Fiber 10 Gigabit-Ethernet PCI-E or Two-Port LR Single Mode Fiber 10 Gigabit-Ethernet PCI-E cards.

Hardware Assist rules can automatically bypass all UDP (User Datagram Protocol) connections. You can also configure rules for bypassing specific TCP (Transmission Control Protocol) connections. Automatically bypassing these connections decreases the work load on the local Steelhead appliances because the traffic is immediately sent to the kernel of the host machine or out of the other interface before the system receives it.

Note: For a hardware assist rule to be applied to a specific 10G bypass card, the corresponding in-path interface must be enabled and have an IP address.

If the system is not equipped with the necessary card, an error message displays.

Example

```
amnesiac (config) # in-path hw-assist passthrough udp enable
```

Product

Steelhead appliance, Interceptor appliance, Cloud Steelhead

Related Topics

"show in-path hw-assist rules"

in-path hw-assist rule

Description

Enables the hardware UDP pass-through feature.

Syntax

[no] in-path hw-assist rule [accept | pass-through] | [subnet-a <Subnet A>] | [subnet-b <Subnet B>] | [description <"string">] | [vlan <VLAN>] | [rulenum <rulenum>]

Parameters

accept | pass-through	Specify the action of the rule: • **accept** - Accepts traffic for this rule. • **pass-through** - Passes through traffic for this rule.
subnet-a <Subnet A>	Specify an IP address for the subnet that can be both source and destination together with Subnet B. Use the format XXX.XXX.XXX.XXX/XX. **Note:** You can specify all or 0.0.0.0/0 as the wildcard for all traffic.
subnet-b <Subnet B>	Specify an IP address for the subnet that can be both source and destination together with Subnet A. Use the format XXX.XXX.XXX.XXX/XX. **Note:** You can specify all or 0.0.0.0/0 as the wildcard for all traffic.
description <"string">	Specify a description of the rule. The string must be in double-quotes.
vlan <VLAN>	Optionally, specify the VLAN identification number to set the VLAN tag ID: -1 = all, 1 = untagged, maximum = 4094 • Specify all to specify the rule applies to all VLANs. • Select untagged to specify the rule applies to non-tagged connections. **Note:** Pass-through traffic maintains any pre-existing VLAN tagging between the LAN and WAN interfaces. **Note:** To complete the implementation of VLAN tagging, you must set the VLAN tag IDs for the in-path interfaces that the Interceptor appliance uses to communicate with other Interceptor appliance.
rulenum <rulenum>	Specify the rule number to insert the pass-through load-balancing rule before.

Usage

This feature functions only on a Steelhead appliance or Interceptor appliance equipped with one or more Two-Port SR Multimode Fiber 10 Gigabit-Ethernet PCI-E or Two-Port LR Single Mode Fiber 10 Gigabit-Ethernet PCI-E cards.

Hardware Assist rules can automatically bypass all UDP (User Datagram Protocol) connections. You can also configure rules for bypassing specific TCP (Transmission Control Protocol) connections. Automatically bypassing these connections decreases the work load on the local Steelhead appliances because the traffic is immediately sent to the kernel of the host machine or out of the other interface before the system receives it.

Note: For a hardware assist rule to be applied to a specific 10G bypass card, the corresponding in-path interface must be enabled and have an IP address.

If the system is not equipped with the necessary card, an error message displays.

To delete a rule, use the **no** command option as follows:

```
no in-path hw-assist rule rulenum <rule number>
```

Example

```
amnesiac (config) # in-path hw-assist rule accept subnet-a 10.0.0.1/16 subnet-b 10.0.0.4/16 rulenum 
1
```

Product

Steelhead appliance, Interceptor appliance, Cloud Steelhead

Related Topics

"show in-path hw-assist rules"

Handheld Commands

This section describes the handheld commands.

handheld enable

Description

Enables handheld device-specific optimization settings.

Syntax

[no] handheld enable

Parameters

None

Usage

Use this command to activate optimization for handheld devices. You must enter this command on the server-side Steelhead appliance and not on the handheld devices. Enabling this command requires an optimization service restart for your changes to take effect.

Use the **show handheld** command to view the status of handheld device optimization.

The **no** command option disables handheld optimization.

Example

```
amnesiac (config) # handheld enable
amnesiac (config) # service restart
```

Product

Steelhead appliance

Related Topics

"show handheld"

show handheld

Description

Displays whether or not handheld support is enabled.

Syntax

show handheld

Parameters

None

Usage

Use this command to display the status of handheld device optimization on the Steelhead appliance.

Example

```
amnesiac > show handheld
Handheld enabled: no
```

Product

Steelhead appliance

Related Topics

"handheld enable"

Steelhead EX Appliance Feature Commands

This section describes commands that are unique to the Steelhead EX appliance that you can use to configure Steelhead EX appliance features. It includes the following sections:

- "Branch Storage Commands" on page 750
- "VSP Commands" on page 770

Branch Storage Commands

This section describes the branch storage commands that are unique to the Granite Edge-enabled Steelhead EX appliance. Granite is a dual-ended system with Granite Core at the data center and a Granite Edge-enabled Steelhead EX appliance at the edge.

The Granite system enables complete consolidation of storage data at the data center by providing LAN performance for block-level access at the branch office while consolidating storage at the data center. The Granite system eliminates the need for dedicated storage at the branch office, including management and related backup resources. Granite is available with an additional license.

This section also contains:

- "Displaying Branch Storage Information"

device-failover peer clear

Description

Clears the failover peer settings for the current Granite Edge device or Granite Edge-enabled Steelhead appliance.

Syntax

device-failover peer clear

Example

```
Edge1 (config) # device-failover peer clear
Edge1 (config) # show device-failover
```

Product

Steelhead EX appliance

Related Topics

"show device-failover"

device-failover peer set

Description

Specifies and sets the failover peer settings for the current Granite Edge device or Granite Edge-enabled Steelhead appliance.

Syntax

device-failover peer set <serial-number> ip <address> local-if <local-interface-name> additional-ip <additional-ip> local-if2 <local-interface-name2> edge-id <edge-id> [local-if-dc <local-interface-name>]

Parameters

<serial-number>	Specify the serial number of the Granite Edge active peer.
ip <address>	Specify the IP address of the Granite Edge active peer appliance.
local-if <local-interface-name>	Specify the local interface for the standby peer to connect to the active peer.
additional-ip <additional-ip>	Specify the IP address of the Granite Edge active peer, which is different from the first peer IP address specified by the **ip <address>** parameter.
local-if2 <local-interface-name2>	Specify the second local interface name for the standby peer to connect to the second IP address specified by the **additional-ip <additional-ip>** parameter.
edge-id <edge-id>	Specify the self-identifier for the active peer. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** . Both peer appliances must use the same self identifier. In this case, you can use a value that represents the group of appliances.
local-if-dc <local-interface-name>	Optionally, specify the local interface for the current appliance to use when connecting with the Granite Core appliance.

Usage

This command configures the failover peer settings to provide high availability between Granite Edge-enabled Steelhead appliances. High availability enables you to configure two Edge appliances so that either one can fail without disrupting the service of the LUNs being provided by Granite Core.

Example

```
Edge1 (config) # device-failover peer set DA3XS000085C5 ip 10.2.2.2 local-if primary additional-ip
10.3.2.2 local-if2 wan0_0 edge-id branch12
```

Product

Steelhead EX appliance

Related Topics

"show device-failover"

disk-config layout

Description

Switches among five modes of disk-space allocation between Granite Edge and VSP.

Syntax

disk-config layout {vsp | granite | vsp_granite | vsp_ext | vsp_granite_ext}

Parameters

vsp	Specify VSP standalone storage mode to allot all the disk space for VSP functionality. If Granite is not licensed, this mode is not available.
granite	Specify Granite standalone storage mode to allot most of the disk space for Granite storage, while leaving a minimum amount for VSP functionality. If Granite is not licensed, this mode is not available.
vsp_granite	Specify VSP and Granite standalone storage mode to evenly divide disk space between VSP functionality and Granite. If Granite is not licensed, this mode is selected by default.
vsp_ext	Specify this mode for extended VSP storage mode. This mode allots all the disk space for VSP functionality. If Granite is not licensed, this mode is not available. In EX v2.1, disk space is reclaimed for use in storing non-ESXi based virtual machine data as well as converting non-ESXi virtual machine format to ESXi virtual machine format.
vsp_granite_ext	Specify this mode for extended VSP and Granite storage mode. This mode evenly divides disk space between VSP functionality and Granite. In EX v2.1, disk space is reclaimed for use in storing non-ESXi based virtual machine data as well as converting non-ESXi virtual machine format to ESXi virtual machine format.

Usage

When you run this command, the CLI returns the following alert:

```
Switching the layout is a destructive operation. Type 'disk layout <mode selected> confirm'to
confirm. The box will reboot after this.
```

To complete the action, you must enter the confirmation as prompted.

If you want to switch disk-layout modes, the currently configured mode does not appear as an option in the CLI. In the following example, the disk-layout mode is set to the **vsp_granite_ext** option and does not appear as an option in the CLI:

```
Edge1 (config) # disk-config layout?
<disk layout>
granite
vsp
vsp_granite
vsp_ext

Edge1 (config) # disk-config layout vsp
Switching the layout is a destructive operation.
You will lose your unconverted VMs.
In addition, you will have to recreate your local datastore.
Please ensure your data has been backed up.
Type 'disk layout vsp confirm' to proceed with this operation.
If successful, the box will immediately reboot.
```

Note: You cannot choose the disk-space allocation mode that is currently in use. If you choose the current disk-space allocation mode, it is rejected as an invalid disk layout.

Example

```
Edge1 (config) # disk-config layout granite
```

Product

Steelhead EX appliance

Related Topics

"show disk-config"

ip data route

Description

Adds an IPv4 data interface static route.

Syntax

[no] ip data route <interface> <network prefix> <network mask> <next-hop-ip-addr>

Parameters

<interface>	Specify the interface.
<network prefix>	Specify the network prefix.
<network mask>	Specify the netmask.
<next-hop-ip- addr>	Specify the IP address for the next-hop destination in this route.

Usage

Use this command to specify route settings for a data interface in data mode. The data mode provides support for converting additional network interface cards (NICs) added through an external card for use as data NICs.

The **no** command option disables the IPv4 data interface route.

Example

```
Edge1 (config) # ip data route Eth01 190.160.0.0 255.255.0.0 193.162.0.0
```

Product

Steelhead EX appliance

Related Topics

"ip data-gateway," "ipv6 data route," "ipv6 data-gateway," "hardware nic slot"

ipv6 data route

Description

Adds an IPv6 data interface route.

Syntax

[no] ipv6 data route <interface> <ipv6-network-prefix> <next-hop-ipv6addr>

Parameters

<interface>	Specify the interface.
<ipv6-network-prefix>	Specify the network prefix. Use the format X:X:X::X/<0-128>.
<next-hop-ipv6addr>	Specify the IPv6 address for the next-hop destination in this route.

Usage

Use this command to specify IPv6 route settings for a data interface in data mode. The data mode provides support for converting additional network interface cards (NICs) added through an external card for use as data NICs.

The **no** command option disables the IPv6 data interface route.

Example

```
Edge1 (config) # ipv6 data route Eth01 2001:7632::/64 2001:38dc:52::e9a4:c5:6289
```

Product

Steelhead EX appliance

Related Topics

"ip data route," "ip data-gateway," "ipv6 data-gateway," "hardware nic slot"

ip data-gateway

Description

Configures an IPv4 default gateway for a data interface.

Syntax

[no] ip data-gateway <interface> <destination>

Parameters

<interface>	Specify the interface.
<destination>	Specify the IPv4 address of the data interface gateway.

Usage

Use this command to specify the default gateway for a data interface. The data mode provides support for converting additional network interface cards (NICs) added through an external card for use as data NICs.

The **no** command option removes the IPv4 default gateway for the data interface.

Example

```
Edge1 (config) # ip data-gateway Eth01 43.31.40.1
```

Product

Steelhead EX appliance

Related Topics

"ip data route," "ipv6 data route," "ipv6 data-gateway," "hardware nic slot"

ipv6 data-gateway

Description

Configures the IPv6 default gateway for a data interface.

Syntax

[no] ipv6 data-gateway <interface> <destination>

Parameters

<interface>	Specify the interface.
<destination>	Specify the IPv6 address of the data interface gateway.

Usage

Use this command to specify the IPv6 default gateway for the data interface.

The **no** command option removes the IPv6 default gateway

Example

```
Edge1 (config) # ipv6 data-gateway Eth01 2001:cf8:0:41::1
```

Product

Steelhead EX appliance

Related Topics

"ipv6 data route," "ip data route," "ip data-gateway," "hardware nic slot"

storage core add host

Description

Configures the Granite Core connection.

Syntax

storage core add host <hostname> edge-id <id> [port <port>] [local-interface <aux | primary>]

Parameters

host <hostname>	Specify the hostname of the Granite Core host device.
edge-id <id>	Specify the self-identifier of the Granite Core device.
port <port>	Optionally, specify the port the Granite Core device is to listen on.
local-interface {aux | primary}	Optionally, specify the local interface for the connection to the Granite Core device.

Usage

Use this command to specify and configure the connection to the intended Granite Core host.

Example

```
Edge1 (config) # storage core add host CoLo2 edge-id Branch1 local-interface aux
```

Product

Steelhead EX appliance

Related Topics

"show storage core," "show service storage," "storage core host local-interface," "storage core remove,"

storage core host interface

Description

Configures Granite Core interface connection settings.

Syntax

storage core host <hostname> interface {add <hostname> [port <port>] | remove <hostname>}

Parameters

host <hostname>	Specify the hostname of the Granite Core host device.
add <hostname>	Specify to add additional Granite Core hostnames.
port <port>	Optionally, specify the port the Granite Core device is to listen on.
remove <hostname>	Specify to remove the Granite Core hostnames.

Example

```
Edge1 (config) # storage core host CoLo1 interface add CoLo2
```

Product

Steelhead EX appliance

Related Topics

"storage core add host," "show storage core," "storage core remove"

storage core host local-interface

Description

Configures Granite Core local interface connection settings.

Syntax

storage core host <hostname> local-interface {add <local-interface-name> | remove <local-interface-name>}

Parameters

host <hostname>	Specify the hostname of the Granite Core host device.
add <local-interface-name>	Specify to add the local interface used to connect to the Granite Core device.
remove <local-interface-name>	Specify to remove the local interface used to connect to the Granite Core device.

Example

```
Edge1 (config) # storage core host CoLo1 local-interface add primary
```

Product

Steelhead EX appliance

Related Topics

"storage core add host," "show storage core," "storage core remove"

storage core host modify

Description

Modifies the existing Granite Core connection settings.

Syntax

storage core host <hostname> modify {port <port> | new-host <host>}

Parameters

host <hostname>	Specify the hostname of the Granite Core host device.
port <port>	Specify the port the Granite Core device is to listen on.
new-host <host>	Specify the new hostname of the Granite Core host device.

Example

```
Edge1 (config) # storage core host CoLo2 modify new-host Calif2
```

Product

Steelhead EX appliance

Related Topics

"storage core add host," "show storage core," "storage core remove"

storage core remove

Description

Removes the connection to the specified Granite Core host device.

Syntax

storage core remove host <hostname> [force]

Parameters

host <hostname>	Specify the hostname of the Granite Core host device.
force	Specify this parameter to skip the validation check and force the removal, even if the LUNs are still online. **Caution:** Data from online LUNs might be lost. Riverbed strongly recommends that you take the LUN offline first.

Usage

Before using this command, Riverbed strongly recommends that you take offline the LUNs associated with the Granite Core host device.

Example

```
Edge1 (config) # storage core remove CoLo2
```

Product

Steelhead EX appliance

Related Topics

"show storage core," "show service storage"

storage iscsi mpio interface

Description

Adds or removes the specified multi-path I/O (MPIO) interface.

Syntax

storage iscsi mpio interface {add <mpio-interface> | remove <mpio-interface>}

Parameters

add <mpio-interface>	Specify an MPIO interface to add: **aux**, **inpath0_0**, **primary**, **vmaux**, **vmlocal**, or **vmpri.**
remove <mpio-interface>	Removes an MPIO interface.

Usage

MPIO interfaces connect the Granite Core appliance to the network and to the filer through multiple physical interfaces. These redundant connections help prevent loss of connectivity in the event of an interface, switch, cable, or other physical failure.

Example

```
Edge1 (config) # storage iscsi mpio interface primary
```

Product

Steelhead EX appliance

Related Topics

"show storage iscsi"

storage snapshot create

Description

Creates a storage snapshot on the specified LUN.

Syntax

storage snapshot create {lun-alias <lun-alias> | lun-serial <lun-serial>}

Parameters

lun-alias <lun-alias>	Creates a storage snapshot on the LUN specified by the configured alias value number.
lun-serial <lun-serial>	Creates a storage snapshot on the LUN specified by the configured serial number.

Usage

Before using this command, Riverbed recommends that you take offline the LUNs associated with the Granite Core host device.

Example

```
Edge1 (config) # storage snapshot create lun-alias LUN2
```

Product

Steelhead EX appliance

Related Topics

"show storage snapshot"

storage snapshot remove

Description

Removes a storage snapshot on the specified LUN.

Syntax

storage snapshot remove id <snapshot-id>

Parameters

id <snapshot-id>	Removes the private storage snapshot for the LUN as specified by the ID value.

Usage

Before using this command, Riverbed strongly recommends that you take offline the LUNs associated with the Granite Core host device.

Example

```
Edge1 (config) # storage snapshot remove id 308
```

Product

Steelhead EX appliance

Related Topics

"show storage snapshot"

Displaying Branch Storage Information

This section describes the **show** commands for displaying branch storage information.

show device-failover

Description

Displays the failover settings for the current Granite Edge device or Granite Edge-enabled Steelhead appliance.

Syntax

show device-failover

Parameters

None

Example

```
Edge1 # show device-failover
Device failover settings
        Failover peer hostname    : Edge1-234
        Local state               : Active Sync
Heartbeat Connections
         10.13.8.172 -> 10.13.10.229 : true
         10.14.8.172 -> 10.14.10.229 : true
```

Product

Steelhead EX appliance

Related Topics

"device-failover peer set"

show disk-config

Description

Displays the disk configuration layout as specified by the parameters.

Syntax

show disk-config {layout | avail-layouts}

Parameters

layout	Displays the current disk configuration layout.
avail-layouts	Displays available disk configuration layouts.

Example

```
Edge1 # show disk-config layout
Layout: vsp_granite
Description: VSP and Granite Storage Mode
        Volume: var
        Size: 16385Mb
        Volume: vecache
        Size: 9523Mb
        Volume: shark_pfs
        Size: 51200Mb
        Volume: swap
        Size: 4096Mb
        Volume: segstore
        Size: 132506Mb
        Volume: vsp
        Size: 285696Mb
        Volume: ve
        Size: 571392Mb
```

Product

Steelhead EX appliance

Related Topics

"disk-config layout"

show service storage

Description

Displays the status of the Granite Edge service.

Syntax

show service storage

Parameters

None

Example

```
Edge1 # show service storage
Granite-Edge Service: Running
```

Product

Steelhead EX appliance

Related Topics

"show storage core"

show stats storage initiator-bytes

Description

Displays the number of bytes written to and read from the block store via the specified initiator for the specified period of time.

Syntax

show stats storage initiator-bytes {interval <time-interval> initiator <initiator> | start-time <start> end-time <end> initiator <initiator>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **initiator <initiator>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **initiator <initiator>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **initiator <initiator>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
initiator <initiator>	Specify the name of the initiator.

Example

```
Edge1 # show stats storage initiator-bytes interval month initiator iqn.1998-
01.com.vmware:localhost-29e36c8b
Total Bytes Read: 217.86 MB
Total Bytes Written : 6.30 MB
```

Product

Steelhead EX appliance

Related Topics

"show stats storage initiator-iops," "show stats storage initiator-ltncy"

show stats storage initiator-iops

Description

Displays the standard I/O operations per second written to and read from the block store via the specified initiator for the specified period of time.

Syntax

show stats storage initiator-iops {interval <time-interval> initiator <initiator> | start-time <start> end-time <end> initiator <initiator>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **initiator <initiator>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **initiator <initiator>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **initiator <initiator>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
initiator <initiator>	Specify the name of the initiator.

Example

```
Edge1 # show stats storage initiator-iops interval month initiator iqn.1998-
01.com.vmware:localhost-29e36c8b
Average Read IOPS: 0
Average Write IOPS: 0
```

Product

Steelhead EX appliance

Related Topics

"show stats storage initiator-bytes," "show stats storage initiator-ltncy"

show stats storage initiator-ltncy

Description

Displays the average read and write latency for blocks written to and read from the block store via the specified initiator for the specified period of time.

Syntax

show stats storage initiator-ltncy {interval <time-interval> initiator <initiator> | start-time <start> end-time <end> initiator <initiator>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **initiator <initiator>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **initiator <initiator>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **initiator <initiator>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
initiator <initiator>	Specify the name of the initiator.

Example

```
Edge1 > show stats storage initiator-ltncy interval month initiator all
Time: msre:localhost-29e36c8b
Avg Write IO Time: 4 ms
```

Product

Steelhead EX appliance

Related Topics

"show stats storage initiator-bytes," "show stats storage initiator-iops"

show stats storage lun-bytes

Description

Displays the number of bytes written to and read from the specified LUN for the specified period of time.

Syntax

show stats storage lun-bytes {interval <time-interval> lun <lun-id> | start-time <start> end-time <end> lun <lun-id>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **lun <lun-id>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
lun <lun-id>	Specify the name of the LUN.

Usage

Use this command to display the number of megabytes written to and read from the specified LUN for the specified period.

Example

```
Edge1 # show stats storage lun-bytes interval month lun lun2
Total Bytes Read: 571.23 MB
Total Bytes Written : 19.77 MB
Total Hit Count : 558.10 MB
Total Miss Count : 171.50 KB
Mean Commit delay : 0s
Total Bytes Written : 6.64 MB
Total Committed Bytes : 6.64 MB
Total Uncommitted Bytes : 0 Bytes
```

Product

Granite Edge-enabled Steelhead EX appliance

Related Topics

"show stats storage lun-commit-rate"

show stats storage lun-commit-rate

Description

Displays the commit rate for the specified LUN for the specified period of time.

Syntax

show stats storage lun-commit-rate {interval <time-interval> lun <lun-id> | start-time <start> end-time <end> lun <lun-id>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **lun <lun-id>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <start>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
lun <lun-id>	Specify the name of the LUN. Optionally, you can specify **all** to display information for all configured LUNs.

Usage

Use this command to display the commit rates for the specified LUN for the specified period.

Example

```
Edge1 (config) # show stats storage lun-commit-rate interval month lun lun2
```

Product

Granite Edge-enabled Steelhead EX appliance

Related Topics

"show stats storage lun-latency," "show stats storage lun-bytes"

show stats storage lun-iops

Description

Displays the commit rate for the specified LUN for the specified period of time.

Syntax

show stats storage lun-iops {interval <time-interval> lun <lun-id> | start-time <start> end-time <end> lun <lun-id>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **lun <lun-id>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <start>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
lun <lun-id>	Specify the name of the LUN. Optionally, you can specify all to display information for all configured LUNs.

Usage

Use this command to display the number of megabytes and operations written to and read from the specified LUN for the specified period.

Example

```
Edge1 # show stats storage lun-iops interval month lun lun2
```

Product

Steelhead EX appliance

Related Topics

"show stats storage lun-latency," "show stats storage lun-bytes"

show stats storage lun-latency

Description

Displays the average read and write latency for the specified LUN for the specified period of time.

Syntax

show stats storage lun-latency {interval <time-interval> lun <lun-id> | start-time <start> end-time <end> lun <lun-id>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **lun <lun-id>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <start>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
lun <lun-id>	Specify the name of the LUN.

Usage

Use this command to display the average read and write latencies for the specified LUN for the specified period.

Example

```
Edge1 (config) # show stats storage lun-latency interval month lun lun2
Avg Read IO Time: 0 ms
Avg Write IO Time: 0 ms
```

Product

Steelhead EX appliance

Related Topics

"show stats storage lun-bytes"

show stats storage network-bytes

Description

Displays the number of bytes written to and read from the network for the specified period of time.

Syntax

show stats storage network-bytes {interval <time-interval> | start-time <start> end-time <end>}

Parameters

interval <time-interval>	Use this parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** parameter to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** parameter to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.

Usage

Use this command to display the number of bytes written to and read from the network for the specified period.

Example

```
Edge1 (config) # show stats storage network-bytes interval month
Total Data Read: 3 Bytes
Total Data Written: 0 Bytes
```

Product

Steelhead EX appliance

Related Topics

"show stats storage lun-bytes" "show stats storage initiator-bytes"

show storage core

Description

Displays detailed status and information about the configured Granite Core.

Syntax

show storage core

Parameters

None

Example

```
Edge1 # show storage core
Granite-Core: kabar-core.lab
  Configuration status:    Ready
  Address:                 10.1.32.120
  Port:                    7970
  Local Interface:         aux
  Connectivity:            yes
  Id:                      main-sh123
```

Product

Steelhead EX appliance

Related Topics

"storage core add host," "storage core host local-interface," "storage core remove"

show storage iscsi

Description

Displays the iSCSI target configuration details based on the parameters specified.

Syntax

show storage iscsi [initiators [name <initiator>] | initiator-group [name <initiator group>] | lun-alias <lun-alias> | lun-serial <lun-serial> | luns | mpio interfaces | targets]

Parameters

initiators [name <initiator>]	Specify this parameter to display information specific to iSCSI initiator credentials. Optionally, specify the name of a specific initiator to limit the output to information about that initiator.
initiator-group [name <initiator group>]	Specify this parameter to display the details of iSCSI initiator groups, including configuration status and the initiators in the group.
lun-alias <lun-alias>	Specify the LUN alias to display LUN details, including configuration status, size, type, vendor, serial number, and so on. **Note:** Alternatively, you can identify the LUN by its serial number. See the following parameter.
lun-serial <lun-serial>	Specify the LUN serial number to display LUN details, including configuration status, size, type, vendor, serial number, and so on. **Note:** Alternatively, you can identify the LUN by its alias. See the preceding parameter.
luns	Specify this parameter to display the details of all configured LUNs, including configuration status, size, type, vendor, serial number, and so on.
mpio interfaces	Specify this parameter to display the details of multi-path I/O interfaces.
targets	Specify this parameter to display the details of iSCSI targets, including description, security-only status, header-digest status, data-digest status, initiator groups, initiator credentials, and network portals.

Example

```
Edge1 # show storage iscsi
General iSCSI target Configuration:
  Packet data digest:                 Enabled
  Packet header digest:               Enabled
```

Product

Steelhead EX appliance

Related Topics

"show stats storage initiator-bytes," "show stats storage initiator-iops," "show storage core," "show service storage," "storage iscsi mpio interface"

show storage snapshot

Description

Displays the private storage snapshot for the specified LUN connection.

Syntax

show storage snapshot {all | id <snapshot-id> | lun-alias <lun-alias> | lun-serial <lun-serial>}

Parameters

all	Displays the private storage snapshot for all configured LUN connections.
id <snapshot-id>	Displays the private storage snapshot for the LUN as specified by the ID value.
lun-alias <lun-alias>	Displays the private storage snapshot for the LUN as specified by the LUN alias.
lun-serial <lun-serial>	Displays the private storage snapshot for the LUN as specified by the serial number.

Example

```
Edge1 (config) # show storage snapshot all
```

Product

Steelhead EX appliance

Related Topics

"storage snapshot create"

VSP Commands

This section describes the Virtual Services Platform (VSP) commands. You can use VSP to consolidate basic services in the branch (such as print, DNS, and DHCP services) to run in a dedicated partition on the Steelhead EX appliance. VSP offers a VM-based virtualization platform with the most commonly deployed and advanced virtualization tool set. VSP uses ESXi 5.0 as the virtualization platform.

VSP is included in the Steelhead EX appliance functionality and does not require a separate download or license. For detailed information about configuring VSP, see the *Steelhead EX Management Console User's Guide*.

Note: VSP is supported on Steelhead appliance EX *xx*60 models.

Note: Data flow is not supported in EX v2.0.

This section also contains:

- "Displaying VSP Information"

vsp esxi license restore

Description

Restores the default ESXi embedded license.

Syntax

vsp esxi license restore

Parameters

None

Usage

Use this command to replace the existing ESXi license with the default ESXi license, which does not have vCenter functionality.

Example

```
Edge1 (config) # vsp esxi license restore
```

Product

Steelhead EX appliance

Related Topics

"Displaying VSP Information"

vsp esxi password

Description

Specify the VSP ESXi password.

Syntax

vsp esxi password <password string>

Parameters

<password string>	Specify the ESXi password.

Usage

When a password is not synchronized between the RiOS software and ESXi, RiOS cannot communicate with ESXi. The **vsp esxi password** command synchronizes the new password between RiOS and ESXi or pushes the new password to ESXi, depending on the current status of connectivity from RiOS to ESXi.

The **esxi_communication_failed** alarm is triggered if RiOS cannot communicate with ESXi because of a password problem or any other connection problem.

Example

```
Edge1 (config) # vsp esxi password work736
```

Product

Steelhead EX appliance

Related Topics

"Displaying VSP Information"

vsp esxi push-config license key

Description

Configures the RiOS software to push a custom ESXi license key to the ESXi configuration.

Syntax

[no] vsp esxi push-config license key <license key>

Parameters

<license key>	Specify the ESXi license key.

Usage

Use this command to push the custom license key to the ESXi configuration.

Example

```
Edge1 (config) # vsp esxi push-config license key LK1-foo-branch
```

Product

Steelhead EX appliance

Related Topics

“show vsp esxi push-config network”

vsp esxi push-config network ip default-gw

Description

Configures the RiOS software to push the default ESXi IPv4 gateway address to the ESXi configuration.

Syntax

[no] vsp esxi push-config network ip default-gw <gateway-IPv4 address>

Parameters

<gateway-IPv4 address>	Specify the default ESXi IPv4 gateway address for the ESXi configuration.

Usage

The **no** version of the command deletes the ESXi default gateway.

Example

```
Edge1 (config) # vsp esxi push-config network ip default-gw 10.5.16.233
```

Product

Steelhead EX appliance

Related Topics

“show vsp esxi push-config network”

vsp esxi push-config network ip interface enable

Description

Enables the RiOS software to push the configured network IP interface settings to the ESXi configuration.

Syntax

[no] vsp esxi push-config network ip interface <interface-name> enable

Parameters

<interface-name>	Specify the interface name. Choose either **vmk1** for the primary interface or **vmk2** for the auxiliary interface..

Usage

You manage VSP and ESXi through the primary and auxiliary interfaces, using VMware tools such as vSphere Client and vCenter.

If you disable a vmk interface and later decide to enable it, you must either manually create the vmk interface through vSphere or reinstall VSP.

Example

```
Edge1 (config) # vsp esxi push-config network ip interface vmk1 enable
```

Product

Steelhead EX appliance

Related Topics

"show vsp esxi push-config network"

vsp esxi push-config network ip interface ipv4

Description

Configures the ESXi interface IPv4 network interface settings for the ESXi configuration.

Syntax

[no] vsp esxi push-config network ip interface <interface-name> ipv4 {dhcp enable | dhcp-dns enable | static address <ipv4 address> netmask <netmask>}

Parameters

<interface-name>	Specify the interface name. Choose either **vmk1** for the ESXi primary interface or **vmk2** for the ESXi auxiliary interface.
ipv4 dhcp enable	Specify this option to automatically obtain the ESXi IPv4 address from a DHCP server. A DHCP server must be available so that the system can request the IP address from it.
ipv4 dhcp-dns enable	Specify this option to dynamically obtain IPv4 network settings from a DNS server using dynamic DNS.
ipv4 static address <ipv4 address> netmask <netmask>	Specify the ESXi IPv4 address and IPv4 subnet mask. Use this option if you do not use a DHCP server to automatically obtain an IP address.

Usage

You manage VSP and ESXi through the primary and auxiliary interfaces using VMware tools such as vSphere Client and vCenter.

Example

```
Edge1 (config) # vsp esxi push-config network ip interface vmk1 ipv4 dhcp enable

Edge1 (config) # vsp esxi push-config network ip interface vmk2 ipv4 static address 192.105.1.27
netmask 255.255.255.0
```

Product

Steelhead EX appliance

Related Topics

"show vsp esxi push-config network"

vsp esxi push-config network vsphere interface

Description

Configures the RiOS software to push the vSphere network interface settings to the ESXi configuration.

Syntax

vsp esxi push-config network vsphere interface <interface name>

Parameters

<interface-name>	Specify the interface name. Choose either **vmk1** for the ESXi primary interface or **vmk2** for the ESXi auxiliary interface. The default interface is **vmk1**.

Usage

Use this command to specify which interface vSphere Client or vCenter uses for management access.

If you disable a vmk interface and later decide to enable it, you must either manually create the vmk interface through vSphere or reinstall VSP.

Example

```
Edge1 (config) # vsp esxi push-config network vsphere interface vmk1
```

Product

Steelhead EX appliance

Related Topics

"show vsp esxi push-config network"

vsp esxi push-config ntp enable

Description

Configures the RiOS software to push te RiOS NTP server settings to the ESXi configuration.

Syntax

[no] vsp esxi push-config ntp enable

Parameters

None

Usage

Riverbed strongly recommends using the RiOS NTP server settings to ensure consistent time synchronization between the RiOS software and your virtual machines. The **no** version of the command resets the NTP server settings to the default.

Example

```
Edge1 (config) # vsp esxi push-config ntp enable
```

Product

Steelhead EX appliance

Related Topics

"show vsp esxi push-config ntp"

vsp esxi rios-mgmt-ip

Description

Configures the IPv4 address to which the RiOS software connects to the local ESXi configuration.

Syntax

[no] vsp esxi rios-mgmt-ip <ipv4-address>

Parameters

<ipv4-address>	Specify the IPv4 address of the local ESXi configuration.

Usage

The **no** version of this command resets the IPv4 address to the default value.

Example

```
Edge1 (config) # vsp esxi rios-mgmt-ip 10.22.12.3
```

Product

Steelhead EX appliance

Related Topics

"show vsp esxi rios-mgmt-ip"

vsp esxi vnc enable

Description

Enables the use of a VNC (Virtual Network Computing) client to connect directly to an ESXi host that is running on a Steelhead EX appliance.

Syntax

[no] vsp esxi vnc enable

Parameters

None

Usage

VNC must be running and indicate an active status before you can connect to the ESXi host on the Steelhead EX appliance.

The **no** version of the command disables the VNC capability.

Example

```
Edge1 (config) # vsp esxi vnc enable
```

Product

Steelhead EX appliance

Related Topics

"vsp esxi vnc password," "vsp esxi vnc port"

vsp esxi vnc password

Description

Configures the VNC password.

Syntax

[no] vsp esxi vnc password <password>

Parameters

<password>	Specify the password. The VNC password cannot exceed eight characters.

Usage

Use the **no vsp esxi vnc password <password>** command to remove the VNC password.

Example

```
Edge1 (config) # vsp esxi vnc password brch8106
```

Product

Steelhead EX appliance

Related Topics

"vsp esxi vnc enable," "vsp esxi vnc port"

vsp esxi vnc port

Description

Configures the VNC port number of the virtual machine.

Syntax

[no] vsp esxi vnc port <vnc-port>

Parameters

<vnc-port>	Specify the port number. By default, a VNC client uses port 5900.

Usage

The **no vsp esxi vnc port** command returns the VNC port to the default port.

Example

```
Edge1 (config) # vsp esxi vnc port 5800
```

Product

Steelhead EX appliance

Related Topics

"vsp esxi vnc enable," "vsp esxi vnc password"

vsp install

Description

Runs the VSP service wizard and installs ESXi.

Syntax

vsp install {esxi-password <password>}

Parameters

esxi-password <password>	Specify the ESXi root password that was set during installation.

Usage

Before you use this command, you should configure the disk layout for VSP by using the **disk-config layout** command. To install VSP, ensure that you have allocated disk space to VSP in either the stand-alone modes using the **disk-config layout vsp** or **disc-config layout vsp_ext** commands or the mixed modes using the **disk-config layout vsp_granite** or **disk-config layout vsp_granite_ext** commands.

Example

```
Edge1 (config) # vsp install esxi-password branch08
```

Product

Steelhead EX appliance

Related Topics

"disk-config layout," "vsp reinstall esxi-password"

vsp reinstall esxi-password

Description

Reinstalls ESXi configurations and restarts VSP.

Syntax

vsp reinstall esxi-password <password> [wipe-datastore]

Parameters

<password>	Specify the new ESXi root password set during reinstallation.
wipe-datastore	Optionally, reinstall ESXi with ESXi configurations in RiOS software, re-create the local data store, and restart VSP.

Usage

After reinstallation, the new password set by the **vsp reinstall** command overrides the previous password set by the **vsp install** command.

When you enter this command, the CLI returns the following alert:

```
WARNING: This will wipe out the current ESXi installation, please backup any ESXi data if necessary.
To proceed, use this command:
 'vsp reinstall esxi-password <password> confirm'
```

To complete the action, you must enter the confirmation as prompted. This action restarts VSP.

When you enter this command with the **wipe-datastore** option, the CLI returns the following alert:

```
WARNING: This will wipe out the current ESXi installation and local datastore, please backup any
ESXi data if necessary. To proceed, use this command:
 'vsp reinstall esxi-password <password> wipe-datastore confirm'
```

To complete the action, you must enter the confirmation as prompted. This action restarts VSP.

Example

```
Edge1 (config) # vsp reinstall esxi-password branch213
```

Product

Steelhead EX appliance

Related Topics

"vsp install"

vsp restart

Description

Restarts VSP.

Syntax

vsp restart [force]

Parameters

force	Optionally, force a restart of VSP.

Usage

Use the **vsp restart force** command option to immediately force the restart of VSP.

Example

```
Edge1 (config) # vsp restart
```

Product

Steelhead EX appliance

Related Topics

"Displaying VSP Information"

vsp v1 backup delete

Description

Deletes the VSP version 1 backup file.

Syntax

vsp v1 backup <backup filename> delete

Parameters

<backup filename>	Specify the backup name: **<Steelhead appliance name>-<slotname>-<date>.bkup**.

Example

```
Edge1 (config) # vsp v1 backup gen-sh1-1-20120608-223616.bkup delete
```

Product

Steelhead EX appliance

Related Topics

"show vsp v1 backup"

vsp v1 backup upload

Description

Uploads the VSP version 1 backup file onto a remote server or another Steelhead EX appliance.

Syntax

vsp v1 backup <backup filename> upload <backup URL>

Parameters

<backup filename>	Specify the backup filename: **<Steelhead appliance name>-<slotname>-<date>.bkup.**
<backup URL>	Specify the URL or path name. You can use FTP or SCP to upload the backup file: `scp://username:password@host/path`

Example

```
Edge1 (config) # vsp v1 backup Edge1-1-20120608-223616.bkup upload scp://admin:mypassword@Edge1-
sh2/var/tmp/vsp_backups/
```

Product

Steelhead EX appliance

Related Topics

"show vsp v1 backups," "show vsp"

vsp v1 package delete

Description

Deletes a VSP version 1 package installation file.

Syntax

vsp v1 package <package> delete

Parameters

<package>	Specify the package name.

Usage

If you used VSP with EX v1.0, you can access your v1.0 packages, slots, and backups and migrate them to v2.0. The process involves transferring your data from the EX appliance; converting your packages, slots, and backups; and installing the resulting virtual machines. After you have migrated, or if you choose not to migrate a slot, you can delete the slot to free space.

Example

```
Edge1 (config) # vsp v1 package delete SCPS_factory1.pkg
```

Product

Steelhead EX appliance

Related Topics

"show vsp," "show vsp v1 disk-space," "show vsp v1 packages"

vsp v1 package upload

Description

Uploads a VSP version 1 package to a remote server using a URL.

Syntax

vsp v1 package <package> upload <url>

Parameters

<package>	Specify the package name.
<url>	Specify the URL or path name. You can use FTP or SCP to upload the package: `scp://username:password@host/path`

Example

```
Edge1 (config) # vsp v1 package VSP_factory1.pkg upload scp://admin:mypassword@Edge1-sh2/var/tmp/
vsp_packages/
```

Product

Steelhead EX appliance

Related Topics

"show vsp," "show vsp v1 disk-space," "show vsp v1 packages"

vsp v1 slot archive create

Description

Creates an archive of an existing VSP version 1 slot.

Syntax

vsp v1 slot <slot-name> archive create

Parameters

<slot-name>	Specify the slot name.

Usage

Steelhead EX v2.0 provides a redesigned virtualization platform based on ESXi 5.0. Because of the differences between VSP in EX v1.0 (based on VMware Server 2.0) and VSP in EX v2.0 (based on ESXi), seamless migration of packages and slots from EX v1.0 to v2.0 is not possible.

The process involves migrating your packages, slots, and backups offline and installing the resulting virtual machines.

You must create archives of your existing VSP slots, upload them to a remote server (or download them to a browser), and move them to your Steelhead EX v2.0 appliance.

Depending on the size and characteristics of the archive, this command can take a long time to complete.

Due to the architecture of EX v2.0, the following types of slots do not work correctly if migrated directly to Steelhead EX v2.0:

- **Slots that contain data flow** - Data flow is not supported in EX v2.0. You can convert the packages, but connecting to the network does not work correctly.
- **Slots using watchdogs** - Because ESXi does not have any kind of Virtual Machine level watchdog, slots with watchdogs (both serial and ping) will not have working watchdog functionality.

All other VSP functionality from Steelhead EX v1.0 works as expected.

Example

```
Edge1 (config) # vsp v1 slot vspv1slot archive create
```

Product

Steelhead EX appliance

Related Topics

"Displaying VSP Information"

vsp v1 slot archive delete

Description

Deletes an archive of an existing VSP version 1 slot.

Syntax

vsp v1 slot <slot-name> archive delete [force]

Parameters

<slot-name>	Specify the slot name.

Usage

If you used VSP with EX v1.0, you can access your v1.0 packages, slots, and backups and migrate them to v2.0. The process involves transferring your data from the EX appliance; converting your packages, slots, and backups; and installing the resulting virtual machines. After you have migrated, or if you choose not to migrate a slot, you can delete the slot to free space.

Example

```
Edge1 (config) # vsp v1 slot 1 archive delete
```

Product

Steelhead EX appliance

Related Topics

"Displaying VSP Information"

vsp v1 slot archive upload

Description

Uploads the VSP version 1 slot archive onto a remote server or another Steelhead EX appliance.

Syntax

vsp v1 slot <slot-name> archive upload <url>

Parameters

<slot-name>	Specify the slot name.
<url>	Specify the URL or path name. You can use FTP or SCP to upload the slot archive: `scp://username:password@host/path`

Usage

Steelhead EX v2.0 provides a redesigned virtualization platform based on ESXi 5.0. Because of the differences between VSP in EX v1.0 (based on VMware Server 2.0) and VSP in EX v2.0 (based on ESXi), seamless migration of packages and slots from EX v1.0 to v2.0 is not possible.

The process involves migrating your packages, slots, and backups offline and installing the resulting virtual machines.

You must create archives of your existing VSP slots. After the archive is complete, upload your archive to a remote server using the **vsp v1 slot archive upload** command.

Example

```
Edge1 (config) # vsp v1 slot 1 archive upload scp://admin:mypassword@Edge1-sh2/var/tmp/
vsp_slot_archives/
```

Product

Steelhead EX appliance

Related Topics

"Displaying VSP Information"

vsp v1 slot delete

Description

Deletes the VSP version 1 slot.

Syntax

vsp v1 slot <slot-name> delete [force]

Parameters

<slot-name>	Specify the slot name.

Example

```
Edge1 (config) # vsp v1 slot 1 delete
```

Product

Steelhead EX appliance

Related Topics

"Displaying VSP Information"

vsp v1 slot vm-migration

Description

Migrates and deploys virtual machines to VSP directly on the Steelhead EX appliance.

Syntax

vsp v1 slot <slot-name> vm-migration datastore <name> network-map <net_map> [disk-mode <mode>] [preserve-info uuid] [vm-name <vm_name>]

Parameters

<slot-name>	Specify the slot name.
datastore <name>	Specify the datastore name.
network-map <net_map>	Specify to map the source network to the destination network. Use the format <src1>=<dst1>[,<src2>=<dst2>,...].
disk-mode <mode>	Specify the disk provisioning mode: • **lazy-thick** - thick provisioned lazy zeroed • **eager-thick** - eager thick provisioned lazy zeroed • **thin** - thin provisioned
preserve-info uuid	Select the source VM UUID identity information to preserve.
vm-name <vm_name>	Specify the target VM name. If not specified, the name defaults to the slot name.

Usage

Steelhead EX v2.x provides a redesigned virtualization platform based on ESXi 5.0. Due to the differences between VSP in Steelhead EX v1.x (based on VMware Server 2.0) and VSP in EX v2.x (based on ESXi), Steelhead EX 1.0 virtual machines must be converted to Steelhead EX 2.x format..

Steelhead EX v2.1 and later provides an improved migration method that converts an existing VM installed in a slot to a VM in ESXi without the need to migrate the VM offline and off the appliance. You can perform migration tasks directly on the Steelhead EX appliance.

Some VMs require that you preserve the universally unique identifiers (UUIDs). For example, the SMC-VE needs to preserve the UUID for licensing reasons. The existing SMC-VE license is generated based on UUID. Preserving the UUID allows you to keep the existing license without regenerating a license after VM migration.

Use the **show vsp v1 slot** command to monitor the progress of the migration. The output of this command shows the completion percentage and estimated time remaining to complete the migration process.

The process supports only one active VM migration task at any one time. For detailed information about configuring VSP, see the *Steelhead EX Management Console User's Guide*.

Note: The conversion process is resource intensive and can take several hours, depending on the size of the VM. Appliance performance might be degraded during this time.

Example

```
Edge1 (config) # vsp v1 slot 1 vm-migration datastore riverbed_000eb6025880 network-map
scrnet1=rvbd_hpd_vm_network,srcnet2=rvbd_aux_vm_network disk-mode thick
```

Product

Steelhead EX appliance

Related Topics

"Displaying VSP Information," "show vsp v1 slot"

vsp v1 vm-migration cancel

Description

Cancels the active VM migration.

Syntax

vsp v1 vm-migration cancel

Parameters

None

Usage

The process supports only one active VM migration task at any one time.

You must open a second CLI session to initiate the **vsp v1 vm-migration cancel** command. The active session started by using the **vsp v1 slot vm-migration** command is blocked until the VM migration finishes, an error occurs, or you use the v**sp v1 vm-migration cancel** command in a second CLI session.

This command erases any partially migrated VMs from the system.

Example

```
Edge1 (config) # vsp v1 vm-migration cancel
Successfully cancelled VM migation task
```

Product

Steelhead EX appliance

Related Topics

"Displaying VSP Information," "vsp v1 slot vm-migration"

Displaying VSP Information

This section describes the **show** commands for displaying VSP information.

show vsp

Description

Displays VSP settings.

Syntax

show vsp

Parameters

None

Example

```
Edge1 >  show vsp
 VSP Status:                available
 VSP CPU cores:             4
 VSP Memory:                15.5 GB
 VSP Disk Space:            277.0 GB
 Interface vmlocal status:  running
 Interface vmpri status:    running
 Interface vmaux status:    running
 VNC Enable:                false
 VNC Port:                  5900
 ESXi Iqn:                  iqn.1998-01.com.vmware:localhost-0feca5eb
```

The following output example shows that there is a connection issue and RiOS cannot connect to ESXi:

```
Edge1 >  show vsp
 VSP Status:                disconnected
 VSP CPU cores:             4
[partial output]
```

The following output example shows that there is a connection issue and the ESXi password is out of synchronization with RiOS:

```
Edge1 >  show vsp
 VSP Status:                invalid ESXi password
 VSP CPU cores:             4
[partial output]
```

Product

Steelhead EX appliance

Related Topics

"VSP Commands"

show vsp configured

Description

Displays VSP configuration information.

Syntax

show vsp configured

Parameters

None

Example

```
Edge1 > show vsp configured
VSP Enabled: yes
VNC Enable:  no
VNC Port:    5900
```

Product

Steelhead EX appliance

Related Topics

"VSP Commands"

show vsp esxi push-config network

Description

Displays network configurations pushed to the ESXi configuration.

Syntax

show vsp esxi push-config network {dns | ip {default-gw | interface} | vsphere interface | vswitches}

Parameters

dns	Displays DNS configurations pushed to the ESXi configuration.
ip interface	Displays ESXi IPv4 interface settings pushed to the ESXi configuration.
vsphere interface	Displays vSphere interface settings pushed to the ESXi configuration.
vswitches	Displays vswitch settings pushed to the ESXi configuration.

Example

```
Edge1 > show vsp esxi push-config network dns
Manually add name servers
  10.16.0.30
Domain name
  nbttech.com
  riverbed.com
  lab.nbttech.com

Edge1 > show vsp esxi push-config network vswitches
Name                           Type #Ports MTU   Active
------------------------------ ---- ------ ----- ----------
rvbd_vswitch_aux                    128    1500  vmnic2
  |-> rvbd_aux_portgrp0        vmk
  |-> rvbd_aux_portgrp1        vm
rvbd_vswitch_pri                    128    1500  vmnic1
  |-> rvbd_pri_portgrp0        vmk
  |-> rvbd_pri_portgrp1        vm
vSwitch0                            128    1500  vmnic0
  |-> Management Network       vmk

3 user-defined vSwitch(es)
```

Product

Steelhead EX appliance

Related Topics

"vsp esxi push-config network ip interface ipv4"

show vsp esxi push-config ntp

Description

Displays NTP information pushed to the ESXi configuration.

Syntax

show vsp esxi push-config ntp

Parameters

None

Example

```
Edge1 > show vsp esxi push-config ntp
Push RiOS NTP Config to ESXi:      no
NTP enabled in RiOS:               yes
NTP Startup Policy:                Start and stop with host
NTP servers configured in RiOS
 Name                           Enabled
 ------------------------------ -------
 0.riverbed.pool.ntp.org        true
 1.riverbed.pool.ntp.org        true
 2.riverbed.pool.ntp.org        true
 208.70.196.25                  true
 3.riverbed.pool.ntp.org        true
```

Product

Steelhead EX appliance

Related Topics

"vsp esxi push-config ntp enable"

show vsp esxi rios-mgmt-ip

Description

Displays the IP address connecting RiOS software to the ESXi configuration.

Syntax

show vsp esxi rios-mgmt-ip

Parameters

None

Example

```
Edge1 > show vsp esxi rios-mgmt-ip
RiOS connects to ESXi using IP address: 169.254.199.2
```

Product

Steelhead EX appliance

Related Topics

"vsp esxi rios-mgmt-ip"

show vsp esxi runtime network

Description

Displays ESXi runtime information.

Syntax

show vsp esxi runtime network {default-gateway | vmk interfaces}

Parameters

default-gateway	Displays the ESXi IPv4 runtime default gateway.
vmk interfaces	Displays information about the configured VM kernel interfaces.

Example

```
Edge1 > show vsp esxi runtime network vmk interfaces
```

```
vmk0(local):
    MTU: 1500
    MAC: 02:0E:B6:02:58:80
    IPv4 Type: DHCP
    IPv4 Address: 169.254.199.2
    IPv4 Netmask: 255.255.255.0
vmk1(primary):
    MTU: 1500
    MAC: 00:0E:B6:02:58:82
    IPv4 Type: STATIC
    IPv4 Address: 10.1.2.3
    IPv4 Netmask: 255.255.0.0
vmk2(aux):
    MTU: 1500
    MAC: 00:0E:B6:02:58:83
    IPv4 Type: DHCP
    IPv4 Address: 192.168.1.2
    IPv4 Netmask: 255.255.255.0
```

Product

Steelhead EX appliance

Related Topics

"VSP Commands"

show vsp esxi version

Description

Displays ESXi version information.

Syntax

show vsp esxi version

Parameters

None

Example

```
Edge1 > show vsp esxi version
Support Status:  supported
Current Version: 5.0.0.819854
Image Version:   5.0.0.819854
```

Product

Steelhead EX appliance

Related Topics

"VSP Commands"

show vsp esxi version-history

Description

Displays ESXi version history.

Syntax

show vsp esxi version-history

Parameters

None

Example

```
Edge1 > show vsp esxi version-history
[20120813-142117] : ESXi version changed to : 5.0.0.716961
```

Product

Steelhead EX appliance

Related Topics

"VSP Commands"

show vsp v1 backup

Description

Displays VSP version 1 backup information for a specific filename.

Syntax

show vsp v1 backup <backup-filename>

Parameters

<backup-filename>	Specify the backup filename: **<Steelhead appliance name>-<slotname>-<date>.bkup**

Example

```
Edge1 > show vsp v1 backup gen-sh1-1-20120608-223616.bkup
% Backup /rbt/vsp/migrate/state/backup/gen-sh1-1-20120608-223616.bkup
```

Product

Steelhead EX appliance

Related Topics

"vsp v1 backup delete," "vsp v1 backup upload"

show vsp v1 backups

Description

Displays VSP version 1 information for all installed backup files.

Syntax

show vsp v1 backups

Parameters

None

Example

```
Edge1 > show vsp v1 backups
There are no backups available
```

Product

Steelhead EX appliance

Related Topics

"vsp v1 backup delete," "vsp v1 backup upload"

show vsp v1 disk-space

Description

Displays disk space information for migration.

Syntax

show vsp v1 disk-space

Parameters

None

Example

```
Edge1 > show vsp v1 disk-space
Disk Space:  48.40 GB used / 127.30 GB free / 175.70 GB total
Memory:      0 MB used / 7721 MB free / 7721 MB total
```

Product

Steelhead EX appliance

Related Topics

"VSP Commands"

show vsp v1 package

Description

Displays VSP version 1 package information for a specific package.

Syntax

show vsp v1 package <package>

Parameters

<package>	Specify the package filename.

Example

```
Edge1 > show vsp v1 package my-package.pkg
Package my-package.pkg:
  Valid:                    Yes

  Name:                     my
  Uncompressed size:        1.05MB
  Version:                  1
  Encrypted:                No
  Description:
    My package
[partial output]
```

Product

Steelhead EX appliance

Related Topics

"VSP Commands"

show vsp v1 packages

Description

Displays VSP version 1 information for all packages.

Syntax

show vsp v1 packages

Parameters

None

Example

```
Edge1 > show vsp v1 packages
Packages:
  my-package.pkg
  his-package.pkg
  another-package.pkg
```

Product

Steelhead EX appliance

Related Topics

"VSP Commands"

show vsp v1 slot

Description

Displays information about a specific VSP slot.

Syntax

show vsp v1 slot <slot name>

Parameters

<slot name>	Specify the slot name. The default names are **1**, **2**, **3**, **4**, **5**

Example

```
Edge1 > show vsp v1 slot 4
Slot 4:
  Package:
   Name: Ubuntu_AUX_PRI_5GB
   Description: Ubuntu Server with 2 MGMT interfaces

  Enabled:                  no
  Memory Size:              512 (MB)
  Slot Size on Disk:        5.00 GB
  Number of CPUs:           1
  Has Dataflow:             no
  Has Persistent Disk:      no
  Network(s)                Bridge, Bridged-aux
  Migrated:                 yes
  Deployment Sizes:
     Thick (lazy zero):     5.00 GB
     Thin:                  Unknown
  Archive Created:          no
  Archive Uploaded:         no

  VM migration in progress:    yes
  %complete:                   5%
  Est Time Remaining:          0:03:29
```

Product

Steelhead EX appliance

Related Topics

“Displaying VSP Information,” “vsp v1 slot archive delete,”“vsp v1 slot archive upload,”“vsp v1 slot delete”

show vsp v1 slot

Description

Displays information about a specific VSP slot.

Syntax

show vsp v1 slot <slot name>

Parameters

<slot name>	Specify the slot name. The default names are **1**, **2**, **3**, **4**, **5**

Example

```
Edge1 > show vsp v1 slot 1
Slot 1:
  Package:
   Name: Tiny
   Version: 1
   Description:
       Tiny package

  Enabled:                 No
  Priority:                Normal
  Clone Restore Pending:   No
  Memory Size:             128 (MB)
  Slot Size on Disk:       1.05 MB
  Attached Disks:
    Name                            Size        Adapter  Bus
    ------------------------------  ----------  -------- -----
    tiny                            1.00 MB     IDE      0:0
    Total Attached Disk Space:      1.00 MB

  Watchdog:
    Slot Status:           Not Applicable (Slot is not enabled)
    Timeout:               10 second(s)
    Startup Grace Period:  60 second(s)
    VNI Policy on fail:    Bypass-on-failure
    VM Reboot on fail:     No
    Ping Monitoring:       Disabled
      Ping Interval:       5 second(s)
      IP:                  0.0.0.0
    Heartbeat Monitoring:  Not supported
      Heartbeat Port:      None

  Optimization VNIs:
    Name                            T  I  N  VLAN   MAC
    ------------------------------  -  -  -  -----  -----------------
    1:QALanBridge                   L  R  R  none   00:0C:29:4F:9F:B1
    1:QAWanBridge                   W  R  R  none   00:0C:29:4F:9F:BB

    (T) Type:                  L=Lan  W=Wan  V=V-Inpath
    (I) Default IP Policy:     P=Pass  R=Redirect  C=Copy  L=L2-Switch
    (N) Default Non-IP Policy: P=Pass  R=Redirect  C=Copy  L=L2-Switch

  Management VNIs:
    Name                                 Bridged To  MAC
    -----------------------------------  ----------  -----------------
    1:QABridgeMgmt                       primary     00:0C:29:4F:9F:A7
```

Product

Steelhead EX appliance

Related Topics

"vsp v1 slot archive delete,""vsp v1 slot archive upload,""vsp v1 slot delete"

show vsp v1 slots

Description

Displays information about all VSP version 1 installed slots.

Syntax

show vsp v1 slots

Parameters

None

Example

```
Edge1 > show vsp v1 slots
Slot 1:
  Vacant

---------------------------------------------------------------------------
Slot 2:
  Vacant
```

Product

Steelhead EX appliance

Related Topics

"VSP Commands" "vsp v1 slot archive delete,""vsp v1 slot archive upload,""vsp v1 slot delete"

Granite Core Commands

This section describes the commands unique to the Granite Core system. You can use the command line to perform basic configuration tasks, display configuration information, and check status. It includes the following section:

- "Displaying Granite Core Information"

device-failover peer clear

Description

Clears the failover peer configuration for the current Granite Core appliance.

Syntax

device-failover peer clear

Parameters

Usage

This command is used to properly deactivate high availability between two Granite Core appliances. See the Usage section that follows.

To remove a high-availability configuration between two Granite Core appliances (GC01 and GC02, for the purposes of this example), use the following commands in the listed sequence:

1. Disable the GC02 appliance.
2. On GC01, run "device-failover peer clear" to clear the local failover configuration.
3. Enable GC02 and run "device-failover peer clear" to clear the local failover configuration.
4. On GC02, run "device-failover self-config activate" to return the appliance to solo mode.

Example

```
Core_02 (config) # device-failover peer clear
Core_02 (config) # show device-failover
```

Product

Granite Core

Related Topics

"show device-failover"

device-failover peer set

Description

Sets the failover peer configuration.

Syntax

device-failover peer set <peerip> [local-if <local-interface>] additional-ip <additional-ip> [local-if2 <localinterface2>]

Parameters

<peerip>	Specify the IP address of the failover peer appliance.
local-if <local-interface>	Specify the local interface for connecting with the failover peer appliance.
additional-ip <additional-ip>	Specify an additional IP address for the failover peer appliance.
local-if2 <local-interface2>	Specify an additional local interface for connecting with the failover peer appliance.

Usage

Use this command to ensure that Granite Core provides high availability for Windows and ESX servers in case of a single failure.

Example

```
Core_02 (config) # device-failover peer set 10.1.1.1 local-if eth0_0 additional-ip 10.2.1.1
```

Product

Granite Core

Related Topics

"device-failover peer-config activate," "show device-failover"

device-failover peer-config activate

Description

Activates the failover configuration on the failover peer device.

Syntax

device-failover peer-config activate

Parameters

None

Usage

Use this command to enable two Granite Core appliances to be configured so that either one can fail without disrupting the service of any of the LUNs being provided by the Granite system.

Example

```
Core_02 (config) # device-failover peer-config activate
```

Product

Granite Core

Related Topics

"device-failover peer clear," "device-failover peer set," "device-failover self-config activate," "show device-failover"

device-failover peerip

Description

Adds or removes the specified IP address to or from the failover configuration.

Syntax

device-failover peerip {add <peerip> [local-if <local-interface>] | remove <peerip>}

Parameters

add <peerip>	Specify the IP address of the failover peer.
local-if <local-interface>	Specify the local interface for connecting with the failover peer.
remove <peerip>	Specify the IP address of the peer to be removed from the failover configuration.

Usage

Use this command to modify the IP address of the failover peer. First remove the existing setting and then add the new value.

Example

```
Core_02 (config) # device-failover peerip remove 10.1.1.1
Core_02 (config) # device-failover peerip add 10.1.1.2
```

Product

Granite Core

Related Topics

"device-failover peer set," "device-failover peer clear," "device-failover peer-config activate," "show device-failover"

device-failover self-config activate

Description

Activates the failover configuration on the current device.

Syntax

device-failover self-config activate

Parameters

None

Usage

Use this command to enable two Granite Core appliances to be configured so that either one can fail without disrupting the service of any of the LUNs being provided by the Granite system.

Example

```
Core_02 (config) # device-failover self-config activate
```

Product

Granite Core

Related Topics

"device-failover peer clear," "device-failover peer set," "device-failover peer-config activate," "show device-failover"

edge add id

Description

Adds a Granite Edge device to the running Granite Core configuration.

Syntax

edge add id <id>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** .

Usage

Use this command to add a Granite Edge device to the current Granite Core configuration. Each Granite Edge device is configured with a unique self-identifier (which is configured through the Granite Edge device.)

Example

```
Core_02 (config) # edge add id BranchEdge001
```

Product

Granite Core

Related Topics

"failover-peer edge add id," "show edge," "show failover-peer storage iscsi"

edge id blockstore

Description

Configures the block store for the specified Granite Edge device.

Syntax

edge id <id> blockstore enc-type <enc-type>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, .** , and **-** .
enc-type <enc-type>	Set the block store encryption type: • **NONE** - No block store encryption. • **AES_128** - Encrypt block store with AES 128-bit key. • **AES_192** - Encrypt block store with AES 192-bit key. • **AES_256** - Encrypt block store with AES 256-bit key.

Example

```
Core_02 (config) # edge id Branch006a blockstore enc-type AES_128
```

Product

Granite Core

Related Topics

"failover-peer edge id blockstore," "show edge"

edge id iscsi data-digest

Description

Includes or excludes the data digest in the iSCSI PDU for the specified Granite Edge device.

Syntax

edge id <id> iscsi data-digest {enable | disable}

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, .** , and **-** .
enable	Specify this value to include the data digest in the iSCSI PDU in communications with the specified Granite Edge device.
disable	Specify this value to exclude the data digest from the iSCSI PDU in communications with the specified Granite Edge device.

Usage

The data digest can help to identify, reject, and request retransmission of a corrupt PDU.

Example

```
Core_02 (config) # edge id branch-009a iscsi data-digest disable
Core_02 (config) # edge id branch-009a iscsi data-digest enable
```

Product

Granite Core

Related Topics

"failover-peer edge id iscsi data-digest," "show edge,""storage iscsi data-digest"

edge id iscsi header-digest

Description

Includes or excludes the header digest in the iSCSI packet for the specified Granite Edge device.

Syntax

edge id <id> iscsi header-digest {enable |disable}

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** .
enable	Specify this value to include the header digest in the iSCSI packet in communications with the specified Granite Edge device.
disable	Specify this value to exclude the header digest from the iSCSI packet in communications with the specified Granite Edge device.

Usage

The data digest can help to identify, reject, or request retransmission of a corrupt PDU.

Example

```
Core_02 (config) # edge id branch-009a iscsi header-digest disable
Core_02 (config) # edge id branch-009a iscsi header-digest enable
```

Product

Granite Core

Related Topics

"failover-peer edge id iscsi header-digest," "show edge," "storage iscsi header-digest"

edge id iscsi initiator add

Description

Adds an iSCSI initiator to the specified Granite Edge device.

Syntax

edge id <id> iscsi initiator add <username> auth {None | CHAP chap-user <username> [mutual-chap <name>]}

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, .** , and **-** .
auth	Specify one of the following authentication options: • **CHAP chap-user <name>** - Enables CHAP and specifies the CHAP user name. You must specify an existing CHAP user. • **None** - No authentication.
mutual-chap <name>	Specify the new value for the mutual CHAP user.

Example

```
Core_02 (config) # edge id Branch006a iscsi initiator add iqn.1991-05.com.microsoft:jshmoe-
win7.wannabe.com CHAP chap-user Chap13NYC
```

Product

Granite Core

Related Topics

"failover-peer edge id iscsi initiator add,""edge id iscsi initiator modify," "edge id iscsi initiator remove," "show edge"

edge id iscsi initiator modify

Description

Modifies the authorization configuration of an existing iSCSI initiator credential in the specified Granite Edge device.

Syntax

edge id <id> iscsi initiator modify <username> auth {None | CHAP chap-user <chap-user> [mutual-chap <name>]}

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, .** , and **-** .
auth	Specify one of the following authentication options: • **CHAP chap-user <name>** - Enables CHAP and specifies the CHAP user name. You must specify an existing CHAP user. • **None** - No authentication.
mutual-chap <name>	Specify the new value for the mutual CHAP user.

Usage

Use this command to modify the CHAP authorization settings for the specified iSCSI initiator credential at the specified Granite Edge device.

Example

```
Core_02 (config) # edge id Branch006a iscsi initiator modify iqn.1991-05.com.microsoft:jshmoe-
win7.wannabe.com auth CHAP chap-user Chap13NYC
```

Product

Granite Core

Related Topics

"failover-peer edge id iscsi initiator modify," "edge id iscsi initiator add," "edge id iscsi initiator remove," "show edge"

edge id iscsi initiator remove

Description

Removes the specified iSCSI initiator credential from the specified Granite Edge device configuration.

Syntax

edge id <id> iscsi initiator remove <name>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** .
<name>	Specify the iSCSI initiator credential to be removed.

Example

```
Core_02 (config) # edge id Branch006a iscsi initiator remove iqn.1991-05.com.microsoft:jshmoe-
win7.wannabe.com
```

Product

Granite Core

Related Topics

"failover-peer edge id iscsi initiator modify," "edge id iscsi initiator add," "edge id iscsi initiator modify," "show edge"

edge id iscsi initiator-group

Description

Creates or deletes an iSCSI initiator group for the specified Granite Edge.

Syntax

edge id <id> iscsi initiator-group {create | delete} <name>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** .
{create | delete}	Creates or deletes the specified iSCSI initiator group.
<name>	Specify the name of the iSCSI initiator group to be created or deleted.

Example

```
Core_02 (config) # edge id Branch006a iscsi initiator-group create defaultiGroup
```

Product

Granite Core

Related Topics

"failover-peer edge id iscsi initiator-group," "show edge"

edge id iscsi initiator-group modify

Description

Modifies the iSCSI initiator group in the specified Granite Edge device by adding or removing an iSCSI initiator credential.

Syntax

edge id <id> iscsi initiator-group modify <groupname> initiator {add | remove} <name>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** .
<groupname>	Specify the iSCSI initiator group to be modified.
{add | remove}	Specify the appropriate value to add or remove the specified initiator credential to the group.
<name>	Specify the initiator credential to be added or removed.

Example

```
Core_02 (config) # edge id Branch006a iscsi initiator-group modify defaultiGroup initiator add
iqn.1991-05.com.microsoft:jshmoe-win7.wannabe.com
```

Product

Granite Core

Related Topics

"failover-peer edge id iscsi initiator-group modify," "show edge"

edge id iscsi target modify-name

Description

Modifies the target name setting in the specified Granite Edge device.

Syntax

edge id <id> iscsi target modify-name <target-name>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** .
<target-name>	Specify the new value for the target name.

Example

```
Core_02 (config) # edge id Edge1 iscsi target modify-name iqn.2003-10.com.hoosgau:432716056
```

Product

Granite Core

Related Topics

"failover-peer edge id iscsi target modify-name," "show edge"

edge id iscsi target portal ignore ip address

Description

Configures the specified Granite Edge device to ignore the specified target portal IP address.

Syntax

edge id <id> iscsi target portal ignore ip address <address>

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** .
address <address>	Specify the target portal IP address to be ignored.

Example

```
Core_02 (config) # edge id Edge2 iscsi target portal ignore ip address 10.1.2.3
```

Product

Granite Core

Related Topics

"failover-peer edge id iscsi target portal ignore ip address," "show edge"

edge id iscsi target portal listen ip address

Description

Configures the specified Granite Edge device to listen to the specified target portal IP address.

Syntax

edge id <id> iscsi target portal listen ip address <address> [port <port>]

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** .
address <address>	Specify the target portal IP address to be listened to.
port <port>	Specify the port on the listening target portal. The default is 3260.

Example

```
Core_02 (config) # edge id Edge2 iscsi target portal listen ip address 10.1.2.3 port 3260
```

Product

Granite Core

Related Topics

"failover-peer edge id iscsi target portal listen ip address," "show edge"

edge id iscsi target portal modify ip address

Description

Configures the specified Granite Edge device to listen to the specified target portal IP address.

Syntax

edge id <id> iscsi target portal modify ip address <address> port <port>

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
address <address>	Modify the target portal IP address to be listened to.
port <port>	Optionally, modify the port on the listening target portal. The default is 3260.

Example

```
Core_02 (config) # edge id Edge2 iscsi target portal modify ip address 10.1.2.3 port 3260
```

Product

Granite Core

Related Topics

"failover-peer edge id iscsi target portal modify ip address," "show edge"

edge id iscsi target security-only

Description

Configures the iSCSI target on the specified Granite Edge device to accept either secured or unsecured initiator authentication.

Syntax

edge id <id> iscsi target security-only {enable | disable}

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
enable	Specify this value to enable the specified Granite Edge device to accept only secured initiator authentication.
disable	Specify this value to enable the specified Granite Edge device to accept unsecured initiator authentication.

Example

```
Core_02 (config) # edge id 10.1.2.3 iscsi target security-only enable
```

Product

Granite Core

Related Topics

"failover-peer edge id iscsi target security-only," "show edge"

edge id prepop schedule add

Description

Adds a new prepopulation schedule for the specified Granite Edge device.

Syntax

edge id <id> prepop schedule add sched-name <sched-name> start-week-day <start-week-day> start-time <start-time> stop-week-day <stop-week-day> stop-time <stop-time>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
sched-name <sched-name>	Specify the name of the prepopulation schedule.
start-week-day <start-week-day>	Specify the start day for the schedule. Use the first three characters (lowercase) of the English term for the day of the week: for example, sun, mon, tue, and so on.
start-time <start-time>	Specify the start time for the schedule. Use the format HH:MM:SS.
stop-week-day <stop-week-day>	Specify the stop day for the schedule. Use the first three characters (lowercase) of the English term for the day of the week: for example, sun, mon, tue, and so on.
stop-time <stop-time>	Specify the stop time for the schedule. Use the format HH:MM:SS.

Example

```
Core_02 (config) # edge id Branch006a prepop schedule add sched-name WeeklySynch start-week-day mon
start-time 00:01:00 stop-week-day mon stop-time 03:01:00
```

Product

Granite Core

Related Topics

"failover-peer edge id prepop schedule add," "show edge"

edge id prepop schedule modify

Description

Modifies the settings of the specified prepopulation schedule on the specified Granite Edge device.

Syntax

edge id <id> prepop schedule modify sched-name <sched-name> start-week-day <start-week-day> start-time <start-time> stop-week-day <stop-week-day> stop-time <stop-time>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** .
sched-name <sched-name>	Specify a modified name of the prepopulation schedule.
start-week-day <start-week-day>	Specify a modified start day for the schedule. Use the first three characters (lowercase) of the English term for the day of the week: for example, sun, mon, tue, and so on.
start-time <start-time>	Specify a modified start time for the schedule. Use the format HH:MM:SS.
stop-week-day <stop-week-day>	Specify a modified stop day for the schedule. Use the first three characters (lowercase) of the English term for the day of the week: for example, sun, mon, tue, and so on.
stop-time <stop-time>	Specify a modified stop time for the schedule. Use the format HH:MM:SS.

Example

```
Core_02 (config) # edge id Branch006a prepop schedule modify sched-name MondaySynch start-week-day
mon start-time 00:02:00 stop-week-day mon stop-time 03:02:00
```

Product

Granite Core

Related Topics

"failover-peer edge id prepop schedule modify sched-name," "show edge"

edge id prepop schedule remove

Description

Removes the specified new prepopulation schedule from the specified Granite Edge device.

Syntax

edge id <id> prepop schedule remove sched-name <sched-name>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
sched-name <sched-name>	Specify the name of the prepopulation schedule to be removed.

Example

```
Core_02 (config) # edge id Branch006a prepop schedule remove sched-name MondaySynch
```

Product

Granite Core

Related Topics

"failover-peer edge id prepop schedule remove" "show edge"

edge id virtual-ip

Description

Adds or removes a virtual IP address configuration for the specified Granite Edge device.

Syntax

edge id <id> virtual-ip {add | remove} <address>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
<address>	Specify the IP address to be configured for the specified Granite Edge device.

Example

```
Core_02 (config) # edge id Branch006a virtual-ip add 10.0.0.2
```

Product

Granite Core

Related Topics

"failover-peer edge id virtual-ip," "show edge"

edge modify id clear-serial

Description

Clears the saved serial value for the Granite Edge device so that it can be replaced.

Syntax

edge modify id <id> clear-serial

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.

Example

```
Core_02 (config) # edge modify id Branch006a clear-serial
```

Product

Granite Core

Related Topics

"failover-peer edge modify id clear-serial," "show edge"

edge modify preferred-if

Description

Sets the preferred interface on the Granite Core for Granite Edge device connections.

Syntax

edge modify preferred-if {add | remove} <preferred-if>

Parameters

[add | remove]	Specify the appropriate value to add or remove the specified interface to or from the edge configuration.
<preferred-if>	Specify the interface for Granite Edge device connections.

Usage

Use this command for high availability deployments.

In the event of a failover event, this setting ensures that the Granite Edge devices connect to the Granite Core failover peer.

For redundancy, add multiple interfaces in the order of preference.

Example

```
Core_02 (config) # edge modify preferred-if add aux
```

Product

Granite Core

Related Topics

"Branch Storage Commands" "show edge"

edge remove id

Description

Removes the specified Granite Edge device from the Granite Core configuration.

Syntax

edge remove id <id>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z**, **A** through **Z**, **.** **,** and **-**.

Example

```
Core_02 (config) # edge remove id Branch006a
```

Product

Granite Core

Related Topics

"failover-peer edge remove id," "show edge"

failover-peer edge add id

Description

Adds a Granite Edge device to the configuration of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge add id <id>

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to be added.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the intended Granite Core device becomes operational, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge add id Edge3
```

Product

Granite Core

Related Topics

"edge add id," "show edge"

failover-peer edge id blockstore

Description

Configures the block store for the specified Granite Edge device on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> blockstore enc-type <enc-type>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** .
enc-type <enc-type>	Set the block store encryption type: • **NONE** - No block store encryption. • **AES_128** - Encrypt block store with AES 128-bit key. • **AES_192** - Encrypt block store with AES 192-bit key. • **AES_256** - Encrypt block store with AES 256-bit key.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge id Edge1 blockstore enc-type AES_128
```

Product

Granite Core

Related Topics

"edge id blockstore"

failover-peer edge id iscsi data-digest

Description

Includes or excludes the data digest in or from the iSCSI PDU for the specified Granite Edge device on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> iscsi data-digest {enable | disable}

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, .** **,** and **-**.
enable	Specify this parameter to include the data digest in the iSCSI PDU in communications with the specified Granite Edge device.
disable	Specify this parameter to exclude the data digest from the iSCSI PDU in communications with the specified Granite Edge device.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge id Edge1 iscsi data-digest disable
Core_02 (config) # failover-peer edge id Edge1 iscsi data-digest enable
```

Product

Granite Core

Related Topics

"edge id iscsi data-digest"

failover-peer edge id iscsi header-digest

Description

Includes or excludes the header digest in the iSCSI packet for the specified Granite Edge device on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> iscsi header-digest {enable | disable}

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** .
enable	Specify this parameter to include the header digest in the iSCSI packet in communications with the specified Granite Edge device.
disable	Specify this parameter to exclude the header digest from the iSCSI packet in communications with the specified Granite Edge device.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge id Edge1 iscsi header-digest disable
Core_02 (config) # failover-peer edge id Edge1 iscsi header-digest enable
```

Product

Granite Core

Related Topics

"edge id iscsi header-digest"

failover-peer edge id iscsi initiator add

Description

Adds an iSCSI initiator to the specified Granite Edge device on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> iscsi initiator add <username> auth CHAP chap-user <username> [mutual-chap <name>]

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-** .
auth CHAP	Specify one of the following CHAP options: • **chap-user <username>** - Specify to enable CHAP and set the CHAP user name. • **mutual-chap <name>** - Optionally, specify the name of the mutual CHAP user.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge id Edge1 iscsi initiator add iqn.1991-05.com.microsoft:jshmoe-
win7.wannabe.com auth CHAP chap-user Chap13NYC
```

Product

Granite Core

Related Topics

"edge id iscsi initiator add"

failover-peer edge id iscsi initiator modify

Description

Modifies the authorization configuration of an existing iSCSI initiator credential in the specified Granite Edge device on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> iscsi initiator modify <username> {auth {CHAP chap-user <chap-user> | None} | mutual-chap <name>}

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **- .**
auth	Specify one of the following authentication options: • **CHAP chap-user <name>** - Enables CHAP and specifies the CHAP user name. You must specify an existing CHAP user. • **None** - No authentication.
mutual-chap <name>	Specify the new value for the mutual CHAP user.

Usage

Use this command to modify the CHAP authorization settings for the specified iSCSI initiator credential at the specified Granite Edge device.

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge id Edge1 iscsi initiator modify iqn.1991-
05.com.microsoft:jshmoe-win7.wannabe.com auth CHAP chap-user Chap13NYC
```

Product

Granite Core

Related Topics

"edge id iscsi initiator modify"

failover-peer edge id iscsi initiator remove

Description

Removes the specified iSCSI initiator credential from the specified Granite Edge device configuration device on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> iscsi initiator remove <username>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
<username>	Specify the iSCSI initiator credential to be removed.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Consider the following example: Core1 and Core2 are configured as failover peers. Edge1 is linked to Core1. You want to remove an iSCSI initiator credential from the Edge1 configuration. However, Core1 is down but Core2 is operational. On Core2, run the following command:

```
edge failover-peer edge id Edge1 iscsi initiator remove iqn.1991-05.com.microsoft:jshmoe-
win7.wannabe.com
```

When Core1 resumes operation, the Edge1 configuration changes are added to its configuration.

Example

```
Core_02 (config) # failover-peer edge id Edge1 iscsi initiator remove iqn.1991-
05.com.microsoft:jshmoe-win7.wannabe.com
```

Product

Granite Core

Related Topics

"edge id iscsi initiator remove"

failover-peer edge id iscsi initiator-group

Description

Creates or deletes an iSCSI initiator group for the specified Granite Edge device on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> iscsi initiator-group {create | delete} <name>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
{create | delete}	Specify the appropriate value to create or delete the specified iSCSI initiator group.
<name>	Specify the name of the iSCSI initiator group to be created or deleted.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge id Branch006a iscsi initiator-group create defaultiGroup
```

Product

Granite Core

Related Topics

"edge id iscsi initiator-group"

failover-peer edge id iscsi initiator-group modify

Description

Adds or removes an iSCSI initiator credential to or from the specified iSCSI initiator group in the specified Granite Edge device, on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> iscsi initiator-group modify <groupname> initiator {add | remove} <username>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
<groupname>	Specify the iSCSI initiator group to be modified.
{add | remove}	Specify the appropriate value to add or remove the specified initiator credential to or from the group.
<username>	Specify the initiator credential to be added or removed.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge id Branch006a iscsi initiator-group modify defaultiGroup add
iqn.1991-05.com.microsoft:jshmoe-win7.wannabe.com
```

Product

Granite Core

Related Topics

"edge id iscsi initiator-group modify"

failover-peer edge id iscsi target modify-name

Description

Modifies the target name setting in the specified Granite Edge device on behalf of an unavailable Granite Core device through its failover peer

Syntax

failover-peer edge id <id> iscsi target modify-name <target-name>

Parameters

<id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
<target-name>	Specify the new value for the target name.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge id Edge1 iscsi target modify-name iqn.2003-
10.com.hoosgau:432716056
```

Product

Granite Core

Related Topics

"edge id iscsi target modify-name"

failover-peer edge id iscsi target portal ignore ip address

Description

Configures the specified Granite Edge device to ignore the specified target portal IP address on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> iscsi target portal ignore ip address <address>

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
address <address>	Specify the target portal IP address to be ignored.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge id Edge2 iscsi target portal ignore ip address 10.1.2.3
```

Product

Granite Core

Related Topics

"edge id iscsi target portal ignore ip address"

failover-peer edge id iscsi target portal listen ip address

Description

Configures the specified Granite Edge device to listen to the specified target portal IP address on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> iscsi target portal listen ip address <address> port <port>

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
address <address>	Specify the target portal IP address to be listened to.
port<port>	Specify the port on the listening target portal. The default is 3260.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge id Edge1 iscsi target portal listen ip address 10.1.2.3
```

Product

Granite Core

Related Topics

"edge id iscsi target portal listen ip address"

failover-peer edge id iscsi target portal modify ip address

Description

Configures the specified Granite Edge device to listen to the specified target portal IP address on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> iscsi target portal modify ip address <address> [port <port>]

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
address <address>	Modify the target portal IP address to be listened to.
port<port>	Optionally, modify the port on the listening target portal. The default is 3260.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge id Edge2 iscsi target portal modify ip address 10.1.2.3
```

Product

Granite Core

Related Topics

"edge id iscsi target portal modify ip address"

failover-peer edge id iscsi target security-only

Description

Configures the iSCSI target on the specified Granite Edge device to accept either secured or unsecured initiator authentication on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> iscsi target security-only {enable | disable}

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
enable	Specify this value to enable the specified Granite Edge device to accept only secured initiator authentication.
disable	Specify this value to enable the specified Granite Edge device to accept unsecured initiator authentication.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer edge id 10.1.2.3 iscsi target security-only enable
```

Product

Granite Core

Related Topics

"edge id iscsi target security-only"

failover-peer edge id prepop schedule add

Description

Adds a new prepopulation schedule for the specified Granite Edge device on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> prepop schedule add sched-name <sched-name> start-week-day <start-week-day> start-time <start-time> stop-week-day <stop-week-day> stop-time <stop-time>

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
sched-name <sched-name>	Specify the name of the prepopulation schedule.
start-week-day <start-week-day>	Specify the start day for the schedule. Use the first three characters (lowercase) of the English term for the day of the week: for example, sun, mon, tue, and so on.
start-time <start-time>	Specify the start time for the schedule. Use the format HH:MM:SS.
stop-week-day <stop-week-day>	Specify the stop day for the schedule. Use the first three characters (lowercase) of the English term for the day of the week: for example, sun, mon, tue, and so on.
stop-time <stop-time>	Specify the stop time for the schedule. Use the format HH:MM:SS.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Consider the following example: Core1 and Core2 are configured as failover peers. Edge1 is linked to Core1. You want to create a new prepopulation schedule for the Edge1 configuration. However, Core1 is down but Core2 is operational. On Core2, run the following command:

```
failover-peer edge id Branch006a prepop schedule add sched-name WeeklySynch start-week-day mon
start-time 00:01:00 stop-week-day mon stop-time 03:01:00
```

When Core1 resumes operation, the Edge1 configuration changes are added to its configuration.

Example

```
Core_02 (config) # failover-peer edge id Branch006a prepop schedule add sched-name WeeklySynch
start-week-day mon start-time 00:01:00 stop-week-day mon stop-time 03:01:00
```

Product

Granite Core

Related Topics

"edge id prepop schedule add"

failover-peer edge id prepop schedule modify sched-name

Description

Modifies the settings of the specified prepopulation schedule on the specified Granite Edge device, on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> prepop schedule modify sched-name <sched-name> start-week-day <start-week-day> start-time <start-time> stop-week-day <stop-week-day> stop-time <stop-time>

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, .** , and **-**.
sched-name <sched-name>	Specify a modified name for the prepopulation schedule.
start-week-day <start-week-day>	Specify a modified start day for the schedule. Use the first three characters (lowercase) of the English term for the day of the week: for example, sun, mon, tue, and so on.
start-time <start-time>	Specify a modified start time for the schedule. Use the format HH:MM:SS.
stop-week-day <stop-week-day>	Specify a modified stop day for the schedule. Use the first three characters (lowercase) of the English term for the day of the week: for example, sun, mon, tue, and so on.
stop-time <stop-time>	Specify a modified stop time for the schedule. Use the format HH:MM:SS.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Consider the following example: Core1 and Core2 are configured as failover peers. Edge1 is linked to Core1. You want to modify an existing prepopulation schedule for the Edge1 configuration. However, Core1 is down but Core2 is operational. On Core2, run the following command:

```
failover-peer edge id Branch006a prepop schedule modify sched-name WeeklySynch start-week-day mon
start-time 00:01:00 stop-week-day mon stop-time 03:01:00
```

When Core1 resumes operation, the Edge1 configuration changes are added to its configuration.

Example

```
Core_02 (config) # failover-peer edge id Branch006a prepop schedule modify sched-name MondaySynch
```

```
start-week-day mon start-time 00:02:00 stop-week-day mon stop-time 03:02:00
```

Product

Granite Core

Related Topics

"edge id prepop schedule modify"

failover-peer edge id prepop schedule remove

Description

Removes the specified new prepopulation schedule from the specified Granite Edge device, on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> prepop schedule remove sched-name <sched-name>

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, . ,** and **-**.
sched-name <sched-name>	Specify the name of the prepopulation schedule to be removed.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Consider the following example: Core1 and Core2 are configured as failover peers. Edge1 is linked to Core1. You want to remove a prepopulation schedule from the Edge1 configuration. However, Core1 is down but Core2 is operational. On Core2, run the following command:

```
failover-peer edge id Branch006a prepop schedule remove sched-name WeeklySynch start-week-day mon
start-time 00:01:00 stop-week-day mon stop-time 03:01:00
```

When Core1 resumes operation, the Edge1 configuration changes are added to its configuration.

Example

```
Core_02 (config) # failover-peer edge id Branch006a prepop schedule remove sched-name MondaySynch
```

Product

Granite Core

Related Topics

"edge id prepop schedule remove"

failover-peer edge id virtual-ip

Description

Adds or removes a virtual IP address configuration for the specified Granite Edge device, on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge id <id> virtual-ip {add | remove} <address>

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z**, **A** through **Z**, **.** , and **-**.
add <address>	Specify the virtual IP address to be added to the configuration.
remove <address>	Specify the virtual IP address to be removed from the configuration.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Consider the following example: Core1 and Core2 are configured as failover peers. Edge1 is linked to Core1. You want to add a virtual IP address configuration to the Edge1 configuration. However, Core1 is down but Core2 is operational. On Core2, run the following command:

```
failover-peer edge id Branch006a virtual-ip add 10.0.0.2
```

When Core1 resumes operation, the Edge1 configuration changes are added to its configuration.

Example

```
Core_02 (config) # failover-peer edge id Branch006a virtual-ip add 10.0.0.2
```

Product

Granite Core

Related Topics

"edge id virtual-ip"

failover-peer edge modify id clear-serial

Description

Clears the saved serial value for the Granite Edge device so that it can be replaced, on behalf of an unavailable Granite Core device, through its failover peer.

Syntax

failover-peer edge modify id <id> clear-serial

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z**, **A** through **Z**, **.** , and **-**.

Example

```
Core_02 (config) # failover-peer edge modify id Branch006a clear-serial
```

Product

Granite Core

Related Topics

"edge modify id clear-serial"

failover-peer edge remove id

Description

Removes the specified Granite Edge device from the Granite Core configuration, on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer edge remove id <id>

Parameters

id <id>	Specify the self-identifier of the Granite Edge device to which the configuration is to be pushed. This value is case-sensitive and limited to the following characters: **0** through **9**, **a** through **z, A** through **Z, .** , and **-**.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Consider the following example: Core1 and Core2 are configured as failover peers. Edge1 is linked to Core1. You want to remove Edge1 from the Core1 configuration. However, Core1 is down but Core2 is operational. On Core2, run the following command:

```
failover-peer edge remove id Branch006a
```

When Core1 resumes operation, the Edge1 configuration changes are added to its configuration.

Example

```
Core_02 (config) # failover-peer edge remove id Branch006a
```

Product

Granite Core

Related Topics

"edge modify id clear-serial"

failover-peer storage iscsi chap add

Description

Adds a CHAP user to the storage configuration on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer storage iscsi chap add username <username> password <password>

Parameters

username <username>	Specify the user name for CHAP authentication.
password <password>	Specify the password for the new CHAP user.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi chap add username DefaultChap password CHAPpw
```

Product

Granite Core

Related Topics

"storage iscsi chap add," "show storage iscsi"

failover-peer storage iscsi chap delete

Description

Deletes the specified CHAP user from the current storage configuration on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer storage iscsi chap delete username <name> [force]

Parameters

username <username>	Specify the CHAP user to be deleted.
force	Include this parameter to force deletion if the CHAP user is currently enabled.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi chap delete username DefaultChap
```

Product

Granite Core

Related Topics

"storage iscsi chap delete," "show storage iscsi"

failover-peer storage iscsi chap modify

Description

Modifies the password of the specified CHAP user, on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer storage iscsi chap modify username <username> password <password>

Parameters

username <username>	Specify the CHAP user to be modified.
password <password>	Displays information about the configured VM kernel interfaces.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi chap modify username DefaultChap password newCHAPpw
```

Product

Granite Core

Related Topics

"storage iscsi chap modify"

failover-peer storage iscsi chap username

Description

Enables or disables the specified CHAP user, on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer storage iscsi chap username <name> {disable | enable}

Parameters

username <name>	Specify the CHAP user to be enabled or disabled.
disable	Specify this parameter to disable the specified CHAP user.
enable	Specify this parameter to enable the specified CHAP user.

Usage

Run the "show storage iscsi" or "show failover-peer storage iscsi" command to display whether or not the CHAP user is enabled.

Disable or enable the CHAP user as needed.

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi chap username JoeyD disable
```

Product

Granite Core

Related Topics

"show storage iscsi," "show failover-peer storage iscsi"

failover-peer storage iscsi data-digest

Description

Includes or excludes the data digest in the iSCSI PDU, on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer storage iscsi data-digest {enable | disable}

Parameters

enable	Specify this parameter to include the data digest in the iSCSI PDU.
disable	Specify this parameter to exclude the data digest from the iSCSI PDU.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi data-digest disable
Core_02 (config) # failover-peer storage iscsi data-digest enable
```

Product

Granite Core

Related Topics

"edge id iscsi data-digest," "show failover-peer storage iscsi"

failover-peer storage iscsi header-digest

Description

Includes or excludes the data digest in the iSCSI PDU on behalf of an unavailable Granite Core device through its failover peer.

Syntax

failover-peer storage iscsi header-digest {enable | disable}

Parameters

enable	Specify this parameter to include the header digest in the iSCSI PDU.
disable	Specify this parameter to exclude the header digest from the iSCSI PDU.

Usage

The header digest can help to identify, reject, or request retransmission of a corrupt PDU.

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi header-digest disable
Core_02 (config) # failover-peer storage iscsi header-digest enable
```

Product

Granite Core

Related Topics

"storage iscsi header-digest," "show failover-peer storage iscsi," "edge id iscsi header-digest"

failover-peer storage iscsi initiator modify auth mutual-chap

Description

Configures iSCSI initiator authentication mutual CHAP settings for the failover peer.

Syntax

failover-peer storage iscsi initiator modify auth mutual-chap {chap-user <name> | enable | disable}

Parameters

chap-user <name>	Specify the mutual CHAP user. You must specify an existing CHAP user.
enable	Specify this parameter to enable mutual CHAP authentication.
disable	Specify this parameter to disable mutual CHAP authentication.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Use this command to:

- enable or disable mutual CHAP authentication for the iSCSI initiator configuration.
- specify the mutual CHAP user.

You can specify only existing CHAP users.

Example

```
Core_02 (config) # failover-peer storage iscsi initiator modify auth mutual-chap chap-user
existingCHAPUser
Core_02 (config) # failover-peer storage iscsi initiator modify auth mutual-chap enable
```

Product

Granite Core

Related Topics

"storage iscsi initiator modify auth mutual-chap"

failover-peer storage iscsi initiator modify name

Description

Modifies the initiator name in the iSCSI initiator configuration.

Syntax

failover-peer storage iscsi initiator modify name <name>

Parameters

name <name>	Specify the new initiator name for the iSCSI initiator configuration.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the intended Granite Core device becomes operational, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi initiator modify name iqn.2003-
10.com.hoosegow:werdna-initiator
```

Product

Granite Core

Related Topics

"storage iscsi initiator modify name"

failover-peer storage iscsi mpio interface remove

Description

Removes the specified local interface for MPIO from the iSCSI initiator configuration.

Syntax

failover-peer storage iscsi mpio interface remove name <name>

Parameters

name <name>	The local interface to be removed. To view a list of local interfaces configured for MPIO, use the "show failover-peer storage iscsi mpio interfaces" command.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Examples

```
Core_02 (config) # show failover-peer storage iscsi mpio interfaces
Interfaces configured for MPIO
        eth0_2
        eth0_3
Core_02 (config) # failover-peer storage iscsi mpio interface remove name eth0_2
```

Product

Granite Core

Related Topics

"failover-peer storage iscsi session mpio," "failover-peer storage iscsi session mpio standard-routes," "show failover-peer storage iscsi mpio interfaces"

failover-peer storage iscsi portal add host

Description

Adds an iSCSI portal configuration to the iSCSI initiator configuration.

Syntax

failover-peer storage iscsi portal add host <hostname> [port <port>] auth {CHAP chap-user <name> | None}

Parameters

host <hostname>	Specify the IP address of the iSCSI portal.
port <port>	Optionally, specify a port number. The default is 3260.
auth	Specify one of the following authentication options: • **CHAP chap-user <name>** - Enables CHAP and specifies the CHAP user name. You must specify an existing CHAP user. • **None** - No authentication.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi portal add host 10.2.3.4 port 3260 auth CHAP chap-
user JoeyD
```

Product

Granite Core

Related Topics

"storage iscsi portal add host"

failover-peer storage iscsi portal host disc-portal add

Description

Manually adds a portal IP address to the iSCSI portal configuration.

Syntax

failover-peer storage iscsi portal host <hostname> disc-portal add ip <ip> [port <port>]

Parameters

<hostname>	Specify the hostname of the iSCSI portal configuration to which the additional IP address is to be added.
<ip>	Specify the IP address of the discovered portal to be added to the iSCSI portal configuration.
[port <port>]	Optionally, specify a port number to the additional IP address.

Usage

If you have enabled multi-path I/O (MPIO), this command enables you to add existing IP addresses available on the filer for connections with the Granite Core appliance.

MPIO enables a single iSCSI portal configuration to connect with the filer on multiple IP addresses.

Use the "failover-peer storage iscsi portal host rescan-portals" and "show failover-peer storage iscsi disc-portals portal" commands to discover portals on the specified iSCSI initiator.

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Examples

```
Core_02 (config) # failover-peer storage iscsi portal host 123.45.6.789 add 132.45.6.780
```

Product

Granite Core

Related Topics

"show failover-peer storage iscsi disc-portals portal," "failover-peer storage iscsi portal host disc-portal modify," "failover-peer storage iscsi portal host disc-portal remove," "failover-peer storage iscsi portal host rescan-portals"

failover-peer storage iscsi portal host disc-portal modify

Description

Modifies the ID and/or port settings of the specified portal host configuration.

Syntax

failover-peer storage iscsi portal host <hostname> disc-portal modify id <disc-portal> port <port>

Parameters

<hostname>	Specify the hostname of the iSCSI portal configuration to which the additional IP address is to be added..
id <disc-portal>	Specify the new ID value for the specified portal host.
<port>	Specify the new port number for specified portal host.

Usage

This command is intended to be used for portals discovered for multi-path I/O (MPIO) configurations. MPIO enables a single iSCSI portal configuration to connect with the filer on multiple IP addresses.

Use the "failover-peer storage iscsi portal host rescan-portals" and "show failover-peer storage iscsi disc-portals portal" commands to discover portals on the specified iSCSI initiator.

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Examples

```
Core_02 (config) # failover-peer storage iscsi portal host 123.45.6.789 modify id principal port
3260
```

Product

Granite Core

Related Topics

"show failover-peer storage iscsi disc-portals portal," "failover-peer storage iscsi portal host disc-portal add," "failover-peer storage iscsi portal host disc-portal remove," "failover-peer storage iscsi portal host rescan-portals"

failover-peer storage iscsi portal host disc-portal remove

Description

Removes the specified discovered portal configuration from the iSCSI portal configuration.

Syntax

failover-peer storage iscsi portal host <hostname> disc-portal remove id <disc-portal>

Parameters

<hostname>	Specify the hostname of the iSCSI portal configuration to which the additional IP address is to be removed.
<disc-portal>	Specify the IP address of the discovered portal to be removed from the iSCSI portal configuration.

Usage

This command is intended to be used for portals discovered for multi-path I/O (MPIO) configurations. MPIO enables a single iSCSI portal configuration to connect with the filer on multiple IP addresses.

Use the "failover-peer storage iscsi portal host rescan-portals" and "show failover-peer storage iscsi disc-portals portal" commands to discover portals on the specified iSCSI initiator.

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Examples

```
Core_02 (config) # failover-peer storage iscsi portal host 123.45.6.789 remove 132.45.6.780
```

Product

Granite Core

Related Topics

"show failover-peer storage iscsi disc-portals portal," "failover-peer storage iscsi portal host disc-portal add," "failover-peer storage iscsi portal host disc-portal modify," "failover-peer storage iscsi portal host rescan-portals"

failover-peer storage iscsi portal host offline-luns

Description

Takes offline all configured LUNs serviced by the specified portal.

Syntax

failover-peer storage iscsi portal host <hostname> offline-luns

Parameters

host <hostname>	Specify the IP address of the iSCSI portal.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi portal host 10.2.3.4 offline-luns
```

Product

Granite Core

Related Topics

"storage iscsi portal host offline-luns"

failover-peer storage iscsi portal host rescan-luns

Description

Rescans iSCSI targets associated with the specified portal.

Syntax

failover-peer storage iscsi portal host <hostname> rescan-luns {all | target name <name>}

Parameters

host <hostname>	Specify the IP address of the iSCSI portal.
all	Rescans all iSCSI targets associated with the specified portal.
target name <name>	Rescans only the specified target.

Usage

Use this command to ensure that newly configured iSCSI targets are added.

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi portal host 10.2.3.4 rescan-luns all
```

Product

Granite Core

Related Topics

"storage iscsi portal host rescan-luns"

failover-peer storage iscsi portal host rescan-portals

Description

Rescans the specified iSCSI portal configuration for discoverable and available portals.

Syntax

failover-peer storage iscsi portal host <hostname> rescan-portals

Parameters

<hostname>	Specify the hostname of the iSCSI portal configuration from which the discovered portal is to be removed.

Usage

This command is intended to be used for portals discovered for multi-path I/O (MPIO) configurations. MPIO enables a single iSCSI portal configuration to connect with the filer on multiple IP addresses.

After portals have been discovered, you can add them to the iSCSI portal configuration using the "failover-peer storage iscsi portal host disc-portal add" command.

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi portal host 123.45.6.789 rescan-portals
```

Product

Granite Core

Related Topics

"show failover-peer storage iscsi disc-portals portal," "failover-peer storage iscsi portal host disc-portal add," "failover-peer storage iscsi portal host disc-portal modify," "failover-peer storage iscsi portal host rescan-portals"

failover-peer storage iscsi portal host rescan-targets

Description

Rescans all iSCSI targets associated with the specified portal.

Syntax

failover-peer storage iscsi portal host <hostname> rescan-targets

Parameters

host <hostname>	Specify the IP address of the iSCSI portal.

Usage

Use this command to ensure that newly configured iSCSI targets are added.

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi portal host 10.2.3.4 rescan-targets
```

Product

Granite Core

Related Topics

"storage iscsi portal host rescan-targets"

failover-peer storage iscsi portal host target add

Description

Adds an iSCSI target configuration to the specified portal.

Syntax

failover-peer storage iscsi portal host <hostname> target add name <name> [port <port>] [snapshot-host <hostname>]

Parameters

host <hostname>	Specify the IP address of the iSCSI portal to which the target is to be added.
name <name>	Specify the name of the target.
port <port>	Optionally, specify a port number the iSCSI target is listening on. The default is 3260.
snapshot-host <hostname>	Optionally, specify the IP address for the storage snapshot.

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi portal host 10.2.3.4 target add name iqn.2003-
10.com.hoosgau:432716056 port 3260
```

Product

Granite Core

Related Topics

"storage iscsi portal host target add"

failover-peer storage iscsi portal host target modify

Description

Modifies the settings of the specified iSCSI portal target.

Syntax

failover-peer storage iscsi portal host <hostname> target modify name <name> [latency threshold <ms>] | [port <port>] | [snapshot-host <hostname>] | [snapshot-method {none | auto}]

Parameters

host <hostname>	Specify the IP address of the iSCSI portal with the target configuration.
name <name>	Modify the name of the target.
port <port>	Optionally, modify the port number the iSCSI target is listening on. The default is 3260.
snapshot-host <hostname>	Optionally, modify the IP address for the storage snapshot.
snapshot-method {none | auto}	Optionally, modify the snapshot method by specifying one of the following • **none** - No snapshot management • **auto** - Automatically detect snapshot management if already configured

Usage

All **failover-peer edge** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi portal host 10.2.3.4 target modify name iqn.2003-
10.com.hoosgau:432716056
```

Product

Granite Core

Related Topics

"storage iscsi portal host target modify"

failover-peer storage iscsi portal host target offline-luns

Description

Takes offline all configured LUNs serviced by the specified iSCSI target.

Syntax

failover-peer storage iscsi portal host <hostname> target offline-luns name <name>

Parameters

host <hostname>	Specify the IP address of the iSCSI portal with the target configuration.
name <name>	Specify the name of the target.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi portal host 10.2.3.4 target offline-luns name
iqn.2003-10.com.hoosgau:432716056
```

Product

Granite Core

Related Topics

"storage iscsi portal host target offline-luns"

failover-peer storage iscsi portal host target remove

Description

Removes an iSCSI target configuration from the specified portal.

Syntax

failover-peer storage iscsi host <hostname> target remove name <name>

Parameters

host <hostname>	Specify the IP address of the iSCSI portal with the target configuration to be removed.
name <name>	Specify the name of the target to be removed.

Usage

You must first remove all LUNs from a target before you can remove the target itself.

Use the "storage host-info add" command to remove all LUNs from a target.

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi portal host 10.2.3.4 target remove name iqn.2003-
10.com.hoosgau:432716056
```

Product

Granite Core

Related Topics

"storage host-info add," "storage iscsi portal host target remove"

failover-peer storage iscsi portal modify host auth

Description

Modifies the authentication settings of the specified iSCSI portal.

Syntax

failover-peer storage iscsi portal modify host <hostname> auth {CHAP chap-user <name> | None}

Parameters

host <hostname>	Specify the IP address of the iSCSI portal to be modified.
auth	Specify one of the following authentication options: • **CHAP chap-user <name>** - Enables CHAP and specifies the CHAP user name. You must specify an existing CHAP user. • **None** - No authentication.

Usage

This command allows you to modify the portal within a running session.

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi portal modify host 10.2.3.4 auth None
```

Product

Granite Core

Related Topics

"storage iscsi portal modify host auth"

failover-peer storage iscsi portal modify host port

Description

Modifies the port setting of the iSCSI portal.

Syntax

failover-peer storage iscsi portal modify host <hostname> port <port>

Parameters

host <hostname>	Specify the IP address of the iSCSI portal whose port setting is to be modified.
port <port>	Specify the new port number for the iSCSI portal to listen on. The default is 3260.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi portal modify host 10.2.3.4 port 3260
```

Product

Granite Core

Related Topics

"storage iscsi portal modify host port"

failover-peer storage iscsi portal remove host

Description

Removes an iSCSI portal configuration from the iSCSI initiator configuration.

Syntax

failover-peer storage iscsi portal remove host <hostname>

Parameters

host <hostname>	Specify the IP address of the iSCSI portal configuration to be removed.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi portal remove host 10.2.3.4
```

Product

Granite Core

Related Topics

"storage iscsi portal remove host"

failover-peer storage iscsi session mpio

Description

Enables or disables MPIO functionality for the iSCSI initiator configuration.

Syntax

failover-peer storage iscsi session mpio {disable | enable}

Parameters

disable	Specify this parameter to disable MPIO functionality.
enable	Specify this parameter to enable MPIO functionality.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi session mpio enable
```

Product

Granite Core

Related Topics

"show storage iscsi mpio interfaces"

failover-peer storage iscsi session mpio standard-routes

Description

Enables or disables standard routing for MPIO interfaces.

Syntax

failover-peer storage iscsi session mpio standard-routes {disable | enable}

Parameters

disable	Specify this parameter to disable standard routing for MPIO connections.
enable	Specify this parameter to enable standard routing for MPIO connections.

Usage

If the iSCSI portal is not in the same subnet as the interfaces configured for MPIO, this functionality allows the connection to be established using standard routing.

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage iscsi session mpio standard-routes enable
```

Product

Granite Core

Related Topics

"storage iscsi session mpio standard-routes,"

failover-peer storage snapshot add host

Description

Specifies the host settings for the Snapshot credential.

Syntax

failover-peer storage snapshot add host <host> type <type> {username <username> password <password>} [protocol <NetApp protocol>] [port <NetApp port>]

Parameters

host <hostname>	Specify the IP address of the Snapshot credential.
type <type>	Specify one of the following storage systems: • EMC-CLARiiON • Dell-EqualLogic • NetApp **Note:** If you specify NetApp, you must specify protocol and port settings in addition to user name and password.
username <username>	Supply a valid user name for the Snapshot credential.
password <password>	Supply a valid password for the Snapshot credential.
protocol <NetApp protocol>	For NetApp configuration only, specify either HTTP or HTTPS.
port <NetApp port>	For NetApp configuration only, specify the port on the NetApp array.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage snapshot add host 10.11.12.13 type EMC-CLARiiON username
jdoe password h00haa
```

Product

Granite Core

Related Topics

"storage snapshot add host," "show failover-peer storage snapshot"

failover-peer storage snapshot host modify

Description

Modifies the Snapshot credentials for the storage array.

Syntax

failover-peer storage snapshot host <host> modify {port <port> | protocol <protocol> | username <username> password <password>}

Parameters

host <host>	Specify the IP address of the Snapshot credential whose credentials are to be modified.
port <NetApp port>	For NetApp configuration only, specify a new value for the port on the NetApp array.
protocol <NetApp protocol>	For NetApp configuration only, specify either HTTP or HTTPS.
username <username>	Supply a valid user name for the Snapshot credential.
password <password>	Supply a valid password for the Snapshot credential.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage snapshot host 10.11.12.13 modify username jdoe password
h00haa
```

Product

Granite Core

Related Topics

"storage snapshot host modify," "show failover-peer storage snapshot"

failover-peer storage snapshot remove host

Description

Removes the Snapshot credential configuration.

Syntax

failover-peer storage snapshot remove host <host>

Parameters

host <host>	Specify the IP address of the Snapshot credential configuration to be removed.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 (config) # failover-peer storage snapshot remove host 10.11.12.13
```

Product

Granite Core

Related Topics

"storage snapshot remove host," "show failover-peer storage snapshot"

storage block-disk rescan

Description

Rescans for new local disks available for discovery.

Syntax

storage block-disk rescan

Parameters

None

Example

```
Core_02 (config) # storage block-disk rescan
```

Product

Granite Core

Related Topics

"storage host-info add", "storage host-info modify", "storage host-info remove"

storage host-info add

Description

Adds a new host configuration for snapshot operations.

Syntax

[failover-peer] storage host-info add host <host> username <username> password <password> host-type <host-type>

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on the failover peer of the current appliance. If the peer is unavailable, the changed configuration is automatically applied when the appliance returns to service. All **failover-peer** commands enable you to configure an unavailable Granite Core appliance through its failover peer. When the Granite Core appliance returns to service, the new configuration is added automatically.
<host>	Specify the hostname or IP address.
<username>	Create the required username.
<password>	Create the required password.
<host-type>	Specify the host type.

Usage

This command is part of a workflow for configuring application-consistent snapshot and data protection settings on the current appliance:

- Use the "storage host-info add" (the current command) or "storage host-info modify" command to configure one or more proxy hosts for the snapshots.
- Use the "storage lun modify client-type" command to specify the LUN client type as Windows or VMware.
- Enable and configure application-consistent snapshots:
  – "storage lun modify snapshot clear-host"
  – "storage lun modify snapshot-config app-consistent"
- Enable and configure data protection:
  – "storage lun modify snapshot host"
  – "storage lun modify snapshot-config proxy-backup"
- Enable and configure the snapshot schedule:
  – "storage lun modify scheduled-snaps"

– "storage lun modify scheduled-snaps add"

Example

```
Core_02 (config) # storage host-info add host SAN-14
```

Product

Granite Core

Related Topics

"storage host-info modify", "storage host-info remove"

storage host-info modify

Description

Modifies an existing host configuration for snapshot operations.

Syntax

[failover-peer] storage host-info modify host <host> [username <username> password <password>] [host-type <host-type>]

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
<host>	Specify the hostname or IP address of the host whose configuration is to be modified.
<username>	Optionally, modify the username.
<password>	Optionally, modify the password.
<host-type>	Optionally, modify the host type.

Usage

This command is part of a workflow for configuring application-consistent snapshot and data protection settings on the current appliance:

- Use the "storage host-info add" or "storage host-info modify" command (the current command) to configure one or more proxy hosts for the snapshots.
- Use the "storage lun modify client-type" command to specify the LUN client type as Windows or VMware.
- Enable and configure application-consistent snapshots:
  – "storage lun modify snapshot clear-host"
  – "storage lun modify snapshot-config app-consistent"
- Enable and configure data protection:
  – "storage lun modify snapshot host"
  – "storage lun modify snapshot-config proxy-backup"
- Enable and configure the snapshot schedule:
  – "storage lun modify scheduled-snaps"
  – "storage lun modify scheduled-snaps add"

Example

```
Core_02 (config) # storage host-info modify host SAN-14 username pilot62 password Sw3245e
```

Product

Granite Core

Related Topics

"storage host-info remove"

storage host-info remove

Description

Removes the specified snapshot host configuration.

Syntax

[failover-peer] storage host-info remove host <host>

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
<host>	Specify the hostname or IP address of the host whose configuration is to be removed.

Example

```
Core_02 (config) # storage host-info remove host SAN-14
```

Product

Granite Core

Related Topics

"storage host-info modify", "storage host-info add"

storage iscsi chap add

Description

Adds a CHAP user to the current storage configuration.

Syntax

storage iscsi chap add username <username> password <password>

Parameters

username <username>	Specify the user name for CHAP authentication.
password <password>	Specify the password for the new CHAP user.

Example

```
Core_02 (config) # storage iscsi chap add username DefaultChap password CHAPpw
```

Product

Granite Core

Related Topics

"failover-peer storage iscsi chap add," "show storage iscsi"

storage iscsi chap delete

Description

Deletes the specified CHAP user from the current storage configuration.

Syntax

storage iscsi chap delete username <username> [force]

Parameters

username <username>	Specify the CHAP user to be deleted.
force	Forces deletion if the CHAP user is currently enabled.

Example

```
Core_02 (config) # storage iscsi chap delete username DefaultChap
```

Product

Granite Core

Related Topics

"failover-peer storage iscsi chap delete," "show storage iscsi"

storage iscsi chap modify

Description

Modifies the password of the specified CHAP user.

Syntax

storage iscsi chap modify username <username> password <password>

Parameters

username <username>	Specify the CHAP user whose password is to be modified
password <password>	Specify the new password for the CHAP user.

Example

```
Core_02 (config) # storage iscsi chap modify username DefaultChap password newCHAPpw
```

Product

Granite Core

Related Topics

"failover-peer storage iscsi chap modify," "show storage iscsi"

storage iscsi chap username

Description

Enables or disables the specified CHAP user.

Syntax

storage iscsi chap username <name> {disable | enable}

Parameters

username <username>	Specify the CHAP user to be enabled or disabled.
disable	Specify this parameter to disable the specified CHAP user.
enable	Specify this parameter to enable the specified CHAP user.

Usage

Run the "show storage iscsi" or "show failover-peer storage iscsi" command to display whether or not the CHAP user is enabled.

Disable or enable the CHAP user as needed.

Example

```
Core_02 (config) # storage iscsi chap username JoeyD disable
```

Product

Granite Core

Related Topics

"show storage iscsi," "failover-peer storage iscsi chap username," "show failover-peer storage iscsi"

storage iscsi data-digest

Description

Includes or excludes the data digest in the iSCSI PDU.

Syntax

storage iscsi data-digest {disable | enable}

Parameters

disable	Specify this parameter to exclude the data digest from the iSCSI PDU.
enable	Specify this parameter to include the data digest in the iSCSI PDU.

Usage

The data digest can help to identify, reject, or request retransmission of a corrupt PDU.

Example

```
Core_02 (config) # storage iscsi data-digest disable
Core_02 (config) # storage iscsi data-digest enable
```

Product

Granite Core

Related Topics

"failover-peer storage iscsi data-digest," "show failover-peer storage iscsi" "edge id iscsi data-digest," "show storage iscsi"

storage iscsi header-digest

Description

Includes or excludes the header digest in or from the iSCSI PDU.

Syntax

storage iscsi header-digest {enable | disable}

Parameters

enable	Specify this parameter to include the header digest in the iSCSI PDU.
disable	Specify this parameter to exclude the header digest from the iSCSI PDU.

Usage

The header digest can help to identify, reject, or request retransmission of a corrupt PDU.

Example

```
Core_02 (config) # storage iscsi header-digest disable
Core_02 (config) # storage iscsi header-digest enable
```

Product

Granite Core

Related Topics

"failover-peer storage iscsi header-digest," "show failover-peer storage iscsi," "edge id iscsi header-digest," "show storage iscsi"

storage iscsi initiator modify auth mutual-chap

Description

Configures iSCSI initiator authentication mutual CHAP settings.

Syntax

storage iscsi initiator modify auth mutual-chap {chap-user <name> | disable | enable}

Parameters

chap-user <name>	Specify the mutual CHAP user. You must specify an existing CHAP user.
disable	Specify this parameter to disable mutual CHAP authentication.
enable	Specify this parameter to enable mutual CHAP authentication.

Usage

Use this command to:

- enable or disable mutual CHAP authentication for the iSCSI initiator configuration.
- specify the mutual CHAP user.

You can specify only existing CHAP users.

Example

```
Core_02 (config) # storage iscsi initiator modify auth mutual-chap chap-user existingCHAPUser
Core_02 (config) # storage iscsi initiator modify auth mutual-chap enable
```

Product

Granite Core

Related Topics

"failover-peer storage iscsi initiator modify auth mutual-chap," "storage iscsi initiator modify name," "show storage iscsi"

storage iscsi initiator modify name

Description

Modifies the initiator name in the iSCSI initiator configuration.

Syntax

storage iscsi initiator modify name <name>

Parameters

name <name>	Specify the new initiator name for the iSCSI initiator configuration.

Example

```
Core_02 (config) # storage iscsi initiator modify name iqn.2003-10.com.hoosegow:werdna-initiator
```

Product

Granite Core

Related Topics

"failover-peer storage iscsi initiator modify name," "show storage iscsi"

storage iscsi mpio interface add

Description

Adds the specified local interface for MPIO to the iSCSI initiator configuration.

Syntax

storage iscsi mpio interface add name <name>

Parameters

name <name>	Specify the local interface to be added.

Example

```
Core_02 (config) # storage iscsi mpio interface add name eth0_1
```

Product

Granite Core

Related Topics

"storage iscsi mpio interface remove," "storage iscsi session mpio standard-routes," "show storage iscsi mpio interfaces"

storage iscsi mpio interface remove

Description

Removes the specified local interface for MPIO from the iSCSI initiator configuration.

Syntax

storage iscsi mpio interface remove name <name> [all]

Parameters

name <name>	Specify the local interface to be removed. To view a list of local interfaces configured for MPIO, use the "show storage iscsi mpio interfaces" command.
all	Remove all MPIO interfaces.

Example

```
Core_02 (config) # show storage iscsi mpio interfaces
Interfaces configured for MPIO
        eth0_2
        eth0_3
Core_02 (config) # storage iscsi mpio interface remove name eth0_2
```

Product

Granite Core

Related Topics

"show storage iscsi disc-portals portal," "storage iscsi session mpio standard-routes," "storage iscsi mpio interface add"

storage iscsi portal add host

Description

Adds an iSCSI portal configuration to the iSCSI initiator configuration.

Syntax

storage iscsi portal add host <hostname> [port <port>] auth {CHAP chap-user <name> | None}

Parameters

host <hostname>	Specify the IP address of the iSCSI portal.
port <port>	Optionally, specify a port number. The default is 3260.
auth	Specify one of the following authentication options: • **CHAP chap-user <name>** - Enables CHAP and specifies the CHAP user name. You must specify an existing CHAP user. • **None** - No authentication.

Example

```
Core_02 (config) # storage iscsi portal add host 10.2.3.4 port 3260 auth CHAP chap-user JoeyD
```

Product

Granite Core

Related Topics

"storage iscsi portal host target add," "storage iscsi portal host target modify," "storage iscsi portal host target remove," "storage iscsi portal modify host auth," "storage iscsi portal modify host port," "storage iscsi portal remove host"

storage iscsi portal host disc-portal add

Description

Manually adds a discovered portal IP address to the iSCSI portal configuration.

Syntax

storage iscsi portal host <hostname> disc-portal add ip <ip> [port <port>]

Parameters

<hostname>	Specify the hostname of the iSCSI portal configuration to which the additional IP address is to be added.
<ip>	Specify the IP address of the added, discovered portal.
[port <port>]	Optionally, specify a port number to the additional IP address.

Usage

If you have enabled multi-path I/O (MPIO), this command enables you to add existing IP addresses available on the filer for connections with the Granite Core appliance.

MPIO enables a single iSCSI portal configuration to connect with the filer on multiple IP addresses.

Use the "storage iscsi portal host rescan-portals" command to discover portals on the specified iSCSI initiator.

Example

```
Core_02 (config) # storage iscsi portal host 123.45.6.789 add 132.45.6.780
```

Product

Granite Core

Related Topics

"show storage iscsi disc-portals portal," "storage iscsi portal host disc-portal modify," "storage iscsi portal host disc-portal remove," "storage iscsi portal host rescan-portals"

storage iscsi portal host disc-portal modify

Description

Modifies the ID and/or port settings of the specified portal host configuration.

Syntax

storage iscsi portal host <hostname> disc-portal modify id <disc-portal> port <port>

Parameters

<hostname>	Specify the hostname of the iSCSI portal configuration that is to be modified.
id <disc-portal>	Specify the new ID value for the specified portal host.
<port>	Specify the new port number for specified portal host.

Usage

This command is intended to be used for portals discovered for multi-path I/O (MPIO) configurations. MPIO enables a single iSCSI portal configuration to connect with the filer on multiple IP addresses.

Use the "storage iscsi portal host rescan-portals"command to discover portals on the specified iSCSI initiator portal.

Example

```
Core_02 (config) # storage iscsi portal host 123.45.6.789 disc-portal modify id principal port 3260
```

Product

Granite Core

Related Topics

"show storage iscsi disc-portals portal"

storage iscsi portal host disc-portal remove

Description

Removes the specified discovered portal configuration from the iSCSI portal configuration.

This command is intended to be used for portals discovered for multi-path I/O (MPIO) configurations. MPIO enables a single iSCSI portal configuration to connect with the filer on multiple IP addresses.

Syntax

storage iscsi portal host <hostname> disc-portal remove id <disc-portal>

Parameters

<hostname>	Specify the hostname of the iSCSI portal configuration to which the additional IP address is to be added.
<disc-portal>	Specify the IP address of the discovered portal to be removed from the iSCSI portal configuration.

Usage

Use the "storage iscsi portal host rescan-portals" command to discover portals on the specified iSCSI initiator portal.

Example

```
Core_02 (config) # storage iscsi portal host 123.45.6.789 disc-portal remove 132.45.6.780
```

Product

Granite Core

Related Topics

"show stats storage filer-ios," "storage iscsi portal host disc-portal add," "storage iscsi portal host disc-portal modify," "storage iscsi portal host rescan-portals"

storage iscsi portal host offline-luns

Description

Takes offline all configured LUNs serviced by the specified portal.

Syntax

storage iscsi portal host <hostname> offline-luns

Parameters

host <hostname>	Specify the IP address of the iSCSI portal.

Example

```
Core_02 (config) # storage iscsi portal host 10.2.3.4 offline-luns
```

Product

Granite Core

Related Topics

"storage iscsi mpio interface add," "storage iscsi portal host target modify," "storage iscsi portal host target remove"

storage iscsi portal host rescan-luns

Description

Rescans iSCSI targets associated with the specified portal.

Syntax

storage iscsi portal host <hostname> rescan-luns {all] | target name <name>}

Parameters

host <hostname>	Specify the IP address of the iSCSI portal.
all	Rescans all iSCSI targets associated with the specified portal.
target name <name>	Rescans only the specified target.

Usage

Use this command to ensure that recently configured iSCSI targets are added.

Example

```
Core_02 (config) # storage iscsi portal host 10.2.3.4 rescan all
```

Product

Granite Core

Related Topics

“failover-peer storage iscsi portal host rescan-luns,” “storage iscsi portal host rescan-targets”

storage iscsi portal host rescan-portals

Description

Rescans the specified iSCSI portal configuration for discoverable and available portals.

This command is intended to be used for portals discovered for multi-path I/O (MPIO) configurations. MPIO enables a single iSCSI portal configuration to connect with the filer on multiple IP addresses.

Syntax

storage iscsi portal host <hostname> rescan-portals

Parameters

<hostname>	Specify the hostname of the iSCSI portal configuration from which the discovered portal is to be removed.

Usage

After portals have been discovered, you can add them to the iSCSI portal configuration using the “storage iscsi portal host disc-portal add” command.

Example

```
Core_02 (config) # storage iscsi portal host 123.45.6.789 rescan-portals
```

Product

Granite Core

Related Topics

“show stats storage filer-ios,” “storage iscsi portal host disc-portal add,” “storage iscsi portal host disc-portal remove,” “storage iscsi portal host disc-portal modify”

storage iscsi portal host rescan-targets

Description

Rescans all iSCSI targets associated with the specified portal.

Syntax

storage iscsi portal host <hostname> rescan-targets

Parameters

host <hostname>	Specify the IP address of the iSCSI portal.

Usage

Use this command to ensure that recently configured iSCSI targets are added.

Example

```
Core_02 (config) # storage iscsi portal host 10.2.3.4 rescan-targets
```

Product

Granite Core

Related Topics

"storage iscsi mpio interface add," "storage iscsi portal host target modify," "storage iscsi portal host rescan-luns,"

storage iscsi portal host target add

Description

Adds an iSCSI target configuration to the specified portal.

Syntax

storage iscsi portal host <hostname> target add name <name> [port <port>] [snapshot-host <hostname>]

Parameters

host <hostname>	Specify the IP address of the iSCSI portal to which the target is to be added.
name <name>	Specify the name of the target.
port <port>	Optionally, specify a port number the iSCSI target is listening on. The default is 3260.
snapshot-host <hostname>	Optionally, specify the IP address for the storage snapshot.

Example

```
Core_02 (config) # storage iscsi portal host 10.2.3.4 target add name iqn.2003-
10.com.hoosgau:432716056 port 3260
```

Product

Granite Core

Related Topics

"storage iscsi mpio interface add," "storage iscsi portal host target modify"

storage iscsi portal host target modify

Description

Modifies the settings of the specified iSCSI portal target.

Syntax

storage iscsi portal host <hostname> target modify name <name> [latency threshold <ms>] [port <port>] [snapshot-host <hostname>] [snapshot-method {none | auto}]

Parameters

host <hostname>	Specify the IP address of the iSCSI portal with the target configuration.
name <name>	Modify the name of the target.
latency threshold <ms>	Optionally, modify the latency threshold, in milliseconds.
port <port>	Optionally, modify the port number the iSCSI target is listening on. The default is 3260.
snapshot-host <hostname>	Optionally, modify the IP address for the storage snapshot.
snapshot-method <method>	Optionally, modify the snapshot method by specifying one of the following: • **none** - No snapshot management • **auto** - Automatically detect snapshot management if already configured

Example

```
Core_02 (config) # storage iscsi portal host 10.2.3.4 target modify name iqn.2003-
10.com.hoosgau:432716056
```

Product

Granite Core

Related Topics

"storage iscsi mpio interface add," "storage iscsi portal host target remove"

storage iscsi portal host target offline-luns

Description

Takes offline all configured LUNs serviced by the specified iSCSI target.

Syntax

storage iscsi portal host <hostname> target offline-luns name <name>

Parameters

host <hostname>	Specify the IP address of the iSCSI portal with the target configuration.
name <name>	Specify the name of the target.

Example

```
Core_02 (config) # storage iscsi portal host 10.2.3.4 target offline-luns name iqn.2003-
10.com.hoosgau:432716056
```

Product

Granite Core

Related Topics

"storage iscsi mpio interface add," "storage iscsi portal host target modify"

storage iscsi portal host target remove

Description

Removes an iSCSI target configuration from the specified portal.

Syntax

storage iscsi portal host <hostname> target remove name <name>

Parameters

host <hostname>	Specify the IP address of the iSCSI portal with the target configuration to be removed.
name <name>	Specify the name of the target to be removed.

Usage

You must first remove all LUNs from a target before you can remove the target itself.

Use the "storage lun remove" command to remove all LUNs from a target.

Example

```
Core_02 (config) # storage iscsi portal host 10.2.3.4 target remove name iqn.2003-
10.com.hoosgau:432716056
```

Product

Granite Core

Related Topics

"storage iscsi mpio interface add," "storage iscsi portal host target modify"

storage iscsi portal modify host auth

Description

Modifies the authentication settings of the specified iSCSI portal.

Syntax

storage iscsi portal modify host <hostname> auth {CHAP chap-user <name> | None}

Parameters

host <hostname>	Specify the IP address of the iSCSI portal to be modified.
auth	Specify one of the following authentication options: • **CHAP chap-user <name>** - Enables CHAP and specifies the CHAP user name. You must specify an existing CHAP user. • **None** - No authentication.

Usage

This command allows you to modify the portal within a running session.

Example

```
Core_02 (config) # storage iscsi portal modify host 10.2.3.4 auth None
```

Product

Granite Core

Related Topics

"storage iscsi mpio interface add," "storage iscsi portal host target modify," "storage iscsi portal host target remove"

storage iscsi portal modify host port

Description

Modifies the port settings of the specified iSCSI portal.

Syntax

storage iscsi portal modify host <hostname> port <port>

Parameters

host <hostname>	Specify the IP address of the iSCSI portal whose port setting is to be modified.
port <port>	Specify the new port number for the iSCSI portal to listen on. The default is 3260.

Example

```
Core_02 (config) # storage iscsi portal modify host 10.2.3.4 port 3260
```

Product

Granite Core

Related Topics

"storage iscsi mpio interface add," "storage iscsi portal host target modify," "storage iscsi portal remove host"

storage iscsi portal remove host

Description

Removes an iSCSI portal configuration from the iSCSI initiator configuration.

Syntax

storage iscsi portal remove host <hostname>

Parameters

host <hostname>	Specify the IP address of the iSCSI portal configuration to be removed.

Example

```
Core_02 (config) # storage iscsi portal remove host 10.2.3.4
```

Product

Granite Core

Related Topics

"storage iscsi mpio interface add," "storage iscsi portal host target modify," "storage iscsi portal host target remove"

storage iscsi session mpio

Description

Enables or disables MPIO functionality for the iSCSI initiator configuration.

Syntax

storage iscsi session mpio {disable | enable}

Parameters

disable	Specify this parameter to disable MPIO functionality.
enable	Specify this parameter to enable MPIO functionality.

Example

```
Core_02 (config) # storage iscsi session mpio enable
```

Product

Granite Core

Related Topics

"failover-peer storage iscsi session mpio"

storage iscsi session mpio standard-routes

Description

Enables or disables standard routing for MPIO interfaces.

If the iSCSI portal is not in the same subnet as the interfaces configured for MPIO, this functionality allows the connection to be established using standard routing.

Syntax

storage iscsi session mpio standard-routes {disable | enable}

Parameters

disable	Specify this parameter to disable standard routing for MPIO connections.
enable	Specify this parameter to enable standard routing for MPIO connections.

Example

```
Core_02 (config) # storage iscsi session mpio standard-routes enable
```

Product

Granite Core

Related Topics

"failover-peer storage iscsi session mpio standard-routes"

storage lun add block-disk

Description

Adds a block disk LUN for the Granite Core appliance.

You can add only discovered LUNs.

Syntax

[failover-peer] storage lun add block-disk serial <serial> alias <alias-name>

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
serial <serial>	Specify the LUN with its serial number.
alias <alias-name>	Specify an alias name for the added LUN.

Example

```
Core_02 (config) # storage lun add block-disk serial 60a98132486e2f374f9f6f795f61565a alias
LUN4Edge2
```

Product

Granite Core

Related Topics

"storage lun add edge-local", "storage lun add iscsi"

storage lun add edge-local

Description

Adds an edge local LUN for the Granite Core appliance.

You can add only discovered LUNs.

Syntax

[failover-peer] storage lun add edge-local edge-id <id> size <MBs> alias <alias-name>

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
edge-id <id>	Specify the self-identifier of the Granite Edge appliance to which the LUN is to be added.
size <MBs>	Specify the size of the LUN, in megabytes. The minimum value is 8 MB. The maximum depends on the available space for the blockstore.
alias <alias-name>	Specify an alias name for the added LUN.

Example

```
Core_02 (config) # storage lun add edge-local edge-id Edge2 size 256 alias LUN4Edge2
```

Product

Granite Core

Related Topics

"storage lun add block-disk", "storage lun add iscsi"

storage lun add iscsi

Description

Adds an iSCSI LUN for the Granite Core appliance.

Syntax

[failover-peer] storage lun add iscsi serial <serial> alias <alias-name>

Parameters

serial <serial>	Specify the iSCSI serial number at the storage array. You must use a multiple of 512.
alias <alias-name>	Optionally, specify an alias name for the LUN.

Example

```
Core_02 (config) # storage lun add iscsi serial hqD6Wo/hWNjx alias LUN4Edge2
```

Product

Granite Core

Related Topics

"storage lun add block-disk", "storage lun add edge-local"

storage lun modify auth-igroup

Description

Adds or removes an authorized group of iSCSI initiator credentials (igroup) to the LUN specified by its LUN alias.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} auth-igroup {add | remove} <igroup-name>

Parameters

alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
add <igroup-name>	Specify the authorized group of iSCSI initiator credentials (igroup) to be added the specified LUN.
remove <igroup-name>	Specify the authorized group of iSCSI initiator credentials (igroup) to be removed from the specified LUN.

Example

```
Core_02 (config) # storage lun modify alias DC-B01 auth-igroup add igroupName
```

Product

Granite Core

Related Topics

"storage lun modify auth-igroup", "storage lun modify auth-initiator"

storage lun modify auth-initiator

Description

Adds or removes an authorized iSCSI initiator to or from the LUN specified by its alias.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} auth-initiator {add | remove} <initiator-name>

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
add <initiator-name>	Use this parameter to add the specified, authorized iSCSI initiator to the specified LUN.
remove <initiator-name>	Use this parameter to remove the authorized iSCSI initiator from the specified LUN.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 auth-initiator add iqn.2003-
10.com.hoosegow:werdna-initiator
```

Product

Granite Core

Related Topics

"storage lun modify auth-initiator"

storage lun modify client-type

Description

Modifies the client type (VMware, Windows, other) of the configured LUN, specified by its alias.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} client-type <client-type> [force]

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
client-type <client-type>	Specify the new client type in lowercase letters: **vmware**, **windows**, or **other**.
[force]	Optionally, include this parameter to force the change in client type.

Usage

This command is part of a workflow for configuring application-consistent snapshot and data protection settings on the current appliance:

- Use the "storage host-info add" or "storage host-info modify" command to configure one or more proxy hosts for the snapshots.
- Use the "storage lun modify client-type" command (the current command) to specify the LUN client type as Windows or VMware.
- Enable and configure application-consistent snapshots:

  - "storage lun modify snapshot clear-host"
  - "storage lun modify snapshot-config app-consistent"
- Enable and configure data protection:
  - "storage lun modify snapshot host"
  - "storage lun modify snapshot-config proxy-backup"
- Enable and configure the snapshot schedule:
  - "storage lun modify scheduled-snaps"
  - "storage lun modify scheduled-snaps add"

Example

```
Core_02 (config) # storage lun modify alias LUN2GO client-type vmware
```

Product

Granite Core

Related Topics

"show storage lun"

storage lun modify failover

Description

Enables or disables the failover configuration. This command is enabled by default.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} failover {disable | enable}

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
disable	Disables the failover configuration.
enable	Enables the failover configuration.

Example

```
Core_02 (config) # storage lun modify alias LUN2GO failover enable
```

Product

Granite Core

Related Topics

"show storage lun,""Branch Storage Commands"

storage lun modify map edge-id

Description

Maps the LUN to the specified Granite Edge appliance.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} map edge-id <edge-self-identifier>

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial<serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
edge-id <edge-self-identifier>	Specify the self-identifier of the Granite Edge appliance to which the LUN is to be added.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 map edge-id Edge2
```

Product

Granite Core

Related Topics

"storage host-info add"

storage lun modify mpio path

Description

Configures MPIO paths for the LUN.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} mpio path {allow | exclude | preferred} path-id <path-id>

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial<serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
allow	Allows the specified path to be used in the MPIO configuration.
exclude	Excludes the specified path from being used in the MPIO configuration.
preferred	Configures the specified path as the preferred (principal) path for connections.

Example

```
Core_02 (config) # storage lun modify {alias <alias> | serial <serial>} mpio path allow path-id aux
```

Product

Granite Core

Related Topics

"storage lun modify mpio policy"

storage lun modify mpio policy

Description

Configures MPIO paths for the LUN.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} mpio policy {roundrobin | fixedpath}

Parameters

alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
roundrobin	Select this option for paths usage to rotate.
fixedpath	Select this option to configure specific paths.

Example

```
Core_02 (config) # storage lun modify {alias <alias> | serial <serial>} mpio policy roundrobin
```

Product

Granite Core

Related Topics

"storage lun modify mpio path"

storage lun modify new-alias

Description

Modifies the alias name for the specified LUN.

Syntax

[failover-peer] storage lun {alias <alias> | serial <serial>} new-alias <new-alias>

Parameters

alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
new-alias <new-alias>	Specify the new alias name. In addition to alphanumeric characters, you may also use the hyphen (-), underscore (_), and slashes (/).

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 new-alias LUN4EDGE6
```

Product

Granite Core

Related Topics

"Branch Storage Commands"

storage lun modify offline

Description

Takes offline the LUN indicated by the alias or serial number.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} offline

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.

Usage

This process might take a few minutes to complete.

Prior to taking the LUN offline with this command, you must stop the Windows server at the edge using the LUN and unmount the LUN (if the Windows server is running on ESX).

To complete LUN removal, use "storage lun remove" on page 875.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 offline

Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx offline
```

Product

Granite Core

Related Topics

"storage lun remove," "storage lun modify online"

storage lun modify online

Description

Brings online the LUN indicated by the alias or serial number.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} online

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 online

Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx online
```

Product

Granite Core

Related Topics

"storage lun modify offline,"

storage lun modify pinned

Description

Pins or unpins the LUN specified by its alias or serial number.

When a LUN is pinned, the data is reserved and not subject to the normal block store eviction policies.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} pinned {disable | enable}

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
disable	Set the LUN to an unpinned state.
enable	Set the LUN to a pinned state.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 pinned enable

Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx pinned enable
```

Product

Granite Core

Related Topics

"show storage lun," "storage lun modify prepop"

storage lun modify prepop

Description

Enable prepopulation for the LUN specified by its alias or serial number.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} prepop {enable | disable}

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
enable	Enables prepopulation from the specified LUN.
disable	Disables prepopulation from the specified LUN.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 prepop enable
Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx prepop disable
```

Product

Granite Core

Related Topics

"show storage lun," "storage lun modify prepop schedule add," "storage lun modify prepop schedule modify-sched," "storage lun modify prepop schedule remove"

storage lun modify prepop schedule add

Description

Adds a new prepopulation schedule for the LUN specified by its alias or serial number.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} prepop schedule add sched-name <sched-name> start-week-day <start-week-day> start-time <start-time> stop-week-day <stop-week-day> stop-time <stop-time>

Parameters

alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
sched-name <sched-name>	Specify the name of the prepopulation schedule.
start-week-day <start-week-day>	Specify the start day for the schedule. Use the first three characters (lowercase) of the English term for the day of the week: for example, **sun**, **mon**, **tue**, and so on.
start-time <start-time>	Specify the start time for the schedule. Use the format HH:MM:SS.
stop-week-day <stop-week-day>	Specify the stop day for the schedule. Use the first three characters (lowercase) of the English term for the day of the week: for example, **sun**, **mon**, **tue**, and so on.
stop-time <stop-time>	Specify the stop time for the schedule. Use the format HH:MM:SS.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 prepop schedule add sched-name WeeklySynch
start-week-day mon start-time 00:01:00 stop-week-day mon stop-time 03:01:00

Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx prepop schedule add sched-name WeeklySynch
start-week-day mon start-time 00:01:00 stop-week-day mon stop-time 03:01:00
```

Product

Granite Core

Related Topics

"show storage lun," "storage lun modify prepop," "storage lun modify prepop schedule modify-sched," "storage lun modify prepop schedule remove"

storage lun modify prepop schedule modify-sched

Description

Modifies the specified prepopulation schedule for the LUN specified by its alias or serial number.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} prepop schedule modify-sched sched-name <sched-name> start-week-day <start-week-day> start-time <start-time> stop-week-day <stop-week-day> stop-time <stop-time>

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
sched-name <sched-name>	Specify the modified name of the existing prepopulation schedule to be modified.
start-week-day <start-week-day>	Specify the modified start day for the schedule. Use the first three characters (lowercase) of the English term for the day of the week: for example, **sun**, **mon**, **tue**, and so on.
start-time <start-time>	Specify the modified start time for the schedule. Use the format HH:MM:SS.
stop-week-day <stop-week-day>	Specify the modified stop day for the schedule. Use the first three characters (lowercase) of the English term for the day of the week: for example, **sun**, **mon**, **tue**, and so on.
stop-time <stop-time>	Specify the modified the stop time for the schedule. Use the format HH:MM:SS.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 prepop schedule modify-sched sched-name
WeeklySynch start-week-day mon start-time 00:01:00 stop-week-day mon stop-time 03:01:00

Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx prepop schedule modify-sched sched-name
WeeklySynch start-week-day mon start-time 00:01:00 stop-week-day mon stop-time 03:01:00
```

Product

Granite Core

Related Topics

"show storage lun", "storage lun modify prepop,""storage lun modify prepop schedule add,""storage lun modify prepop schedule remove"

storage lun modify prepop schedule remove

Description

Removes the specified new prepopulation schedule from the specified LUN.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} prepop schedule remove sched-name <sched-name>

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
sched-name <sched-name>	Specify the name of the prepopulation schedule to be removed.

Example

```
Core_02 (config) # storage lun modify alias LUN2 prepop schedule remove sched-name MondaySynch
Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx prepop schedule remove sched-name
MondaySynch
```

Product

Granite Core

Related Topics

"show storage lun,""storage lun modify prepop", "storage lun modify prepop schedule add", "storage lun modify prepop schedule modify-sched"

storage lun modify prepop smart

Description

Enables smart prepopulation on the LUN specified by its alias or serial number.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} prepop smart {disable | enable}

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
disable	Disables prepopulation on the specified LUN.
enable	Enables prepopulation on the specified LUN.

Usage

You need to use smart prepopulation only if your LUN is not NTFS or VMFS.

Prepopulation can be enabled only if the LUN is pinned. For details, see "storage lun modify pinned".

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 prepop smart enable
Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx prepop smart enable
```

Product

Granite Core

Related Topics

“show storage lun,””storage lun modify prepop”, “storage lun modify prepop schedule add”, “storage lun modify prepop schedule modify-sched”

storage lun modify prepop start-now

Description

Begins the prepopulation process for the specified LUN configuration, starting from the current time.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} prepop start-now

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.

Example

```
Core_02 (config) # storage lun modify alias LUN2 prepop start-now

Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx prepop start-now
```

Product

Granite Core

Related Topics

“show storage lun,” “storage lun modify prepop,” “storage lun modify prepop schedule add,” “storage lun modify prepop schedule modify-sched,” “storage lun modify prepop smart”

storage lun modify pri-snap

Description

Configures private snapshot settings for the LUN specified by its alias or serial numbers.

You set either the maximum number of private snapshots that can be retained at any time, or enable and set a static value to be prepended to the private snapshot file names.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} pri-snap {max <count> | static-name {enable name <pri-snap-name> | disable}]

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
max <count>	Specify the maximum number of private snapshots to be taken of the specified LUN.
name <pri-snap-name>	Specify a string to be prepended to the file names of snapshots taken of this LUN.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 pri-snap max 14
Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx pri-snap static-name disable
```

Product

Granite Core

Related Topics

"show storage lun," "storage lun modify scheduled-snaps," "storage lun modify scheduled-snaps add,"

storage lun modify scheduled-snaps

Description

Enables or disables the scheduled snapshots feature for the specified LUN.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} scheduled-snaps {enable | disable} [force]

Parameters

alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
{enable | disable}	Enable or disable the scheduled snapshots feature for the specified LUN.
force	Include this parameter to force enable or force disable scheduled snapshots if the LUN is online. Riverbed recommends that you first take the LUN offline before enabling or disabling the scheduled snapshots feature.

Usage

This command is part of a workflow for configuring application-consistent snapshot and data protection settings on the current appliance:

- Use the "storage host-info add" or "storage host-info modify" command to configure one or more proxy hosts for the snapshots.
- Use the "storage lun modify client-type" command to specify the LUN client type as Windows or VMware.
- Enable and configure application-consistent snapshots:
  - "storage lun modify snapshot clear-host"
  - "storage lun modify snapshot-config app-consistent"

- Enable and configure data protection:
  - “storage lun modify snapshot host”
  - “storage lun modify snapshot-config proxy-backup”
- Enable and configure the snapshot schedule:
  - “storage lun modify scheduled-snaps” (the current command)
  - “storage lun modify scheduled-snaps add”

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 scheduled-snaps enable

Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx scheduled-snaps disable
```

Product

Granite Core

Related Topics

“storage lun modify scheduled-snaps add”

storage lun modify scheduled-snaps add

Description

Adds the specified snapshot policy to the configuration of the specified LUN.

A single snapshot policy can be assigned to more than one LUN, but each LUN can be associated with only a single snapshot policy.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} scheduled-snaps add <policy-name> [force]

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
add <policy-name>	Specify the snapshot policy to be added to the LUN. You define snapshot policies using the “storage snapshot policy add” command.
force	Include this parameter to force the invocation of the policy if the LUN is online. Riverbed recommends that you first take the LUN offline before making changes to snapshot configurations.

Usage

This command is part of a workflow for configuring application-consistent snapshot and data protection settings on the current appliance:

- Use the “storage host-info add” or “storage host-info modify” command to configure one or more proxy hosts for the snapshots.
- Use the “storage lun modify client-type” command to specify the LUN client type as Windows or VMware.
- Enable and configure application-consistent snapshots:
  - “storage lun modify snapshot clear-host”

- "storage lun modify snapshot-config app-consistent"

- Enable and configure data protection:
  - "storage lun modify snapshot clear-host"
  - "storage lun modify snapshot-config proxy-backup"
- Enable and configure the snapshot schedule:
  - "storage lun modify scheduled-snaps"
  - "storage lun modify scheduled-snaps add" (the current command)

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 scheduled-snaps policy add hourly5

Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx scheduled-snaps policy add hourly5
```

Product

Granite Core

Related Topics

"storage lun modify scheduled-snaps remove"

storage lun modify scheduled-snaps remove

Description

Removes any currently associated snapshot policy from the configuration of the specified LUN.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} scheduled-snaps remove [force]

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
force	Include this parameter to force the disassociation of the policy if the LUN is online. Riverbed recommends that you first take the LUN offline before making changes to snapshot configurations.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 scheduled-snaps policy add hourly5
Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx scheduled-snaps policy add hourly5
```

Product

Granite Core

Related Topics

"storage lun modify scheduled-snaps", "storage lun modify scheduled-snaps add"

storage lun modify scsi-res

Description

Enables or disables the specified LUN using SCSI reservations.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} scsi-res {disable | enable}

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
disable	Specify this parameter to disable the LUN using SCSI reservations.
enable	Specify this parameter to enable the LUN using SCSI reservations.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 scsi-res disable
Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx scsi-res enable
```

Product

Granite Core

Related Topics

"storage lun modify-all scsi-res"

storage lun modify snapshot clear-host

Description

Clears the snapshot host configuration from the configuration of the specified LUN.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} snapshot clear-host

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.

Usage

This command is part of a workflow for configuring application-consistent snapshot and data protection settings on the current appliance:

- Use the "storage host-info add" or "storage host-info modify" command to configure one or more proxy hosts for the snapshots.
- Use the "storage lun modify client-type" command to specify the LUN client type as Windows or VMware.
- Enable and configure application-consistent snapshots:
  - "storage lun modify snapshot clear-host" (the current command)
  - "storage lun modify snapshot-config app-consistent"
- Enable and configure data protection:
  - "storage lun modify snapshot host"
  - "storage lun modify snapshot-config proxy-backup"
- Enable and configure the snapshot schedule:
  - "storage lun modify scheduled-snaps"
  - "storage lun modify scheduled-snaps add"

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 snapshot clear-host
Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx snapshot clear-host
```

Product

Granite Core

Related Topics

"storage lun modify snapshot-config app-consistent"

storage lun modify snapshot-config app-consistent

Description

Configures application-consistent snapshots for the current appliance.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} snapshot-config app-consistent {clear | disable | enable | vmware } [host-info <host-info>] [datacenter <datacenter>] [include-vms <include-regex>] [exclude-vms <exclude-regex>] [script-timeout <seconds>] [quiesce-guest {enable | disable}]

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
clear	Clears the application-consistent snapshot configuration for the current appliance.
disable	Disables application-consistent snapshots for the current appliance.
enable	Enables application-consistent snapshots for the current appliance.
vmware	Include this parameter to modify VMware-specific parameters for the application-consistent snapshots configuration. Specify any combination of the following parameters: • **host-info <host-info>** - Specify the host information for VMware. • **datacenter <datacenter> -** Optionally, specify a datacenter for VMware-based application-consistent snapshots. • **include-vms <include-regex> -** Optionally, specify by regular expression the names of the VMs to be included. • **exclude-vms <exclude-regex> -** Optionally, specify by regular expression the names of the VMs to be excluded. • **script-timeout <seconds>** - Optionally, specify the time-out period for the application-consistent snapshot operation. Alternatively, specify any combination of the following parameters: • **quiesce-guest {enable | disable}** - Enables or disables quiescing VMs in the application-consistent snapshots. You cannot combine this parameter with any other VMware-specific parameters.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 snapshot-config app-consistent quiesce-guest
enable
Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx snapshot-config app-consistent quiesce-
guest disable
```

Product

Granite Core

Related Topics

“storage lun modify snapshot clear-host”

storage lun modify snapshot-config proxy-backup

Description

Configures data protection for snapshots for the failover peer of the current appliance.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} snapshot-config proxy-backup {clear | disable | enable | vmware {[datacenter <datacenter>] [exclude-hosts <exclude-host-regex>] [exclude-vms <exclude-regex>] [host-info <host-info>] [include-hosts <include-host-regex>] [include-vms <include-regex>] [script-timeout <seconds>] [snapshot-type <snapshot-type>]} | windows {[host-info <host-info>] [proxy-group <proxy-group>] [script-timeout <seconds>] [snapshot-type <snapshot-type>]}

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
clear	Clears the proxy backup host configuration.
disable	Disables the proxy backup for snapshots.
enable	Enables the proxy backup for snapshots.
vmware	Include this parameter to modify VMware-specific parameters for the proxy backup configuration. Specify any combination of the following parameters: • **datacenter <datacenter>** - Optionally, specify a datacenter for VMware-based application-consistent snapshots. • **exclude-hosts <exclude-host-regex>** - Optionally, specify by regular expression the ESXi hosts to be excluded. • **exclude-vms <exclude-regex>** - Optionally, specify by regular expression the names of the VMs to be excluded. • **host-info <host-info>** - Optionally, specify the host information for the proxy backup. • **include-hosts <include-host-regex>** - Optionally, specify by regular expression the ESXi hosts to be included. • **include-vms <include-regex>** - Optionally, specify by regular expression the names of the VMs to be included. • **script-timeout <seconds>** - Optionally, specify the time-out period for the backup operation on the proxy server. • **snapshot-type <snapshot-type>** - Optionally, specify the type of backup: **daily**, **hourly**, or **weekly**.
windows	Include this parameter to modify Windows-specific parameters for the proxy backup configuration. Specify any combination of the following parameters: • **host-info <host-info>** - Optionally, specify the host information for the proxy backup. • **proxy-group <proxy-group>** - Specify the storage group/Initiator group for the proxy (backup) server. • **script-timeout <seconds>** - Optionally, specify the time-out period for the backup operation on the proxy server. • **snapshot-type <snapshot-type>** - Optionally, specify the type of backup: **daily**, **hourly**, or **weekly**.

Usage

This command is part of a workflow for configuring application-consistent snapshot and data protection settings on the current appliance:

- Use the “storage host-info add” or “storage host-info modify” command to configure one or more proxy hosts for the snapshots.
- Use the “storage lun modify client-type” command to specify the LUN client type as Windows or VMware.
- Enable and configure application-consistent snapshots:

  - "storage lun modify snapshot clear-host"
  - "storage lun modify snapshot-config app-consistent"
- Enable and configure data protection:
  - "storage lun modify snapshot-config proxy-backup" (the current command)
- Enable and configure the snapshot schedule:
  - "storage lun modify scheduled-snaps"
  - "storage lun modify scheduled-snaps add"

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 snapshot-config proxy-backup datacenter
gandolfo

Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx snapshot-config proxy-backup datacenter
gandolfo
```

Product

Granite Core

Related Topics

"storage lun modify scheduled-snaps", "storage lun modify scheduled-snaps add"

storage lun modify snapshot host

Description

Creates the hostname of the storage array used as the snapshot host.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} snapshot host <host>

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
<host>	Specify the name of the storage array.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 snapshot host LUN4Edge2
Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx snapshot host hqD6Wo/hWNjx
```

Product

Granite Core

Related Topics

"storage lun modify snapshot clear-host"

storage lun modify storage-group

Description

Specifies the storage group applicable to LUNs in an EMC storage array.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} [failover-peer] storage-group <storage-group>

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
<storage-group>	Specify the name of the storage group.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 snapshot storage-group central

Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx storage-group central
```

Product

Granite Core

Related Topics

"show storage lun"

storage lun modify unmap

Description

Unmaps the specified LUN from the Granite Core appliance.

Syntax

[failover-peer] storage lun modify {alias <alias> | serial <serial>} unmap [force]

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the LUN to be modified by its alias. Alternatively, you can specify the LUN by its serial number.
serial <serial>	Specify the LUN to be modified by its serial number. Alternatively, you can specify the LUN by its alias.
force	Include this parameter to force the unmapping if the LUN is online. Riverbed recommends that you first take the LUN offline before unmapping it. See "storage lun modify offline" on page 858.

Example

```
Core_02 (config) # storage lun modify alias LUN4Edge2 unmap
Core_02 (config) # storage lun modify serial hqD6Wo/hWNjx unmap
```

Product

Granite Core

Related Topics

"storage lun modify offline"

storage lun modify-all scsi-res

Description

Enables or disables SCSI reservations for all configured LUNs.

Syntax

[failover-peer] storage lun modify-all scsi-res {disable | enable}

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
disable	Specify this parameter to disable SCSI reservations.
enable	Specify this parameter to enable SCSI reservations.

Example

```
Core_02 (config) # storage lun modify-all scsi-res enable
```

Product

Granite Core

Related Topics

"Branch Storage Commands"

storage lun remove

Description

Removes the specified LUN from the Granite Core configuration.

Syntax

[failover-peer] storage lun remove {alias <alias> | serial <serial>} [force]

Parameters.

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
alias <alias>	Specify the alias of the LUN to be removed.
serial <serial>	Specify the iSCSI serial number of the LUN to be removed.
force	Include this parameter to force the removal if the LUN is online. Riverbed recommends that you first take the LUN offline before removing it. See "storage lun modify offline" on page 858.

Usage

Prior to removing the LUN from the Granite Core configuration, you must take it offline using "storage lun modify offline" on page 858.

Example

```
Core_02 (config) # storage lun remove alias LUN4Edge2 force
```

Product

Granite Core

Related Topics

"storage lun modify offline"

storage snapshot add host

Description

Specifies the host settings for the Snapshot credential.

Syntax

storage snapshot add host <host> type <type> {username <username> password <password>} [protocol <NetApp protocol>] [port <NetApp port>]

Parameters

host <hostname>	Specify the IP address of the Snapshot credential.
type <type>	Specify one of the following storage systems: • EMC-CLARiiON • Dell-EqualLogic • Amazon-EBS • NetApp **Note:** If you specify NetApp, you must specify protocol and port settings in addition to user name and password.
username <username>	Supply a valid user name for the Snapshot credential.
password <password>	Supply a valid password for the Snapshot credential.
protocol <NetApp protocol>	For NetApp configuration only, specify either HTTP or HTTPS.
port <NetApp port>	For NetApp configuration only, specify the port on the NetApp array.

Usage

Use this command to configure one or more storage arrays for snapshots.

Example

```
Core_02 (config) # storage snapshot add host 10.11.12.13 type EMC-CLARiiON username johndoe password
h00haa
```

Product

Granite Core

Related Topics

"storage block-disk rescan," "storage snapshot host modify," "storage snapshot remove host"

storage snapshot host modify

Description

Modifies the Snapshot credentials for the storage array.

Syntax

storage snapshot host <host> modify {[port <port>] | [protocol <protocol>] | [username <username> password <password>]}

Parameters

host <host>	Specify the IP address of the Snapshot credential whose credentials are to be modified.
port <NetApp port>	For NetApp configuration only, specify a new value for the port on the NetApp array.
protocol <NetApp protocol>	For NetApp configuration only, specify either HTTP or HTTPS.
username <username>	Supply a valid user name for the Snapshot credential.
password <password>	Supply a valid password for the Snapshot credential.

Example

```
Core_02 (config) # storage snapshot host 10.11.12.13 modify username adugas password h00haa
```

Product

Granite Core

Related Topics

"storage snapshot add host," "storage snapshot remove host"

storage snapshot policy add

Description

Adds a new snapshot policy to the configuration of the current appliance.

Syntax

[failover-peer] storage snapshot policy add <policy-name>

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
<policy name>	Specify the name of the new policy.

Example

```
Core_02 (config) # storage snapshot policy add Weekly20130606
```

Product

Granite Core

Related Topics

"Branch Storage Commands"

storage snapshot remove host

Description

Removes the Snapshot credential configuration.

Syntax

storage snapshot remove host <host>

Parameters

host <host>	Specify the IP address of the Snapshot credential configuration to be removed.

Example

```
Core_02 (config) # storage snapshot remove host 10.11.12.13
```

Product

Granite Core

Related Topics

"storage snapshot add host," "storage snapshot host modify"

storage snapshot policy modify add-daily

Description

Adds a daily snapshot schedule to the specified snapshot policy.

Syntax

[failover-peer] storage snapshot policy modify <policy-name> add-daily hour <schedule-hour> {days <schedule-days> | everyday} [max-snap-count <max-count>] [force]

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
<policy name>	Specify the name of the policy to be modified.
hour <schedule-hour>	Specify the time for the snapshot to be taken. Use the format HH:MM:SS.
days <schedule-days>	Specify the day of the week for the snapshot to be taken. Use the first three characters (lowercase) of the English term for the day of the week: for example, **sun**, **mon**, **tue**, and so on.
everyday	Use this parameter to specify daily snapshots.
max-snap-count <max-count>	Specify the maximum number of weekly snapshots to be retained.
force	Include this parameter to force the change (in case the policy is currently assigned).

Example

```
Core_02 (config) # storage snapshot policy modify DailyLUN17 add-daily everyday
```

Product

Granite Core

Related Topics

"storage snapshot policy modify add-hourly," "storage snapshot policy modify add-weekly," "storage snapshot policy remove," "storage snapshot policy rename"

storage snapshot policy modify add-hourly

Description

Adds an hourly snapshot schedule to the specified snapshot policy.

Syntax

[failover-peer] storage snapshot policy modify <policy-name> add-hourly {everyhour | hours <schedule-hours>} [max-snap-count <max-count>] [force]

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
<policy name>	Specify the name of the policy to be modified.
everyhour	Use this parameter to specify hourly snapshots.
hours <schedule-hours>	Specify multiple times, delimited by a comma. Use the format HH:MM:SS.
max-snap-count <max-count>	Specify the maximum number of hourly snapshots to be retained.
force	Include this parameter to force the change (in case the policy is currently assigned).

Example

```
Core_02 (config) # storage snapshot policy modify DailyLUN17 add-daily everyhour
```

Product

Granite Core

Related Topics

"Branch Storage Commands"

storage snapshot policy modify add-weekly

Description

Adds a weekly snapshot schedule to the specified snapshot policy.

Syntax

[failover-peer] storage snapshot policy modify <policy-name> add-weekly hour <schedule-hour> day <schedule-day> [max-snap-count <max-count>] [force]

Parameters

<policy name>	Specify the name of the policy to be modified.
hour <schedule-hour>	Specify the time for the snapshot to be taken. Use the format HH:MM:SS.
day <schedule-day>	Specify the day of the week for the snapshot to be taken. Use the first three characters (lowercase) of the English term for the day of the week: for example, **sun**, **mon**, **tue**, and so on.
max-snap-count <max-count>	Specify the maximum number of weekly snapshots to be retained.
force	Include this parameter to force the change (in case the policy is currently assigned).

Example

```
Core_02 (config) # storage snapshot policy modify WeeklyLUN17 add-weekly 10;00;00 day mon
```

Product

Granite Core

Related Topics

"storage snapshot policy modify add-hourly," "storage snapshot policy modify add-daily," "storage snapshot policy remove," "storage snapshot policy rename"

storage snapshot policy remove

Description

Removes the specified snapshot policy from the configuration of the current appliance.

Syntax

[failover-peer] storage snapshot policy remove <policy-name>

Parameters

<policy name>	Specify the name of the policy to be removed.

Example

```
Core_02 (config) # storage snapshot policy remove Weekly20130606
```

Product

Granite Core

Related Topics

"storage snapshot policy modify add-hourly," "storage snapshot policy modify add-daily," "storage snapshot policy modify add-weekly," "storage snapshot policy rename"

storage snapshot policy rename

Description

Adds a new snapshot policy to the configuration of the current appliance.

Syntax

[failover-peer] storage snapshot policy rename <policy-name> new-name <new-policy-name> [force]

Parameters

[failover-peer]	Optionally, include this parameter to perform the command on an unavailable failover peer of the current appliance. The changed configuration is automatically applied when the appliance returns to service.
<policy name>	Specify the name of the policy to be modified.
<new- policy name>	Specify the new name.
[force]	Include this parameter to force the change (in case the policy is currently assigned).

Example

```
Core_02 (config) # storage snapshot policy reanme Weekly20130606 new-name WeeklyLUNJacob
```

Product

Granite Core

Related Topics

"storage snapshot policy modify add-hourly," "storage snapshot policy modify add-daily," "storage snapshot policy modify add-weekly," "storage snapshot policy remove"

Displaying Granite Core Information

This section describes the **show** commands for displaying Granite Core information.

show device-failover

Description

Displays the failover configuration settings (if any), including failover peer hostname, failover peer port, local state, peer state, self-configuration, peer configuration, and peer interfaces.

Syntax

show device-failover

Usage

Use this command to display the configuration settings for failover.

Example

```
Core_02 > show device-failover
Device failover settings
        Failover peer hostname    : chief-sh2020
        Failover peer port        : 7970
        Local state           : Active (self configuration)
        Peer state          : Active (self configuration)
        Self configuration  : Activated
        Peer configuration  : Activated
        Peer interfaces     : 10.1.10.100
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show edge

Description

Displays detailed information about the Granite Edge devices connected to the current Granite Core.

Syntax

show edge [preferred-if | id <id> | id <id> [blockstore] | id <id> iscsi initiator-group [name <initiator group>]| id <id> iscsi initiators [name <initiator>] | id <id> iscsi targets [name <targetname>]]

Parameters

preferred-if	Displays the preferred interface for Granite Edge connections.
id <id>	Optionally, specify the ID of a Granite Edge device to limit the output to information about that machine.
blockstore	Displays the write reserve and encryption type settings of the block store. You must use this parameter in conjunction with the <id> parameter.
iscsi initiator-group [name <initiator group>]	Displays the details of iSCSI initiator groups, including configuration status and the initiators in the group. Optionally, specify the name of an initiator group (igroup) to limit the output to information about that group. You must use this parameter in conjunction with the <id> parameter.
iscsi initiators [name <initiator>]	Displays the details of iSCSI initiator credentials. Optionally, specify the name of a specify initiator to limit the output to information about that initiator. You must use this parameter in conjunction with the <id> parameter.
iscsi targets [name <targetname>]	Displays the details of iSCSI targets, including description, security-only status, header-digest status, data-digest status, initiator groups, initiator credentials, and network portals. Optionally, specify the name of a specify initiator to limit the output to information about that target. You must use this parameter in conjunction with the <id> parameter.

Usage

Use this command to display configuration details about Granite Edge devices connected to the current Granite Core. The following information is displayed:

- ID of the Granite Edge device
- Configuration status
- IP address
- Connection duration
- Virtual IP address
- Mapped LUNs
- Prepopulation schedule details

Example

```
Core_02 > show edge
Granite-Edge Id: amnesia
  Configuration status:    Ready
  Address:                 Unknown
  Connection duration:     0s

Virtual IP addresses:

Mapped LUNs:
  Serial :                 IET:VIRTUAL-DISK:0001:768

Prepop schedules:
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show failover-peer edge

Description

Displays detailed information about the Granite Edge devices connected to the failover peer configured for the current Granite Core. Use this command to view details about an unavailable Granite Core device though its failover peer.

Syntax

show failover-peer edge [id <id> | blockstore | iscsi initiator-group [name <initiator group>] | iscsi initiators [name <initiator>] | iscsi targets [name <targetname>]]

Parameters

id <id>	Optionally, specify the ID of a Granite Edge device to limit the output to information about that machine.
blockstore	Displays the write reserve and encryption type settings of the block store. **Note:** Must be used in conjunction with the <id> parameter.
iscsi initiator-group [name <initiator group>]	Displays the details of iSCSI initiator groups, including configuration status and the initiators in the group. Optionally, specify the name of an initiator group (igroup) to limit the output to information about that group. **Note:** Must be used in conjunction with the <id> parameter.
iscsi initiators [name <initiator>]	Displays the details of iSCSI initiator credentials. Optionally, specify the name of a specify initiator to limit the output to information about that initiator. **Note:** Must be used in conjunction with the <id> parameter.
iscsi targets [name <targetname>]	Displays the details of iSCSI targets, including description, security-only status, header-digest status, data-digest status, initiator groups, initiator credentials, and network portals. Optionally, specify the name of a specify initiator to limit the output to information about that target. **Note:** Must be used in conjunction with the <id> parameter.

Usage

Use this command to display configuration details about Granite Edge devices connected to the failover peer configured for the current Granite Core. The following information is displayed:

- ID of the Granite Edge device
- Configuration status
- IP address
- Connection duration
- Virtual IP addresses
- Mapped LUNs
- Prepopulation schedule details

Example

```
Core_02 > show failover-peer peer
Granite-Edge Id: amnesia
  Configuration status:    Ready
  Address:                 Unknown
  Connection duration:     0s

Virtual IP addresses:

Mapped LUNs:
  Serial :                 IET:VIRTUAL-DISK:0001:768

Prepop schedules:
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show failover-peer storage iscsi

Description

Displays the details of the specified configuration settings for a Granite Core device via its failover peer: for example, if Core01 is not available, you can display configuration information by running the **show failover-peer storage** commands on its failover peer.

Syntax

show failover-peer storage iscsi {chap [username <name>] | data-digest | disc-luns-all | disc-targets [portal <hostname>] | header-digest | initiators [name <initiator>]| chap [username <name>] | data-digest | disc-luns-all | disc-targets [portal <hostname>] | header-digest | initiator -group [name <igroup>]| lun-alias <lun-alias> | lun-serial <lun-serial> | luns | portals | targets}

Parameters

chap [username <name>]	Optionally, specify a CHAP user by name to display details specific to that user. Displays the CHAP users or details of the specified CHAP user.
data-digest	Indicates whether the data digest is enabled or not.
disc-luns-all	Displays a detailed list of discovered iSCSI LUNs.
disc-targets [portal <hostname>]	Displays a detailed list of discovered iSCSI targets. Optionally, specify the hostname of the portal to display details of that target only.
header-digest	Indicates whether the header digest is enabled or not.
initiator	Displays the iSCSI initiator settings, including name, mutual CHAP configuration (enabled or not), and mutual CHAP user name (if enabled).
lun-alias <lun-alias>	Displays the details of the LUN indicated by the specified alias value, including configuration status, size, type, vendor, serial number, and so on.
lun-serial <lun-serial>	Displays the details of the LUN indicated by the specified serial value, including configuration status, size, type, vendor, serial number, and so on.
luns	Displays the details of all configured LUNs, including configuration status, size, type, vendor, serial number, and so on.
portals	Displays the details of all iSCSI portals, including name, port, and CHAP authentication settings (if applicable).
targets	Display the details of the configured iSCSI target.

Example

```
Core_02 > show failover-peer storage iscsi chap username asdf
CHAP user : asdf
```

```
    Configuration status:    Ready
    Enabled:                 Yes
    Password:                ********
    In Use                   No

Core_02 > show failover-peer storage iscsi lun-alias test
Locally Assigned Serial: hqD9Vo/hRSYU
  Configuration status:    Ready
  Alias:                   test
  LUN size:                101.975 MB
  LUN type:                iscsi
  Origin LUN vendor:       NetApp
  Origin LUN serial:       hqD9Vo/hRSYU
  Online:                  yes
  Pinned:                  no
...
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show failover-peer storage iscsi disc-portals portal

Description

Displays the MPIO portals available on the filer for the specified iSCSI portal configuration.

This command is intended to be used for portals discovered for multi-path I/O (MPIO) configurations. MPIO enables a single iSCSI portal configuration to connect with the filer on multiple IP addresses.

Syntax

show failover-peer storage iscsi disc-portals portal <hostname>

Parameters

<hostname>	Specify the hostname of the iSCSI portal configuration.

Usage

After portals have been discovered, you can add them to the iSCSI portal configuration using the "failover-peer storage iscsi portal host disc-portal add" command.

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 > show failover-peer storage iscsi disc-portals portal 123.45.6.789
```

Product

Granite Core

Related Topics

"failover-peer storage iscsi portal host disc-portal add," "failover-peer storage iscsi portal host disc-portal modify," "failover-peer storage iscsi portal host disc-portal remove," "failover-peer storage iscsi portal host rescan-portals"

show failover-peer storage iscsi mpio interfaces

Description

Displays the interfaces currently configured for MPIO connections.

Syntax

show failover-peer storage iscsi mpio interfaces

Parameters

None

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 > show failover-peer storage iscsi mpio interfaces
Interfaces configured for MPIO
        eth0_2
        eth0_3
```

Product

Granite Core

Related Topics

"show storage iscsi mpio interfaces"

show failover-peer storage iscsi session

Description

Displays the iSCSI session information.

Syntax

show failover-peer storage iscsi session

Parameters

None

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Example

```
Core_02 > show failover-peer storage iscsi session
iSCSI mpio support                    : Enabled
iSCSI mpio standard routing allowed : Disabled
iSCSI3 reservation support          : Enabled
iSCSI2 reservation support          : Enabled
iSCSI2 reservation fallback         : Enabled
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show failover-peer storage snapshot

Description

Displays the snapshot settings.

Syntax

show failover-peer storage snapshot [host <hostname>]

Parameters

<hostname>	Specify the hostname of the storage array.

Example

```
Core_02 > show failover-peer storage snapshot
Storage Array: 10.6.x.x
  Configuration status:    Ready
  Port:                    80
  Type:                    Dell EqualLogic
  Username:                yoga
  Protocol:                HTTP

Storage Array: 10.6.x.x
  Configuration status:    Ready
  Port:                    80
  Type:                    Dell EqualLogic
  Username:                yoga
  Protocol:                HTTP
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats failover-peer storage edge-bytes

Description

Displays process statistics for the specified Granite Edge device for the specified period of time.

Syntax

show stats failover-peer storage edge-bytes {interval <time-interval> edge <edge-self-identifier> | start-time <start> end-time <end> edge <edge-self-identifier>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the edge <edge-self-identifier> parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **edge <edge-self-identifier>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **edge <edge-self-identifier>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
edge <edge-self-identifier>	Specify the self-identifier of the desired Granite Edge.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Use this command to answer the following questions:

- How many megabytes have been written to and read from the specified Granite Edge device for the specified period?
- How many megabytes have been prefetched to the specified Granite Edge device for the specified period?

Example

```
Core_02 > show stats failover-peer storage edge-bytes interval month edge Edge01
Total Data Read: 0 Bytes
Total Data Prefetched: 0 Bytes
Total Data Written: 0 Bytes
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats failover-peer storage filer-bytes

Description

Displays the number of bytes written to and read from the specified SAN for the specified period of time by the failover peer of the current appliance.

Syntax

show stats failover-peer storage filer-bytes {interval <time-interval> filer <hostname> | start-time <start> end-time <end> filer <hostname>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **filer <hostname>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
filer <hostname>	Specify the IP address of the filer portal.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Use this command to display how many megabytes have been written to and read from the specified filer for the specified period.

Example

```
Core_02 > show stats failover-peer storage filer-bytes interval month filer 10.1.x.x
Total Data Read: 512 Bytes
Total Data Written: 0 Bytes
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats failover-peer storage filer-ios

Description

Displays the standard I/O operations per second written to and read from the specified filer for the specified period of time.

Syntax

show stats failover-peer storage filer-ios {interval <time-interval> filer <hostname> | start-time <start> end-time <end> filer <hostname>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **filer <hostname>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
filer <hostname>	Specify the IP address of the filer portal.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Use this command to display how many operations have been written to and read from the specified filer for the specified period.

Example

```
Core_02 > show stats failover-peer storage filer-ios interval month filer 10.1.x.x
Total Read IOs: 1
Total Write IOs: 0
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats failover-peer storage filer-latency

Description

Displays the average read I/O and write I/O times (in milliseconds) for the specified filer for the specified period of time.

Syntax

show stats failover-peer storage filer-latency {interval <time-interval> filer <hostname> | start-time <start> end-time <end> filer <hostname>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **filer <hostname>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
filer <hostname>	Specify the IP address of the filer portal.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Use this command to display the average read and write latencies for the specified filer for the specified period.

Example

```
Core_02 > show stats failover-peer storage filer-latency interval month filer 10.1.x.x
Avg Read IO Time: 0 ms
Avg Write IO Time: 0 ms
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats failover-peer storage lun-bytes

Description

Displays the number of bytes written to and read from the specified LUN for the specified period of time.

Syntax

show stats failover-peer storage lun-bytes {interval <time-interval> lun <lun-id>] | start-time <start> end-time <end> lun <lun-id>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **lun <lun-id>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
lun <lun-id>	Specify the locally assigned serial number of the LUN.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Use this command to display the number of megabytes written to and read from the specified LUN for the specified period.

Example

```
Core_02 > show stats failover-peer storage lun-bytes interval month lun hqD9Vo/susiw
Total Data Prefetched: 0 Bytes
Total Data Read (no-prefetch): 0 Bytes
Total Data Written: 0 Bytes
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats failover-peer storage lun-ios

Description

Displays the standard I/O operations per second written to and read from the specified LUN for the specified period of time.

Syntax

show stats failover-peer storage lun-ios {interval <time-interval> lun <lun-id> | start-time <start> end-time <end> lun <lun-id>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **lun <lun-id>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
lun <lun-id>	Specify the locally assigned serial number of the LUN.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Use this command to display how many operations have been written to and read from the specified LUN for the specified period.

Example

```
Core_02 > show stats failover-peer storage lun-ios interval month lun hqD9Vo/hRSYU
Total Read IOs: 1
Total Write IOs: 0
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats failover-peer storage lun-latency

Description

Displays the average read and write latency for the specified LUN for the specified period of time.

Syntax

show stats failover-peer storage lun-latency {interval <time-interval> lun <lun-id> | start-time <start> end-time <end> lun <lun-id>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **lun <lun-id>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
lun <lun-id>	Specify the locally assigned serial number of the LUN.

Usage

All **failover-peer** commands enable you to configure an unavailable Granite Core device through its failover peer. When the Granite Core device returns to service, the new configuration is added automatically.

Use this command to display the average read and write latencies for the specified LUN for the specified period.

Example

```
Core_02 > show stats failover-peer storage lun-latency interval month lun hqD9Vo/
Avg Read IO Time: 0 ms
Avg Write IO Time: 0 ms
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats storage edge-bytes

Description

Displays connectivity statistics that summarize the standard I/O data traffic read from and written to the specified Granite Edge device for the specified period of time.

Syntax

show stats storage edge-bytes {interval <time-interval> edge <edge-self-identifier> | start-time <start> end-time <end> edge <edge-self-identifier>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **edge <edge-self-identifier>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **edge <edge-self-identifier>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **edge <edge-self-identifier>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
edge <edge-self-identifier>	Specify the self-identifier of the desired Granite Edge.

Usage

Use this command to answer the following questions:

- How many megabytes have been written to and read from the specified Granite Edge device for the specified period?
- How many megabytes have been prefetched to the specified Granite Edge device for the specified period?

Example

```
Core_02 > show stats storage edge-bytes interval month edge Edge01
Total Data Read: 0 Bytes
Total Data Prefetched: 0 Bytes
Total Data Written: 0 Bytes
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats storage filer-bytes

Description

Displays the number of bytes written to and read from the specified SAN (storage area network) for the specified period of time.

Syntax

show stats storage filer-bytes {interval <time-interval> filer <hostname> | start-time <start> end-time <end> filer <hostname>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the filer <hostname> parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
filer <hostname>	Specify the IP address of the filer portal.

Usage

Use this command to display how many megabytes have been written to and read from the specified SAN for the specified period.

Example

```
Core_02 > show stats storage filer-bytes interval month filer 10.1.x.x
Total Data Read: 512 Bytes
Total Data Written: 0 Bytes
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats storage filer-ios

Description

Displays the standard I/O operations per second written to and read from the specified SAN (storage area network) for the specified period of time.

Syntax

show stats storage filer-ios {[interval <time-interval> filer <hostname>] | start-time <start> end-time <end> filer <hostname>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **filer <hostname>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
filer <hostname>	Specify the IP address of the filer portal.

Usage

Use this command to display how many operations have been written to and read from the specified SAN for the specified period.

Example

```
Core_02 > show stats storage filer-ios interval month filer 10.1.x.x
Total Read IOs: 1
Total Write IOs: 0
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats storage filer-latency

Description

Displays the average read I/O and write I/O times (in milliseconds) for the specified SAN (storage area network) for the specified period of time.

Syntax

show stats storage filer-latency {interval <time-interval> filer <hostname> | start-time <start> end-time <end> filer <hostname>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **filer <hostname>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
filer <hostname>	Specify the IP address of the filer portal.

Usage

Use this command to display the average read and write latencies for the specified SAN for the specified period.

Example

```
Core_02 > show stats storage filer-latency interval month filer 10.1.x.x
Avg Read IO Time: 0 ms
Avg Write IO Time: 0 ms
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats storage lun-bytes

Description

Displays the number of bytes written to and read from the specified LUN for the specified period of time.

Syntax

show stats storage lun-bytes {interval <time-interval> lun <lun-id> | start-time <start> end-time <end> lun <lun-id>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **lun <lun-id>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **lun <lun-id>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
lun <lun-id>	Specify the IP address of the filer portal.

Usage

Use this command to display the number of megabytes written to and read from the specified LUN for the specified period.

Example

```
Core_02 > show stats storage lun-bytes interval month lun hqD9Vo/susiw
Total Data Prefetched: 0 Bytes
Total Data Read (no-prefetch): 0 Bytes
Total Data Written: 0 Bytes
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats storage lun-ios

Description

Displays the standard I/O operations per second written to and read from the specified LUN for the specified period of time.

Syntax

show stats storage lun-ios {interval <time-interval> lun <lun-id> | start-time <start> end-time <end> lun <lun-id>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **filer <hostname>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
lun <lun-id>	Specify the locally assigned serial number of the LUN.

Usage

Use this command to display how many operations have been written to and read from the specified LUN for the specified period.

Example

```
Core_02 > show stats storage lun-ios interval month lun hqD9Vo/hRSYU
Total Read IOs: 1
Total Write IOs: 0
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats storage lun-latency

Description

Displays the average read and write latency for the specified LUN for the specified period of time.

Syntax

show stats storage lun-latency {interval <time-interval> lun <lun-id> | start-time <start> end-time <end> lun <lun-id>}

Parameters

interval <time-interval>	Use this parameter in conjunction with the **filer <hostname>** parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** and **filer <hostname>** parameters to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
lun <lun-id>	Specify the locally assigned serial number of the LUN.

Usage

Use this command to display the average read and write latencies for the specified LUN for the specified period.

Example

```
Core_02 > show stats storage lun-latency interval month lun hqD9Vo/
Avg Read IO Time: 0 ms
Avg Write IO Time: 0 ms
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats storage network-bytes

Description

Displays the number of bytes written to and read from the network for the specified period of time.

Syntax

show stats storage network-bytes {interval <time-interval>| start-time <start> end-time <end>}

Parameters

interval <time-interval>	Use this parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the end-time <end> parameter to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the start-time <start> parameter to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.

Usage

Use this command to display the number of bytes written to and read from the network for the specified period.

Example

```
Core_02 > show stats storage network-bytes interval month
Total Data Read: 3 Bytes
Total Data Written: 0 Bytes
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats storage network-ios

Description

Displays the standard I/O operations per second written to and read from the network for the specified period of time.

Syntax

show stats storage network-ios {interval <time-interval>] | start-time <start> end-time <end>}

Parameters

interval <time-interval>	Use this parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.

Usage

Use this command to display the average network read and write latencies for the specified period.

Example

```
Core_02 > show stats storage network-ios interval month
Total Read IOs: 3
Total Write IOs: 0
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show stats storage network-latency

Description

Displays the average network read I/O and write I/O times (in milliseconds) for the specified period of time.

Syntax

show stats storage network-latency {interval <time-interval> | start-time <start> end-time <end>}

Parameters

interval <time-interval>	Use this parameter to return statistics for one of the following time intervals: • **1min** - Returns statistics for the last one minute. • **5min** - Returns statistics for the last five minutes. • **hour** - Returns statistics for the last one hour. • **day** - Returns statistics for the last one day. • **week** - Returns statistics for the last one week. • **month** - Returns statistics for the last one month.
start-time <start>	Use this parameter in conjunction with the **end-time <end>** to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.
end-time <end>	Use this parameter in conjunction with the **start-time <start>** to return statistics for the specified time period. Use the format YYYY/MM/DD HH:MM:SS.

Usage

Use this command to display the average network read and write latencies for the specified period.

Example

```
Core_02 > show stats storage network-latency interval month
Avg Read IO Time: 0 ms
Avg Write IO Time: 0 ms
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show storage host-info

Description

Displays the host, username, type, and port configuration for application-consistent snapshots and data protection.

Syntax

show [failover-peer] storage host-info [host <hostname>]

Parameters

[failover-peer]	Include this parameter to perform this command on the failover peer of the current appliance.
host <hostname>	Optionally, specify a hostname to limit the output to that host.

Example

```
Core_02 > show storage host-info host dc
  Host:             dc
  Username:         s
  Type:             vmware_proxy
  Port:             443
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show storage iscsi

Description

Displays the details of the storage iSCSI settings.

Syntax

show storage iscsi {chap [username <name>] | data-digest | disc-luns-all | disc-targets [portal <hostname>] | header-digest | initiators [name <initiator>]| chap [username <name>] | data-digest | disc-luns-all | disc-targets [portal <hostname>] | header-digest | initiator -group [name <igroup>]| lun-alias <lun-alias> | lun-serial <lun-serial> | luns | portals | targets}

Parameters

chap [username <name>]	Specify a CHAP user by name to view the details only that user. Displays the CHAP users or details of the specified CHAP user.
data-digest	Indicates whether the data digest is enabled or not.
disc-luns-all	Displays detailed list of discovered iSCSI LUN.
disc-targets [portal <hostname>]	Displays detailed list of discovered iSCSI targets. Optionally, specify the hostname of the portal to display details of that target only.
header-digest	Indicates whether the header digest is enabled or not.
initiators [name <initiator>]	Displays the iSCSI initiator settings, including name, mutual CHAP configuration (enabled or not), and mutual CHAP user name (if enabled). Optionally, specify the name of an initiator to view details about only that initiator.
initiator-group [name <igroup>]	Displays the iSCSI initiator groups. Optionally, specify the name of an initiator group to view more details about only that initiator group.
lun-alias <lun-alias>	Displays the details of the LUN indicated by the specified alias value, including configuration status, size, type, vendor, serial number, and so on.
lun-serial <lun-serial>	Displays the details of the LUN indicated by the specified serial value, including configuration status, size, type, vendor, serial number, and so on.
luns	Displays the details of all configured LUNs, including configuration status, size, type, vendor, serial number, and so on.
portals	Displays the details of all iSCSI portals, including name, port, and CHAP authentication settings (if applicable).
targets	Display the details of the configured iSCSI target.

Example

```
Core_02 > show storage iscsi chap username asdf
CHAP user : asdf
    Configuration status:    Ready
    Enabled:                 Yes
    Password:                ********
    In Use                   No

Core_02 > show storage iscsi lun-alias test
Locally Assigned Serial: hqD9Vo/hRSYU
  Configuration status:    Ready
  Alias:                     test
  LUN size:                  101.975 MB
  LUN type:                  iscsi
  Origin LUN vendor:         NetApp
  Origin LUN serial:         hqD9Vo/hRSYU
  Online:                    yes
  Pinned:                    no
...
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show storage iscsi disc-portals portal

Description

Displays the interfaces available on the filer for the specified iSCSI portal configuration.

This command is intended to be used for portals discovered for Multi-Path I/O (MPIO) configurations. MPIO enables a single iSCSI portal configuration to connect with the filer on multiple IP addresses.

Syntax

show storage iscsi disc-portals portal <hostname>

Parameters

<hostname>	Specify the hostname of the iSCSI portal configuration.

Parameters

Usage

After portals have been discovered, you can add them to the iSCSI portal configuration using the "storage iscsi portal host disc-portal add" command.

Example

```
Core_02 > show storage iscsi disc-portals portal 123.45.6.789
```

Product

Granite Core

Related Topics

"storage iscsi portal host disc-portal add," "storage iscsi portal host disc-portal modify," "storage iscsi portal host disc-portal remove," "storage iscsi portal host rescan-portals"

show storage iscsi mpio interfaces

Description

Displays the interfaces currently configured for MPIO connections.

Syntax

show storage iscsi mpio interfaces

Parameters

None

Example

```
Core_02 > show storage iscsi mpio interfaces
Interfaces configured for MPIO
        eth0_2
        eth0_3
```

Product

Granite Core

Related Topics

"show failover-peer storage iscsi mpio interfaces"

show storage lun

Description

Displays the details of the storage LUN settings.

Syntax

show [failover-peer] storage lun {alias <alias> | serial <serial>} [snapshot-config]

Parameters

[failover-peer]	Include this parameter to perform this command on the failover peer of the current appliance.
alias <alias>	Specify the alias of the LUN to be displayed.
serial <serial>	Specify the serial value of the LUN to be displayed.
[snapshot-config]	Optionally, displays snapshot configuration details.

Example

```
Core_02 > show storage lun alias yoga_iscsi
Locally Assigned Serial: hoiqdoX\/xxxx
  Configuration status           : Ready
  Alias                          : xxxx_iscsi
  LUN Size                       : 1.00351 GB
  LUN Type                       : iscsi
  Online                         : yes
  Failover Enabled               : yes
  Prefetch                       : Enabled
  Edge mapping                   : gen1-sh15
  Target mapping                 : iqn.2003-10.com.xxxxxxxxx.000
 ...
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show storage luns

Description

Displays details about all the LUNs configured for the current appliance, including:

- Configuration status
- LUN size and type
- Prefetch setting

- Mapped edge appliances
- Target and portal mapping
- Session status
- Prepopulation settings, status, progress, and schedules
- Snapshot settings and schedules
- MPIO policy settings

Syntax

show [failover-peer] storage luns [block-disk | edge-local | iscsi | discovered {block-disk | iscsi}]

Parameters

[failover-peer]	Include this parameter to perform this command on the failover peer of the current appliance.
[block-disk]	Specify this parameter to limit the output to block-disk LUNs.
[edge-local]	Specify this parameter to limit the output to local edge LUNs.
[iscsi]	Specify this parameter to limit the output to iSCSI LUNs.
[discovered {block-disk | iscsi}	Specify this parameter to limit the output to discovered LUNs of the specified type.

Example

```
Core_02 > show storage luns iscsi
Locally Assigned Serial: P3KRP4l4Q4m6
  Configuration status             : Ready
  Alias                            : snapLun
  LUN Size                         : 101.975 MB
  LUN Type                         : iscsi
  Online                           : yes
  Failover Enabled                 : yes
  Prefetch                         : Enabled
...
```

Product

Granite Core

Related Topics

"Granite Core Commands"

show storage lun-global settings

Description

Displays the settings that are applicable to all LUNs.

Syntax

show [failover-peer] storage lun-global settings

Parameters

[failover-peer]	Include this parameter to perform this command on the failover peer of the current appliance.

Example

```
Core_02 > show storage lun-global settings
iSCSI reservations              : Enabled
Minimum local lun size          : 8 MBs
```

Product

Granite Core

Related Topics

“Granite Core Commands”

show storage policies

Description

Displays details about all currently configured snapshot schedule policies.

Syntax

show [failover-peer] storage policies

Parameters

[failover-peer]	Include this parameter to perform this command on the failover peer of the current appliance.

Example

```
Core_02 (config) # show storage policies
Snapshot Schedule Policy : default_policy
  Max Hourly Snaps               : 5
  Max Daily Snaps                : 5
  Max Weekly Snaps               : 5
  Schedule :
             hourly              : everyday  @  everyhour


Snapshot Schedule Policy : default_schedule_policy
  Max Hourly Snaps               : 5
  Max Daily Snaps                : 5
  Max Weekly Snaps               : 5
  Schedule :
             hourly              : everyday  @  everyhour


Snapshot Schedule Policy : test_yoga
  Max Hourly Snaps               : 5
  Max Daily Snaps                : 5
  Max Weekly Snaps               : 5
```

Product

Granite Core

Related Topics

“Granite Core Commands”

show storage snapshot

Description

Displays the storage snapshot headings.

Syntax

show storage snapshot [host <hostname>]

Parameters

[host <hostname>]	Optionally, specify a host to limit the results.

Example

```
Core_02 > show storage snapshot
```

Product

Granite Core

Related Topics

"Granite Core Commands"

Interceptor Appliance Feature Commands

This section describes commands you use to configure Interceptor appliance features. Riverbed recommends that you use the Interceptor Management Console to configure the Interceptor appliance. For details, see the *Interceptor Appliance User's Guide* and the *Interceptor Appliance Deployment Guide*.

Important: You must also set up the host and networking configuration, configure in-path interfaces, and configure in-path rules for deployments that use the Interceptor appliance for load-balancing. These commands are common to the Steelhead appliance and Interceptor appliance. For detailed information, see the previous sections of this chapter.

Interceptor System Commands

This section describes the Interceptor system commands.

Note: For hardware-assist rule commands, see "Hardware-Assist Rule Commands" on page 745.

xbridge enable

Description

Enables the Xbridge feature.

Syntax

[no] xbridge enable

Parameters

None

Usage

Xbridge is a software-packet-processing enhancement supported on Interceptor appliances that use 10-Gbps interfaces. The Xbridge feature provides significant line-throughput performance improvement for optimized and pass-through traffic for 10G interfaces on an Interceptor appliance.

Example

```
amnesiac (config) # xbridge enable
```

Product

Interceptor appliance

Related Topics

"show xbridge"

Interceptor Failover Support Commands

This section describes the Interceptor failover support commands.

failover interceptor name additional-ip

Description

Configures an additional IP address for the failover Interceptor appliance.

Syntax

[no] failover interceptor name <name> additional-ip <ip-addr>

Parameters

<name>	Specify the hostname of the failover Interceptor appliance.
<ip-addr>	Specify an additional forwarding IP address of the failover Interceptor appliance.

Usage

For detailed information about configuring the failover Interceptor process, see the *Interceptor Appliance Deployment Guide*.

The **no** command option disables the failover Interceptor appliance process.

The **failover interceptor name additional-ip** command replaces the **failover buddy name additional-ip** command.

Example

```
amnesiac (config) # failover interceptor name test additional-ip 10.0.0.2
```

Product

Interceptor appliance

Related Topics

"show failover interceptor"

failover interceptor name main-ip

Description

Configures the main IP address for the failover Interceptor appliance.

Syntax

[no] failover interceptor name <name> main-ip <ip-addr>

Parameters

<name>	Specify the hostname of the failover Interceptor appliance.
<ip-addr>	Specify the main connection forwarding IP address of the failover Interceptor appliance.

Usage

For detailed information about configuring the failover Interceptor process, see the *Interceptor Appliance Deployment Guide*.

The **no** command option disables the failover Interceptor appliance process.

The **failover interceptor name main-ip** command replaces the **failover buddy name main-ip** command.

Example

```
amnesiac (config) # failover interceptor name headquarters main-ip 10.0.0.1
```

Product

Interceptor appliance

Related Topics

"show failover interceptor"

Load-Balancing Commands

This section describes the load-balancing commands.

load balance default-rule fair-peering

Description

Enables fair-peering on the default rule.

Syntax

load balance default-rule fair-peering

Parameters

None

Usage

When the Fair Peering feature is enabled for a load balancing rule, the target Steelhead appliance cannot exceed a dynamically determined maximum number of remote peers. When that maximum is reached, peer connections are reassigned. For example, when the maximum limit for one local Steelhead appliance is reached, the load shifts to another local Steelhead appliance

Example

```
amnesiac (config) # load balance default-rule fair-peering
```

Product

Interceptor appliance

Related Topics

"show load balance rules"

load balance fair-peer-v2 enable

Description

Enables fair-peering version 2.

Syntax

load balance fair-peer-v2 enable

Parameters

None

Usage

Fair peering version 2 overrides per rule fair peering when enabled.

Example

```
amnesiac (config) # load balance fair-peer-v2 enable
```

Product

Interceptor appliance

Related Topics

"show load balance rules"

load balance fair-peer-v2 threshold

Description

Configures the peer threshold percentage.

Syntax

load balance fair-peer-v2 threshold <percentage>

Parameters

<percentage>	Specify the threshold percentage. The default percentage is 15.

Usage

Use this command to manually specify the threshold percentage.

Example

```
amnesiac (config) # load balance fair-peer-v2 threshold 20
```

Product

Interceptor appliance

Related Topics

"show load balance rules"

load balance move-rule

Description

Moves the order of the rule in the rule list to the specified number.

Syntax

load balance move-rule rulenum <rulenum> to <rulenum>

Parameters

rulenum <rulenum> to <rulenum>	Specify the rule number to be moved and where to move it.

Example

```
amnesiac (config) # load balance move-rule rulenum 9 to 5
```

Product

Interceptor appliance

Related Topics

"show load balance rules"

load balance rule edit rulenum

Description

Edits a hardware assist rule.

Syntax

load balance rule edit rulenum <rulenum> description <"description">

Parameters

<rulenum>	Specify the rule number to edit.
description <description>	Specify a description for the rule. The description must be in double-quotes.

Example

```
amnesiac (config) # load balance rule edit rulenum 9 description "this is a test"
```

Product

Interceptor appliance

Related Topics

"show load balance rules"

load balance rule pass

Description

Creates load balancing pass-through rule.

Syntax

load balance rule pass [src <subnet>/<mask>][dest <subnet>/<mask> dest-port <port>] | [description <string>] | [peer <ip-addr> {any | probe-only| non-probe}] | [rulenum <rulenum>] | | [vlan <vlan number>]

Parameters

dest <subnet>/<mask>	Specify the IP address for the destination subnet. Use the following format:XXX.XXX.XXX.XXX/XX
dest-port <port>	Specify the destination port number or port label.
description <string>	Specify a description of the rule.
peer <ip-addr> {any | probe-only | non-probe}	Specify the peer IP address to apply pass-through load-balancing rules to this IP address only. Optionally, specify one of the following pass-through load-balancing peer options: • **any** - Applies the pass-through rule to any SYN packet and probe. • **probe-only** - Applies the pass-through rule to any probes from any router. • **non-probe** - Applies the pass-through rule to any SYN packet without a probe.
rulenum <rulenum>	Specify the rule number to insert the pass-through load-balancing rule before.
src <subnet>/<mask>	Specify the IP address for the source network. Use the following format: XXX.XXX.XXX.XXX/XX
vlan <vlan-number>	Specify the VLAN tag Identification Number (ID).

Usage

Configure rules of this type as a second-preference rule for cases where you would like to optimize when connections are available on specified targets, but, in the event targets have reached Admission Control capacity, you would rather pass-through than tax the auto-balance pool. For example, you might use pass-through rules to handle HTTP traffic on port 80.

Load-balancing rules define the characteristics by which traffic is selected for load balancing and the availability of LAN-side Steelhead appliance for such traffic.

Typically, your rules list should:

- Account for traffic over all subnets and ports that have been selected for redirection.
- Account for all Steelhead appliances you have configured as neighbor peers to be targets of redirect rules or reserved for the automatic load-balancing rule.
- If a neighbor Steelhead appliance is specified as a target for a rule, it is reserved for traffic that matches that rule and is not available to the pool used for automatic load-balancing.
- If a neighbor Steelhead appliance is not specified as a target for a rule, it is available for automatic load balancing.
- Account for second-preference cases where you would rather pass-through traffic than tax the autoload-balancing pool.

The Interceptor appliance processes load-balancing rules as follows:

1. Redirect rule matches and the target Steelhead appliance is available: Redirect to a target appliance according to the load balancing algorithm.
2. Redirect rule matches but none of the target Steelhead appliances for the rules are available: Consults the next rule in list.
3. Pass-through rule matches: Pass-through, traversing Riverbed routes but unoptimized.
4. Redirect rule matches but no capacity and it does not match a pass-through rule: Automatically balances load among neighbor Steelhead appliances not reserved by other rules.
5. No rules match or no rules specified, target Steelhead appliances are chosen based on the following rules:
   - **Peer Affinity** - Prefers a target Steelhead appliance that has had a previous connection with the source Steelhead appliance.
   - **Least Connections** - If more than one target Steelhead appliance has peer affinity, the connection is redirected to one that has the least current connections.
   - **No Peer Affinity** - If no Steelhead appliance has peer affinity, the connection is redirected to the Steelhead appliance with the least current connections.

Example

```
amnesiac (config) # load balance rule pass src 10.0.0.1/16 dest 10.0.0.2/16 dest-port 1240 rulenum
3 description test vlan 12
```

Product

Interceptor appliance

Related Topics

"show load balance rules"

load balance rule redirect

Description

Creates load balancing redirect rules.

Syntax

load balance rule redirect [addrs <ip-addr>] | [src <subnet>/<mask>] | [dest <subnet>/<mask> dest-port <port>] | [peer <ip-addr> {any | probe-only | non-probe}] | [[rulenum <rulenum>] | [description <string>] | [vlan <vlan number>] | [fair-peering yes | no]

Parameters

addrs <ip-addr>	Specify a comma-separated list of Steelhead appliance IP addresses to which traffic can be redirected. (Specify the IP address for the Steelhead inpath0_0 interface.) If a rule matches, connections are redirected to a Steelhead appliance in the list according to the load balancing algorithm. This parameter is not required for rules of type pass. You must also configure Interceptor-to-Steelhead appliance communication and Steelhead appliance-to-Interceptor communication for peering between appliances. For detailed information, see "steelhead communication interface" on page 923.
src <subnet>/<mask>	Specify the IP address for the source network. Use the following format: XXX.XXX.XXX.XXX/XX.
dest <subnet>/<mask>	Specify the IP address for the destination network. Use the following format: XXX.XXX.XXX.XXX/XX.
dest-port <port>	Specify a port number or port label.
peer <ip-addr> {any | probe-only | non-probe}	Specify the peer IP address to apply pass-through load-balancing rules to this IP address only. Optionally, specify one of the following pass-through load-balancing peer options: • **any** - Applies the pass-through rule to any SYN packet and probe. • **probe-only** - Applies the pass-through rule to any probes from any router. • **non-probe** - Applies the pass-through rule to any SYN packet without a probe.
rulenum <rulenum>	Specify the rule number. The rule is inserted before the existing pass-through load-balancing rule.
description <string>	Specify a description of the rule.
vlan <vlan-number>	Specify the VLAN tag Identification Number (ID).
fair-peering yes | no	Specify to use fair peering for the load balanced rule.

Usage

Load-balancing rules define the characteristics by which traffic is selected for load balancing and the availability of LAN-side Steelhead appliance for such traffic.

Typically, your rules list should:

- Account for traffic over all subnets and ports that have been selected for redirection.
- Account for all Steelhead appliances you have configured as neighbor peers to be targets of redirect rules or reserved for the automatic load-balancing rule.
- If a neighbor Steelhead appliance is specified as a target for a rule, it is reserved for traffic that matches that rule and is not available to the pool used for automatic load-balancing.
- If a neighbor Steelhead appliance is not specified as a target for a rule, it is available for automatic load balancing.
- Account for second-preference cases where you would rather pass-through traffic than tax the autoload-balancing pool.

The Interceptor appliance processes load-balancing rules as follows:

1. Redirect rule matches and target Steelhead appliance available: Redirect to a target appliance according to the load balancing algorithm.
2. Redirect rule matches but none of the target Steelhead appliances for the rules are available: Consults the next rule in list.
3. Pass-through rule matches: Pass-through, traversing Riverbed routes but unoptimized.
4. Redirect rule matches but no capacity and does not match a pass-through rule: Automatically balances load among neighbor Steelhead appliances not reserved by other rules.
5. No rules match or no rules specified, target Steelhead appliances are chosen based on the following rules:
   - **Peer Affinity** - Prefers a target Steelhead appliance that has had a previous connection with the source Steelhead appliance. If no Steelhead appliance has peer affinity, the connection is redirected to the Steelhead appliance with the least current connections.
   - **Least Connections** - If more than one target Steelhead appliance has peer affinity, the connection is redirected to one that has the least current connections.
   - **No Peer Affinity** - If no Steelhead appliance has peer affinity, the connection is redirected to the Steelhead appliance with the least current connections.

Example

```
amnesiac (config) # load balance rule redirect addrs 10.0.0.1,10.0.0.2 src 10.0.0.1/16 dest
10.0.0.2/16 dest-port 1240 description test vlan 12
```

Product

Interceptor appliance

Related Topics

"show load balance rules"

Interceptor Peering and Redirect Commands

This section describes the Interceptor peering and redirect commands.

conn-trace rule

Description

Configures connection tracing rules.

Syntax

[no] conn-trace rule srcnet <subnet> srcport-start <startport> srcport-end <endport> dstnet <dst ip-addr> dstport-start <startport> dstport-end <endport>

Parameters

srcnet <subnet>	Specify an IP address and mask for the traffic source. Use the format XXX.XXX.XXX.XXX/ XX. You can specify all or 0.0.0.0/0 as the wildcard for all traffic.
srcport-start <port>	Specify the start port for the traffic source.
srcport-end <endport>	Specify the end port for the traffic source.
dstnet <dst ip-addr>	Specify an IP address and mask for the traffic destination. Use the format: XXX.XXX.XXX.XXX/XX. You can specify all or 0.0.0.0/0 as the wildcard for all traffic.
dstport-start <startport>	Specify the start port for the traffic destination.
dstport-end <endport>	Specify the end port for the destination.

Usage

Connection traces enable you to determine to which Steelhead appliances the Interceptor appliance has redirected specific connections. Connection traces also enable users to debug failing or unoptimized connections.

Note: If you manually restart the Interceptor appliance, the connection traces are lost. Prior to restarting, perform a system dump using the **disable** command.

The **no** command option disables the connection tracing.

Example

```
amnesiac (config) # conn-trace rule srcnet 10.0.0.1 srcport-start 1234 srcport-end 4567 dstnet
10.0.0.2 dstport-start 7890 dstport-end 8890
```

Product

Interceptor appliance

Related Topics

"show conn-trace"

interceptor communication allow-failure enable

Description

Allows failure in active-passive Interceptor appliance deployments.

Syntax

[no] interceptor communication allow-failure enable

Parameters

None

Usage

Run this command on all Interceptor appliances on the active and passive links. You must also run the **steelhead communication allow-failure** command on all Steelhead appliances that point to the Interceptor appliances on which you ran this command.

The **interceptor communication allow-failure enable** command replaces the **redirect allow-failure** command.

The **no** command option disables the command.

Example

```
amnesiac (config) # interceptor communication allow-failure enable
```

Product

Interceptor appliance

Related Topics

"show interceptor communication"

interceptor communication interface

Description

Configures the Interceptor interface.

Syntax

interceptor communication interface <interface>

Parameters

<interface>	Specify the name of the interface the appliance uses to communicate with peer Interceptor appliances.

Usage

Your selection must be implemented system-wide. For example, if you decide for Interceptor A to use inpath0_0, you must specify inpath0_0 when you run this command on Interceptor B and any other Interceptor appliance in your deployment.

The **interceptor communication interface** command replaces the **redirect interface** command.

Example

```
amnesiac (config) # interceptor communication interface inpath0_0
You must restart the service for your changes to take effect.
amnesiac (config) # service restart
```

Product

Interceptor appliance

Related Topics

"show steelhead name all"

interceptor communication multi-interface enable

Description

Enables the neighbor multiple interface support.

Syntax

interceptor communication multi-interface enable

Parameters

None

Usage

The **interceptor communication multi-interface enable** command replaces the **redirect multi-interface enable** command.

Example

```
amnesiac (config) # interceptor communication multi-interface enable
```

Product

Interceptor appliance

Related Topics

"show interceptor communication," "show steelhead name all"

interceptor name

Description

Configures an Interceptor peer.

Syntax

interceptor name <host> {additional-ip <ip-addr> | main-ip <ip-addr> [port <port>] | port <port>}

Parameters

<host>	Specify the hostname for a peer Interceptor appliance in-path interface. This is the interface you set when you run the **interceptor communication interface** command on the peer Interceptor appliance.
additional-ip <ip-addr>	Specify an additional IP address for the peer Interceptor appliance.
main-ip <ip-addr>	Specify the main IP address of the peer Interceptor appliance.
port <port>	Specify the corresponding port for the peer Interceptor appliance. The default port is 7860.

Usage

The **interceptor name** command replaces the **redirect peer name** command.

The **no** command option disables the connection to the peer Interceptor appliance.

Assume you want to configure peering between Interceptor A (with primary interface 10.10.10.1. inpath0_0 interface 10.10.10.2, inpath0_1 interface 10.10.10.3) and Interceptor B (with primary interface 10.10.10.11, inpath0_0 10.10.10.12, inpath0_1 interface 10.10.10.13).

1. Log into the CLI for Interceptor A.
2. Specify which in-path interface on Interceptor A to use for Interceptor-to-Interceptor peering:

```
interceptor communication interface inpath0_0
```

3. Add Interceptor B as a peer by specifying the IP address for the Interceptor B inpath0_0 interface:

```
interceptor name interceptB main-ip 10.10.10.12
```

4. Next, log into the CLI for Interceptor B.
5. Specify the Interceptor B interface to use for Interceptor-to-Interceptor peering:

```
interceptor communication interface inpath0_0
```

6. Add Interceptor A as a peer by specifying the IP address for the Interceptor A inpath0_0 interface:

```
interceptor name interceptA main-ip 10.10.10.2
```

The **interceptor name** command replaces the **redirect peer name** command.

Example

```
amnesiac (config) # interceptor name mypeer main-ip 10.10.10.1
```

Product

Interceptor appliance

Related Topics

"show interceptor communication," "show steelhead name all"

steelhead communication ack-timer-cnt

Description

Sets the number of intervals to wait for an acknowledgement (ACK).

Syntax

[no] steelhead communication ack-timer-cnt <integer>

Parameters

<integer>	Specify the number of intervals.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication ack-timer-cnt 5
```

Product

Interceptor appliance

Related Topics

"show steelhead communication"

steelhead communication ack-timer-intvl

Description

Sets the length of time to wait for an acknowledgement (ACK).

Syntax

[no] steelhead communication ack-timer-intvl

Parameters

<milliseconds>	Specify the length of the interval in milliseconds. The default value is 1000 milliseconds.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication ack-timer-intvl 1500
```

Product

Interceptor appliance

Related Topics

"show steelhead communication"

steelhead communication heartbeat enable

Description

Configures Steelhead communication heartbeat settings.

Syntax

[no] steelhead communication heartbeat enable

Parameters

None

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication heartbeat enable
```

Product

Interceptor appliance

Related Topics

"show steelhead communication"

steelhead communication interface

Description

Sets the interface to use for Interceptor-to-Steelhead communication.

Syntax

steelhead communication interface <interfacename>

Parameters

<interfacename>	Specify the interface name.

Usage

The **steelhead communication interface** command replaces the **in-path neighbor interface** command.

Important: Make sure you configure the Steelhead appliance to communicate with this Interceptor appliance on this interface when you configure Steelhead-to-Interceptor communication.

Assume you want to configure peering between Interceptor A (with primary interface 10.10.10.1. inpath0_0 interface 10.10.10.2, inpath0_1 interface 10.10.10.3) and Steelhead Z (with primary interface 10.10.10.21, inpath0_0 10.10.10.22, inpath0_1 interface 10.10.10.**23**).

1. Log into the CLI for Interceptor A.
2. Specify which in-path interface on Interceptor A to use for Interceptor-to-Steelhead peering:

   ```
   steelhead communication interface inpath0_0
   ```

3. Add Steelhead Z as a peer by specifying the name and IP address for the Steelhead Z inpath0_0 interface:

   ```
   steelhead name shaZ main-ip 10.10.10.22
   ```

4. Log in to the CLI for Steelhead Z.
5. Enable the in-path interface:

   ```
   in-path enable
   ```

6. Enable the out-of-path support:

   ```
   in-path oop enable
   ```

7. Enable peering:

   ```
   in-path neighbor enable
   ```

8. Specify the neighbor name and main IP address:

```
   in-path neighbor name interceptA main-ip 10.10.10.2
```

The **no** command option disables the interface.

Example

```
amnesiac (config) # steelhead communication interface inpath0_0
```

Product

Interceptor appliance

Related Topics

“show steelhead communication”

steelhead communication multi-interface enable

Description

Enables the Steelhead communication multiple interface support.

Syntax

[no] steelhead communication multi-interface enable

Parameters

None

Usage

When using more than one data connection on the Steelhead appliance, you must enable multiple interface support. If you enable multiple interface support, the following constraints apply:

- v5.0x Steelhead appliances must be running RiOS v5.0.7 or higher.
- v5.5.x Steelhead appliances must be running RiOS v5.5.2 or higher.
- Load balancing rules apply only to the main IP address.

The **no** command option disables multiple interface support.

The **steelhead communication multi-interface enable** command replaces the **in-path neighbor multi-interface enable** command.

Example

```
amnesiac (config) # steelhead communication multi-interface enable
```

Product

Interceptor appliance

Related Topics

“show steelhead communication”

steelhead communication read-timeout

Description

Sets the response wait time.

Syntax

[no] steelhead communication read-timeout <milliseconds>

Parameters

<milliseconds>	Specify the length of the interval in milliseconds. The default value is 10,000 milliseconds.

Usage

The **no** command option disables this option.

Example

```
amnesiac (config) # steelhead communication read-timeout 5000
```

Product

Interceptor appliance

Related Topics

"show steelhead communication"

steelhead communication recon-timeout

Description

Sets the time period to wait for a reconnect response.

Syntax

[no] steelhead communication recon-timeout <milliseconds>

Parameters

<milliseconds>	Specify the length of the interval in milliseconds. The default value is 10,000 milliseconds.

Usage

The **no** command option disables this option.

Example

```
amnesiac (config) # steelhead communication recon-timeout 5000
```

Product

Interceptor appliance

Related Topics

"show steelhead communication"

steelhead name (Interceptor)

Description

Configures Interceptor-to-Steelhead peering communication.

Syntax

[no] steelhead name <hostname> {additional-ip <ip-addr> | main-ip <ip-addr> [port <port> | paused] | port <port> | reset cap-reduction {all | perm}}

Parameters

<hostname>	Specify the hostname of the Steelhead neighbor peer.
additional-ip<ip-addr>	Optionally, specify an additional IP address for the neighbors.
main-ip<ip-addr>	Specify the main IP address of the neighbor in-path X_X interface.
port<port>	Specify a port number for communication with the neighbor.
paused	Puts the Steelhead neighbor receiving the main connection forwarding into pause mode.
reset cap-reduction {all | perm}	Resets capacity reduction. Specify one of the following: • Resets all capacity reduction. • Resets permanent capacity reduction.

Usage

The **steelhead name** command replaces the **in-path neighbor peer name** command.

Pressure monitoring measures the burden on Steelhead resources, such as CPU, memory, and number of connections. Capacity reduction is an Interceptor appliance strategy for relieving or avoiding pressure.

For detailed information about configuring connection forwarding, see the *Steelhead Appliance Deployment Guide*.

The **no** command option disables the name settings.

Example

```
amnesiac (config) # steelhead name test main-ip 10.0.0.1 port 1234
```

Product

Interceptor appliance

Related Topics

"show steelhead communication," "show steelhead name all"

steelhead name paused

Description

Pauses the neighbor Steelhead appliance.

Syntax

[no] steelhead name <hostname> paused

Parameters

<hostname>	Specify the hostname of the neighbor peer.

Example

```
amnesiac (config) # steelhead name mypeer paused
```

Product

Interceptor appliance

Related Topics

"show steelhead name all"

steelhead pressure-mon enable

Description

Enables neighbor pressure monitoring.

Syntax

steelhead pressure-mon enable

Parameters

None

Usage

Pressure monitoring measures the burden on Steelhead resources, such as CPU, memory, and number of connections. Pressure monitoring does not apply to a paused Steelhead appliance.

Example

```
amnesiac (config) # steelhead pressure-mon enable
```

Product

Interceptor appliance

Related Topics

"show steelhead communication"

steelhead pressure-mon cap-reduction enable

Description

Enables neighbor pressure monitoring capacity reduction.

Syntax

steelhead pressure-mon cap-reduction enable

Parameters

None

Usage

You must first enable pressure monitoring with the "steelhead pressure-mon enable" command. Capacity reduction does not apply to a paused Steelhead appliance.

Example

```
amnesiac (config) # steelhead pressure-mon cap-reduction enable
```

Product

Interceptor appliance

Related Topics

"show steelhead communication"

steelhead pressure-mon perm cap-reduction enable

Description

Enables permanent neighbor pressure monitoring capacity reduction.

Syntax

steelhead pressure-mon perm cap-reduction enable

Parameters

None

Usage

You must first enable pressure monitoring with the "steelhead pressure-mon enable" command. Capacity reduction does not apply to a paused Steelhead appliance.

Example

```
amnesiac (config) # steelhead pressure-mon perm cap-reduction enable
```

Product

Interceptor appliance

Related Topics

"show steelhead communication"

steelhead pressure-mon perm cap-reduction events

Description

Configures number of events on which to impose permanent pressure monitoring capacity reduction.

Syntax

steelhead pressure-mon perm cap-reduction events <number> time <seconds>

Parameters

<number>	Specify the number of events.
<seconds>	Specify the time in seconds

Usage

You must first enable pressure monitoring with the "steelhead pressure-mon enable" command. Capacity reduction does not apply to a paused Steelhead appliance.

Example

```
amnesiac (config) # steelhead pressure-mon perm cap-reduction events 3 time 10
```

Product

Interceptor appliance

Related Topics

"show steelhead communication"

Configuring Load Balancing In-Path Pass-Through Rules

This section describes the commands for configuring in-path pass-through rules for load-balancing.

in-path passthrough move-rule

Description

Moves an in-path pass-through rule.

Syntax

in-path passthrough move-rule rulenum <rulenum> to <rulenum>

Parameters

<rulenum>	Specify the rule number.

Usage

Moves pass-through connection rules so that they can be optimized.

Example

```
amnesiac (config) # in-path passthrough move-rule 2 to 4
```

Product

Interceptor appliance

Related Topics

"show in-path passthrough rules"

in-path passthrough rule allow

Description

Configures an in-path load balancing rule that allows pass-through traffic.

Syntax

in-path passthrough rule allow <cr> | addr <ip-addr> | [port<port> start <port range> end <port>] | description> | rulenum <rule number> | vlan <vlan id>

Parameters

addr <ip-addr>	Specify the subnet IP address.
port <port>	Optionally, specify the port for the subnet.
start <port range> end <port>	Specify the start of the port range and the end port number.
description <description>	Optionally, specify a description of the rule.
rulenum <rulenum>	Optionally, specify a rule number from 1 to N, start, or end. The system evaluate rules in numerical order starting with rule 1. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.
vlan <vlan id>	Specify the VLAN ID.

Usage

A maximum of 105 rules is allowed.

Use reset connection rules to reset an existing connection and force a new connection to be formed. The feature ensures that upon reboot the system resets certain long-lived pass-through connections so they can be optimized. A badly formed rule can block traffic.

This feature is only available in the CLI.

Example

```
amnesiac (config) # in-path passthrough rule allow addr 10.0.0.1 rulenum 1
```

Product

Interceptor appliance

Related Topics

"show in-path passthrough rules"

in-path passthrough rule block

Description

Configures an in-path load balancing rule that blocks pass-through traffic.

Syntax

in-path passthrough rule block <cr> | addr <ip-addr> | [port <port> start <port range> end <port>] | description <description> | rulenum <rule number> | vlan <vlan id>

Parameters

addr <ip-addr>	Specify the subnet IP address.
port <port>	Optionally, specify the port for the subnet.
start <port range> end <port>	Specify the start of the port range and the end port number.
description <description>	Optionally, specify a description of the rule.
<rulenum>	Optionally, specify a rule number from 1 to N, start, or end. The system evaluate rules in numerical order starting with rule 1. If the conditions set in the rule match, then the rule is applied, and the system moves on to the next packet. If the conditions set in the rule do not match, the system consults the next rule. For example, if the conditions of rule 1 do not match, rule 2 is consulted. If rule 2 matches the conditions, it is applied, and no further rules are consulted.
vlan <vlan id>	Specify the VLAN ID.

Usage

These rules block existing pass-through connections and prevent formation of new pass-through connections that match a specified rule. A maximum of 105 rules is allowed.

Use reset connection rules to reset an existing connection and force a new connection to be formed. The feature ensures that upon reboot the system resets certain long-lived pass-through connections so they can be optimized. A badly formed rule can block traffic.

This feature is only available in the CLI.

Example

```
amnesiac (config) # in-path passthrough rule block addr 10.0.0.1 port start 6509 end 6509 vlan 12
```

Product

Interceptor appliance

Related Topics

"show in-path passthrough rules"

in-path passthrough rule edit

Description

Edit an in-path pass-through rule description.

Syntax

in-path passthrough rule edit rulenum <rule number> description <"description">

Parameters

<rulenum>	Specify a rule number to modify.
description <"description">	Specify a description of the rule. The description must be enclosed in double-quotes.

Usage

This feature is only available in the CLI.

Example

```
amnesiac (config) # in-path passthrough rule edit 2 description "blocks traffic to port 6509"
```

Product

Interceptor appliance

Related Topics

"show in-path passthrough rules"

VLAN Segregation Commands

This section describes the VLAN segregation commands available on the Interceptor appliance. VLAN segregation allows network traffic from different groups of users to be kept securely segregated, creating an independent environment for each group or customer. With VLAN segregation enabled, you create instances to segregate traffic to a reserved cluster of Steelheads.

Some commands in this section apply only to a VLAN instance. Those commands are identified with "Interceptor appliance (VLAN instance)" listed in the Product field.

vlan-seg enable

Description

Enables VLAN segregation on the Interceptor appliance. VLAN segregation must be enabled before you can enable instance mode and configure instances.

Syntax

vlan-seg enable

Parameters

None

Usage

You configure VLAN segregation to ensure that traffic from different customers is segregated at all times in a data center. Each instance represents one of the traffic flows that must be segregated. Each instance has a unique configuration independent of another instance in the system.

Each instance must be configured with its own in-path rules, Steelhead appliances, Interceptor peers, port labels, and load balancing rules.

The number of instances supported is limited to 50.

Example

```
amnesiac (config)# vlan-seg enable
Please save your configuration and reload the appliance for your changes to take effect.
```

Product

Interceptor appliance

Related Topics

"instance," "instance-config create," "vlan add," "show detail"

instance-config create

Description

Creates a VLAN instance for VLAN segregation. An instance represents a logical Interceptor VLAN.

Syntax

[no] instance-config create <instance name>

Parameters

<name>	Specify the name of the VLAN segregation instance.

Usage

You configure VLAN segregation to ensure that traffic from different customers is segregated at all times in a data center. Each instance represents one of the traffic flows that must be segregated. Each instance has a unique configuration independent of another instance in the system.

Each instance must be configured with its own in-path rules, Steelhead appliance, Interceptor peers, port labels, load balancing rules, and connection tracing rules.

The number of instances supported is limited to 50.

VLAN segregation must be enabled before you can configure an instance on the appliance. The Interceptor appliance is divided into instances where each instance owns a discrete Steelhead appliance cluster, a shared Interceptor cluster, group settings and configurations that apply to those clusters and unique VLAN tags.

The **no** command option deletes the instance.

Example

```
<<enabling VLAN segregation, creating an instance, entering instance mode, adding a VLAN to an
instance, and restarting the instance>>
amnesiac (config) # vlan-seg enable
Please save your configuration and reload the appliance for your changes to take effect.
amnesiac (config) # instance-config create foo
amnesiac (config) # instance foo
(instance-config)# vlan 10 add
Please restart the instance for your changes to take effect
(instance-config)# restart
```

Product

Interceptor appliance

Related Topics

"instance," "vlan-seg enable," "vlan add," "show detail"

instance-config rename

Description

Renames a VLAN instance for VLAN segregation.

Syntax

instance-config rename <instance name> to <new instance name>

Parameters

<instance name>	Specify the name of the VLAN instance.
<new instance name>	Specify the new name of the VLAN instance.

Usage

The instance name must be a unique alphanumeric string, less than 24 characters.

Example

```
amnesiac (config) # instance-config rename foo to foobar
```

Product

Interceptor appliance

Related Topics

"instance," "vlan-seg enable," "instance-config create," "vlan add," "show detail"

instance

Description

Enters instance-configuration mode for the specified instance. An instance represents a logical Interceptor. You create instances so that you can optimize traffic independently from other instances and provide VLAN segregation.

Syntax

instance <instance name>

Parameters

<instance name>	Specify the name of the VLAN instance.

Usage

After entering instance mode you can:

- enable or restart an instance
- configure in-path rules.
- configure load-balancing rules.
- manage Steelhead appliances (for example, adding and removing).
- add and remove VLANs.

The following commands are available for configuring instances:

- **failover interceptor** For details, see "failover interceptor name additional-ip," "failover interceptor name main-ip"
- **in-path passthrough {move-rule | rule}** For details, see "in-path passthrough move-rule," "in-path passthrough rule allow," "in-path passthrough rule block," "in-path passthrough rule edit"
- **in-path move-rule** For details, see "in-path move-rule"
- **interceptor {communication allow-failure | name}** For details, see "interceptor communication allow-failure enable," "interceptor communication interface," "interceptor communication multi-interface enable,"
- **load balance {default-rule | fair-peer-v2 | move-rule | rule}** For details, see "load balance default-rule fair-peering," "load balance fair-peer-v2 enable," "load balance move-rule," "load balance rule edit rulenum," "load balance rule pass," "load balance rule redirect"
- **show** For details, see "show detail" "show failover interceptor," "show in-path interfaces," "show in-path passthrough rules," "show load balance fair-peer-v2," "show load balance rules," "show steelhead communication," "show steelhead name all,"

- **steelhead communication** For details, see "steelhead communication ack-timer-intvl," "steelhead communication interface," "steelhead communication multi-interface enable," "steelhead communication read-timeout," "steelhead communication recon-timeout"
- **steelhead name** For details, see "steelhead name (Interceptor)," "steelhead name paused,"
- **vlan <id> add** For details, see "vlan add"

Example

```
amnesiac (config)# instance foo
(instance-config)#
```

Product

Interceptor appliance

Related Topics

"instance-config create," "vlan add," "vlan-seg enable," "show detail"

Instance Configuration Mode

This section is a reference for Interceptor instance configuration-mode commands.

To enter instance-configuration mode, use the **instance** command. To exit instance-configuration mode, enter **exit**.

enable

Description

Enables or disables the instance for VLAN segregation.

Syntax

[no] enable

Parameters

None

Usage

Use to enable an instance. The **no** command option disables this feature.

Example

```
amnesiac (config)# instance foo
(instance-config)# enable
```

Product

Interceptor appliance (VLAN instance)

Related Topics

"instance-config create," "vlan add," "vlan-seg enable," "show detail"

restart

Description

Restarts an instance.

Syntax

restart

Parameters

None

Usage

Restart an instance after you modify any of the configuration parameters to apply the changes.

Example

```
(instance-config)# vlan 10 add
Please restart the instance for your changes to take effect
(instance-config)# restart
```

Product

Interceptor appliance (VLAN instance)

Related Topics

"instance-config create," "vlan add," "vlan-seg enable," "show detail"

vlan add

Description

Adds a VLAN to the instance. Adding or removing a VLAN requires a restart of the instance.

Syntax

[no] vlan <vlan id> add

Parameters

<vlan id>	Specify the VLAN ID.

Usage

The instance must be disabled to add or delete a VLAN. The VLAN ID must be unique across all instances. The VLAN ID must be an integer in the range 0-4094, or the keyword untagged. The **no** command option removes the VLAN and corresponding interfaces from the system.

You must restart the instance for your changes to take effect.

You configure VLAN segregation to ensure that traffic from different customers is segregated at all times in a data center. Each instance represents one of the traffic flows that must be segregated. Each instance has a unique configuration independent of another instance in the system.

Each instance must be configured with its own in-path rules, Steelhead appliance, Interceptor peers, port labels, load balancing rules, and connection tracing rules.

The number of instances supported is limited to 50.

Example

```
(instance-config)# vlan 10 add
Please restart the instance for your changes to take effect
(instance-config)# restart
```

Product

Interceptor appliance (VLAN instance)

Related Topics

"instance," "instance-config create," "vlan add," "vlan-seg enable," "show detail"

in-path move-rule

Description

Moves an in-path pass-through rule.

Syntax

in-path move-rule rulenum <rulenum> to <rulenum>

Parameters

<rulenum>	Specify the rule number.

Usage

Moves an in-path rule so that it can be optimized. This command is available only in instance mode.

Example

```
amnesiac (config) # in-path move-rule 2 to 4
```

Product

Interceptor appliance (VLAN instance)

Related Topics

"instance," "instance-config create," "vlan add," "vlan-seg enable" "show detail"

exit

Description

Exit instance-configuration mode.

Syntax

exit

Parameters

None

Usage

Exit instance configuration mode and return to standard configuration mode for the appliance.

Example

```
(instance-config)# exit
amnesiac (config)#
```

Product

Interceptor appliance (VLAN instance)

Related Topics

"instance," "instance-config create," "vlan add," "vlan-seg enable," "show detail"

Displaying Interceptor Settings

This section describes the commands for displaying Interceptor appliance settings. Most of the Steelhead appliance **show** commands are also available in the Interceptor appliance. For detailed information, see Chapter 2, "User-Mode Commands."

show conn-trace

Description

Displays connection tracing status.

Syntax

show conn-trace {connection srcaddr <ip-addr> srcport <port> dstaddr <ip-addr> dstport <port> vlan <vlanid> | rule | summary}

Parameters

<connection>	Displays tracing details of one connection.
srcaddr <ip-addr> srcport <port>	Specify the source IP address, and optionally, source port, for this connection.
dstaddr <ip-addr> dstport <port>	Specify the destination IP address, and optionally, destination port, for this connection.
vlan <vlanid>	Specify the VLAN ID for this connection.
rule	Displays connection tracing rules.
summary	Displays connection tracing summary.

Example

```
amnesiac > show conn-trace summary
Abbreviations: r#: rule matched, O: owner, R: remote, L: local
time created      r# source ip:port        destination ip:port   vlan O state
```

Product

Interceptor appliance

Related Topics

"Interceptor Peering and Redirect Commands"

show detail

Description

Displays information about the current VLAN segregation instance.

Syntax

show detail

Parameters

None

Example

```
(instance-config) # show detail
Instance name: foo
Instance ID: 1
Status: Disabled
VLANs in this instance:
    VLAN: 2
```

Product

Interceptor appliance (VLAN instance)

Related Topics

"instance," "instance-config create," "vlan add," "vlan-seg enable"

show failover interceptor

Description

Displays the failover settings for the Interceptor appliance.

Syntax

show failover interceptor

Parameters

None

Example

```
amnesiac > show failover interceptor
Failover Buddy Name: perf1-int9
Main Address: 172.16.14.4
Additional Addresses: 172.16.121.4
```

Product

Interceptor appliance

Related Topics

"Interceptor Failover Support Commands"

show in-path interfaces

Description

Displays a list of appliance interfaces, indicates whether or not they are currently enabled, and displays the VLAN tag (displays 0 if VLAN is disabled).

Syntax

show in-path interfaces

Parameters

None

Example

```
amnesiac > show in-path interfaces
In-Path Interface(s):
  inpath0_0: enabled  vlan: 0
  inpath0_1: disabled vlan: 0
  inpath1_0: disabled vlan: 0
  inpath1_1: disabled vlan: 0
  inpath2_0: disabled vlan: 0
  inpath2_1: disabled vlan: 0
```

Product

Steelhead appliance, Cloud Steelhead, Interceptor appliance

Related Topics

"Configuring Load Balancing In-Path Pass-Through Rules"

show in-path oop

Description

Displays the out-of-path settings.

Syntax

show in-path oop

Parameters

None

Example

```
amnesiac > show in-path oop
In-path OOP: no
```

Product

Interceptor appliance

Related Topics

"Interceptor Peering and Redirect Commands"

show in-path passthrough rules

Description

Displays in-path pass-through rules.

Syntax

show in-path passthrough rules

Parameters

None

Example

```
amnesiac > show in-path passthrough rules
#   Type     Network              Port                 VLAN
--- -------- -------------------- -------------------- ------
1   allow    all                  all                  all

2   block    172.16.1.1/32        all                  all

3   block    172.16.1.1/32        1234-5678            all

def allow    all                  all                  all
------------------------------------------------------------------------------
3 user added rule(s)
```

Product

Interceptor appliance

Related Topics

"Configuring Load Balancing In-Path Pass-Through Rules"

show instances

Description

Shows all instances configured for the appliance.

Syntax

show instances

Parameters

None

Usage

The instance name must be a unique alphanumeric string, less than 24 characters.

Example

```
amnesiac (config) # show instances
Name   State
====   =====
foo    Disabled
foobar   Enabled
```

Product

Interceptor appliance

Related Topics

"instance," "instance-config create," "show detail"

show interceptor communication

Description

Displays the interface the appliance uses to communicate with peers.

Syntax

show interceptor communication

Parameters

None

Usage

The **show interceptor communication** command replaces the **show redirect** command.

Example

```
amnesiac > show interceptor communication
Redirect Interface: inpath0_0
Multiple Interface Support: yes
Optimize Connections When Peer Interceptor Not Connected: no
```

Product

Interceptor appliance

Related Topics

"Interceptor Peering and Redirect Commands"

show interceptor name all

Description

Displays status of redirect peers. Redirect Peers include Interceptor appliances deployed in parallel to cover asymmetric routing, as well as an Interceptor appliance that functions as a failover interceptor.

Syntax

show interceptor name all [configured]

Parameters

configured	Specify this option to display only a list of configured peers.

Usage

The **show interceptor name all** command replaces the **show redirect peers** command.

Example

```
amnesiac > show interceptor name all

Peer                    Type Version       Backup                Last Reconnect
----------------------- ---- ------------- --------------------- ---------------
perf1-int3              R    3.0.0-beta1   255.255.255.255:0     2011/03/18 12:1
7:29
                             Interface(s): 172.16.153.2:7860     Active
                             Interface(s): 172.16.153.2:40269    Connected
perf1-int8              F    3.0.0-beta1   172.16.14.4:7860      2011/03/18 12:1
7:23
                             Interface(s): 172.16.14.2:40272     Active
                                           172.16.121.2:40268    Connected
                                           172.16.14.2:40273     Connected
                                           172.16.121.2:40269    Connected
Type: 'R' = Redirect
      'F' = Failover
```

Product

Interceptor appliance

Related Topics

"Interceptor Peering and Redirect Commands"

show load balance fair-peer-v2

Description

Displays the load balancing settings for Fair Peering version 2.

Syntax

show load balance fair-peer-v2

Parameters

None

Example

```
amnesiac > show load balance fair-peer-v2
Fair peering V2: no
Threshold: 15%
```

Product

Interceptor appliance

Related Topics

"Load-Balancing Commands"

show load balance rules

Description

Displays load balancing settings.

Syntax

show load balance rules

Parameters

None

Example

```
amnesiac > show load balance rules
#   Type        Source            Destination       VLAN Target(s)
--- ----------- ----------------- ----------------- ---- ---------------
1   redirect    all               all               all  172.0.245.3
                                                         172.0.245.2
                Port: all
                Peer: Any
2   redirect    all               all               all  172.0.245.2
                Port: all
                Peer: Any
def auto        all               all               all  auto
                Port: all
                Peer: Any
------------------------------------------------------------------------------
2 user added rule(s)
```

Product

Interceptor appliance

Related Topics

"Load-Balancing Commands"

show steelhead communication

Description

Displays Steelhead communication settings.

Syntax

show steelhead communication [cf-timer]

Parameter

cf-timer	Displays connection forwarding (CF) timer settings.

Usage

The **show steelhead communication** command replaces the **show in-path neighbor** command.

Example

```
amnesiac > show steelhead communication

Neighbor Pressure Monitoring:            true
    Capacity Reduction Enable:           true
    Permanent Capacity Reduction Enable: true
Neighbor Interface:                      inpath1_0
Multiple Interface Support:              yes
```

Product

Interceptor appliance

Related Topics

"Interceptor Peering and Redirect Commands"

show steelhead name all

Description

Displays Steelhead name settings.

Syntax

show steelhead name all [brief | configured]

Parameters

brief	Displays Steelhead neighbor peers.
configured	Displays configured Steelhead neighbor peers.

Example

```
amnesiac > show steelhead name all

Neighbor 1:
   Name:                     perf1-sh39
   Version:                  cook-x86_64-flamebox-latest-78102
   Last Reconnect:           20011/03/17 13:04:31
   Optimized Connections:    0
   Admission Control:        2000

   Pressure:               Normal
   Interface:                172.16.164.2:40270
       State:                Active

   Interface:                172.16.164.2:40272
       State:                Connected

Neighbor 2:
   Name:                     gen1-sh126
   Version:                  cook-x86_64-flamebox-latest-78102
   Last Reconnect:           20011/03/17 15:31:43
   Optimized Connections:    0
   Admission Control:        6000

   Pressure:               Normal
   Interface:                172.16.165.2:40356
       State:                Active

   Interface:                172.16.165.2:40357
       State:                Connected
```

Product

Interceptor appliance

Related Topics

"Interceptor Peering and Redirect Commands"

show xbridge

Description

Displays the Xbridge settings.

Syntax

show xbridge

Parameters

None

Example

```
amnesiac > show xbridge
Xbridge currently enabled: false
Xbridge enabled after next boot: false
```

Product

Interceptor appliance

Related Topics

“xbridge enable”

Central Management Console Feature Commands

This section describes the Central Management Console (CMC) commands that are unique to the CMC appliance and includes commands up to CMC version 8.5.

Some of the Steelhead appliance CLI commands are also available in the CMC appliance, however Riverbed strongly recommends that you do not use the CLI to configure the CMC appliance, CMC features, or remote Steelhead appliances that you are monitoring and configuring using the CMC.

Riverbed strongly recommends that you use the CMC GUI to configure the CMC appliance, CMC features, and remote Steelhead appliances that you are monitoring and configuring using the CMC.

CMC Compatibility

The recommended versions have been tested with the following CMC versions.

Steelhead Appliance RiOS Version	Recommended Version	CMC Appliance v8.5.x	CMC Appliance v8.0.x	CMC Appliance v7.0.x	CMC Appliance v6.5.x
Steelhead appliance v8.5.x Steelhead CX appliance v8.5.x Steelhead EX appliance v3.0.x	CMC appliance v8.5.x	Parity	Not supported	Not supported	Not supported
Steelhead appliance v8.0.x Steelhead CX appliance v8.0.x Steelhead EX appliance v2.5.x Steelhead EX appliance v2.1.x Steelhead EX appliance v2.0.x	CMC appliance v8.5.x; Edge High Availability only for Steelhead EX appliance v2.0 or later	Parity	Parity	Not supported	Not supported
Steelhead appliance v7.0.x Steelhead CX appliance v7.0.x Steelhead EX appliance v1.0.x	CMC appliance v8.5.x; no Edge High Availability	Parity	Parity	Partial	Partial support with CMC appliance v6.5.3
Steelhead appliance v6.5.x	CMC appliance v8.5.x or CMC appliance v6.5.3*; Steelhead appliance v6.5.1 and later QoS configuration support only	Parity	Parity	Parity	Parity
Steelhead appliance v6.1.x Steelhead appliance v6.0.x Steelhead appliance v5.5.x (v5.5.4 and later)	CMC appliance v8.0.x or CMC appliance v6.5.3*	Monitor only with Steelhead appliance v6.0.0; CMC appliance v6.0.1 unsupported	Parity	Parity	Parity
Interceptor appliance v4.0.x	CMC appliance v8.5.x or CMC appliance v6.5.3*	Parity (via cluster configuration) except VLAN segregation	Monitor only	Monitor only	Monitor only
Interceptor appliance v3.0.x	CMC appliance v8.5.x or CMC appliance v6.5.3*	Parity (via cluster configuration)	Monitor only	Monitor only	Monitor only

Steelhead Appliance RiOS Version	Recommended Version	CMC Appliance v8.5.x	CMC Appliance v8.0.x	CMC Appliance v7.0.x	CMC Appliance v6.5.x
Steelhead Mobile Controller appliance v4.0.x Steelhead Mobile Controller appliance v3.1.x (v3.1.2 and later)	CMC appliance v8.5.x or CMC appliance v6.5.3*	Monitor only	Monitor only	Monitor only	Monitor only
Whitewater appliance v3.0.x	CMC appliance v8.5.x	Monitor only	Not supported	Not supported	Not supported
Granite Core v2.5	CMC appliance v8.5.x	Monitor only	Not supported	Not supported	Not supported

* - Use CMC appliance v6.5.3 if you are using CMC model 8000.

CMC Configuration and Backup Commands

This section describes the CMC commands for backing up the configuration and statistics to a backup server in your network.

cmc backup-config

Description

Backs up the CMC configuration to the configured backup server.

Syntax

cmc backup-config <cr> | name <snapshot name>

Parameters

name <snapshot name>	Specify the name of the configuration snapshot.

Example

```
amnesiac (config) # cmc backup-config
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups"

cmc backup-stats

Description

Backs up statistics to the configured backup server.

Syntax

cmc backup-stats

Parameters

None

Example

```
amnesiac (config) # cmc backup-stats
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups"

cmc reboot

Description

Reboots an appliance or group

Syntax

cmc reboot [appliance <appliance>] | [group <group>] | [switch <no | yes>]

Parameters

appliance <appliance>	Specify the appliance name to reboot.
group <group>	Specify the group name to reboot.
switch <no | yes>	Specify **yes** to switch the boot partition before rebooting; specify **no** to note switch the boot partition before rebooting.

Example

```
amnesiac (config) # cmc reboot appliance gen-sh
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups"

cmc restore-config name

Description

Restores a back-up configuration from the backup server.

Syntax

cmc restore-config name <name> <cr> | vault-pw <password> | omit-vault

Parameters

<name>	Specify the name of configuration snapshot.
vault-pw <password>	Specify the password for backed up secure vault.
omit-vault	Specify to omit restoration the secure vault.

Example

```
amnesiac (config) # cmc restore-config name gen-sh1 omit-vault
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups"

cmc restore-stats

Description

Restores statistics from the configured backup server.

Syntax

cmc restore-stats

Parameters

None

Example

```
amnesiac (config) # cmc restore-stats
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups"

cmc secure-vault unlock appliance

Description

Unlocks the secure vault on the specified appliance.

Syntax

cmc secure-vault unlock appliance <appliance> password <secure vault password>

Parameters

<appliance>	Specify the appliance serial number.
password <secure vault password>	Specify the password for the secure vault of the specified appliance.

Example

```
amnesiac (config) # cmc secure-vault unlock appliance D11AA123456789 password nycD11AA
```

Product

CMC

Related Topics

"cmc secure-vault unlock group"

cmc secure-vault unlock group

Description

Unlocks the secure vault on the appliances in the specified appliance group.

Syntax

cmc secure-vault unlock group <group name> password <secure vault password>

Parameters

<group name>	Specify the name of the group.
password <secure vault password>	Specify the shared password for the secure vault configurations of the appliances in the specified group.

Usage

You can only use this command if all the appliances in the specified group use the same password in the secure vault configurations. Otherwise, use the "cmc secure-vault unlock group" command to unlock the secure vault of individual appliances

Example

```
amnesiac (config) # cmc secure-vault unlock group <manhattan_group> password <nyc123>
```

Product

CMC

Related Topics

"cmc secure-vault unlock group"

CMC Email Commands

This section describes the email commands for the CMC appliance.

cmc email notify appliance aggregate duration

Description

Configures settings for aggregating notifications into periodic emails.

Syntax

cmc email notify appliance aggregate duration <minutes>

Parameters

<minutes>	Specify the number of minutes of aggregate appliance state notifications.

Example

```
amnesiac (config) # cmc email notify appliance aggregate duration 5
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups"

cmc email notify appliance aggregate enable

Description

Enables aggregating notifications into periodic emails.

Syntax

cmc email notify appliance aggregate enable

Parameters

None

Example

```
amnesiac (config) # cmc email notify appliance aggregate enable
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups,"

cmc email notify appliance enable

Description

Enables appliance state notifications.

Syntax

cmc email notify appliance enable

Parameters

None

Example

```
amnesiac (config) # cmc email notify appliance enable
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups,"

CMC Policy Commands

This section describes the policy commands for managing CMC policies.

cmc policy push appliance

Description

Pushes a policy to an appliance or group.

Syntax

cmc policy push appliance <name> | [group <group>] | [restart-service]

Parameters

<name>	Specify the name of target appliance.
group <group>	Specify the group name.
restart-service	Specify to restart the optimization service, if needed.

Example

```
amnesiac (config) # cmc policy push appliance gen-sh restart-service
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups"

cmc policy push group

Description

Pushes a policy to an appliance or group.

Syntax

cmc policy push group<group> | [appliance <name>] | [restart-service]

Parameters

<group>	Specify the name of target group.
appliance <name>	Specify the appliance name.
restart-service	Specify to restart the optimization service, if needed.

Example

```
amnesiac (config) # cmc policy push group mygroup restart-service
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups"

CMC Send CLI Commands

This section describes the commands for sending CLI commands and operations to the Steelhead appliances in your network.

cmc send-cmd appliance

Description

Pushes CLI commands to Steelhead appliances.

Syntax

cmc send-cmd appliance <name> | [group <group>] commands <CLI commands>

Parameters

<group>	Specify the name of target group.
appliance <name>	Specify the appliance name.
commands <CLI commands>	Specify the CLI commands to send. Use a semicolon (;) to separate commands.

Example

```
amnesiac (config) # cmc send-cmd appliance gen-sh commands "show version"
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups"

cmc send-cmd group

Description

Pushes an operation to a Steelhead appliance.

Syntax

cmc send-cmd group <group> | [appliance <name>] commands <CLI commands>

Parameters

<group>	Specify the name of target group.
appliance <name>	Specify the appliance name.
commands <CLI commands>	Specify the CLI commands to send. Use a semicolon (;) to separate commands.

Example

```
amnesiac (config) # cmc send-cmd group mygroup commands "show version"
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups"

cmc send-op appliance

Description

Pushes an operation to a Steelhead appliance.

Syntax

cmc send-op appliance <name> | [group <group>] operation <operation> clean

Parameters

<group>	Specify the name of target group.
appliance <name>	Specify the appliance name.
operation <operation>	Specify the operation: **reload**, **shutdown**, **start**, **stop**, or **restart**
clean	Specify to perform a clean operation.

Example

```
amnesiac (config) # cmc send-op appliance gen-sh operation restart
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups"

cmc send-op group

Description

Pushes an operation to a group of Steelhead appliances.

Syntax

cmc send-op group <group> | [appliance <name>] operation <operation> clean

Parameters

<group>	Specify the name of target group.
appliance <name>	Specify the appliance name.
operation <operation>	Specify the operation: **reload**, **shutdown**, **start**, **stop**, or **restart**
clean	Specify to perform a clean operation.

Example

```
amnesiac (config) # cmc send-op group mygroup operation restart
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups"

CMC System Administration Commands

This section describes the CMC appliance system administration commands.

alarm enable (CMC)

Description

Enables the specified alarm.

Syntax

[no] alarm <type> enable

Parameters

<type>

- **autolicense_error** - This alarm triggers if a critical event for autolicense occurs.
- **autolicense_info** - This alarm triggers if an informational event for autolicense occurs.
- c**mc_daily_config_backup** - This alarm triggers when a CMC appliance configuration backup occurs.
- c**mc_daily_config_backup_restore** - This alarm indicates that a CMC external configuration backup and restore failure occurred.
- c**mc_license_app_insufficient** - This alarm triggers if the CMC appliance has insufficient licenses(s).
- c**mc_license_invalid** - This alarm triggers if one or more CMC licenses are invalid.
- c**mc_license_missing** - This alarm triggers if one or more CMC licenses are missing.
- **config_change** - This alarm triggers when a configuration change is detected.
- **conn_limit_warn** - This alarm triggers when a connection limit is reached.
- **cpu_util_indiv** - Specifies whether the system has reached the CPU threshold for any of the CPUs in the system. If the system has reached the CPU threshold, check your settings. If your alarm thresholds are correct, reboot the Central Management Console
- **critical_temp** - Specifies whether the CPU temperature has exceeded the critical threshold. The default value for the rising threshold temperature is 80° C; the default reset threshold temperature is 70° C.
- **duplex_state** - This alarm indicates that the system has encountered a large number of packet errors in your network. Make sure that the speed and duplex settings on your system match the settings on your switch and router. By default, this alarm is enabled.
- **fan_error** - Specifies whether the system has detected a fan error.
- **flash_error** - This alarm indicates that the system has detected an error with the flash drive hardware.
- **fs_mnt** - This alarm indicates that one of the mounted partitions is full or almost full. This alarm is triggered when only 7% of free space is remaining.
- **hardware** - This alarm indicates the overall health of the hardware.
- **high_usage** - This alarm triggers when high appliance usage is detected.
- **ipmi** - Specifies whether the system has detected IPMI SEL errors.
- **license_expired** - This alarm triggers if one or more features have at least one license installed, but all of them are expired.
- **license_expiring** - This alarm triggers if one or more features is going to expire in two weeks.
- **licensing** - **licensing -** This alarm is the parent licensing alarm and triggers if any of the license_expired, license_expiring, or appliance_unlicensed alarms are active.
- **link_duplex -** This alarm is triggered when an interface was not configured for half-duplex negotiation but has negotiated half-duplex mode. Half-duplex significantly limits the optimization service results. This alarm is enabled by default.
- **link_io_errors -** This alarm is triggered when the link error rate exceeds 0.1% while either sending or receiving packets. This threshold is based on the observation that even a small link error rate reduces TCP throughput significantly. A properly configured LAN connection should experience very few errors. The alarm clears when the rate drops below 0.05%. This alarm is enabled by default.
- **linkstate -** Specifies whether the system has detected a link that is down. The system notifies you through SNMP traps, email, and alarm status.By default, this alarm is not enabled. The **no stats alarm linkstate enable** command disables the link state alarm.

- **memory_error** - Specifies whether the system has detected a memory error.
- **paging** - Specifies whether the system has reached the memory paging threshold. If 100 pages are swapped approximately every two hours the Steelhead appliance is functioning properly. If thousands of pages are swapped every few minutes, then reboot the system. If rebooting does not solve the problem, contact Riverbed Support.
- **pfs_and_rsp** - This alarm indicates that PFS and RSP are both enabled.
- **power_supply** - Indicates an inserted power supply cord does not have power, as opposed to a power supply slot with no power supply cord inserted.
- **raid_error** - Specifies whether the system has encountered RAID errors (for example, missing drives, pulled drives, drive failures, and drive rebuilds). For drive rebuilds, if a drive is removed and then reinserted, the alarm continues to be triggered until the rebuild is complete. Rebuilding a disk drive can take 4-6 hours.
- **raid_disk_indiv** - This alarm indicates that the system has encountered RAID errors (for example, missing drives, pulled drives, drive failures, and drive rebuilds). For drive rebuilds, if a drive is removed and then reinserted, the alarm continues to be triggered until the rebuild is complete. Rebuilding a disk drive can take 4-6 hours.
- **secure_vault** - This alarm indicates a general secure vault error.
- **secure_vault_unlocked** - This alarm indicates whether the secure vault is unlocked. When the vault is unlocked, SSL traffic is not optimized and you cannot encrypt a data store.
- **ssl -** Specifies whether the system has detected an SSL error.
- **sticky_staging_dir** - Specifies whether the system has detected that the process dump staging directory is inaccessible.
- **temperature** - Specifies the CPU temperature.
- **time_drift** - This alarm triggers when a time drift is detected.
- **too_many_half_connections** - This alarm indicates that too many half-opened or half-closed connections are active. By default, this alarm is enabled.
- **unmanaged_peer** - This alarm is triggered when the CMC appliance detects unmanaged peers.
- **upgrade** - This alarm indicates the status of an upgrade.
- **warning_temp -** Specifies whether the CPU temperature has exceeded the warning threshold. The default value for the rising threshold temperature is 80º C; the default reset threshold temperature is 70º C.

Usage

Critical temperature settings cannot be changed. Warning temperature settings can be changed.

The **no** command option disables all statistical alarms. The **no alarm <type> enable** command disables specific statistical alarms.

Example

```
amnesiac # alarm ssl enable
```

Product

CMC

Related Topics

"alarm clear," "alarm clear-threshold," "alarm error-threshold," "show alarm,""show alarms"

CMC Upgrade Commands

This section describes the commands for upgrading the CMC appliance and the Steelhead appliances in your network.

cmc upgrade abort

Description

Aborts appliance upgrades; reboots operations in progress.

Syntax

cmc upgrade abort <cr> | [all active [appliance <ip-addr>| group <group name>]] | [appliance <ip-addr> | group <group name>]

Parameters

[all active [appliance <ip-addr>| group <group name>]]	Aborts all appliances or specified appliances and groups.
appliance <serial number>	Specify the CMC appliance serial number.
group <group name>	Specify the CMC appliance group name.

Example

```
amnesiac (config) # cmc upgrade abort all active appliance 10.0.0.1
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups,"

cmc upgrade appliance

Description

Upgrades target appliances with new software.

Syntax

cmc upgrade appliance <serial number> <cr> [group <group name> <cr>] | image <image name>| image_url <image url> | stop_after [install | reboot]| transition <image name>| transitions_url <image url>

Parameters

appliance <serial number> <cr> | [group <group name> <cr>]	Upgrades the specified appliance and group.
image <image name>	Specify the image name.
image_url	Specify the image URL
stop_after [install | reboot]	Specify when (**install** or **reboot**) the upgrade should stop.
transition <image name>	Specify the 32-bit transition image.
transition_url <image url>	Specify the remote image to use as transition image.

Example

```
amnesiac (config) # cmc upgrade appliance X67XR00007DC1 image rbt_sh 5.5.1h #58_18
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups,"

cmc upgrade auto

Description

Enables automatic upgrades.

Syntax

[no] cmc upgrade auto i386 <image name> x86_64 <image name> image transition <image name>

Parameters

i386 <image name>	Specify the image name to use for 32-bit appliances. Use double-quotes (") to unset.
x86_64 <image name>	Specify the image name to use for 64-bit appliances. Use double-quotes (") to unset.
image transition <image name>	Specify the 32-bit transition image.

Example

```
amnesiac (config) # cmc upgrade auto 1386 rbt_sh 5.5.1h #58_18
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups,"

cmc upgrade concurrent limit

Description

Configures concurrent upgrades.

Syntax

cmc upgrade concurrent limit <# of upgrades>

Parameters

<# of upgrades>	Specify the maximum number of upgrades to process concurrently.

Example

```
amnesiac (config) # cmc upgrade concurrent limit 10
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups,"

cmc upgrade delete

Description

Deletes an appliance image from the image library.

Syntax

cmc upgrade delete <image name>

Parameters

<image name>	Specify the software image name to delete.

Example

```
amnesiac (config) # cmc upgrade delete rbt_sh 5.5.1h #58_18
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups,"

cmc upgrade fetch

Description

Downloads an appliance image to the local image library.

Syntax

cmc upgrade fetch <http, ftp, or scp URL (e.g. scp://username:password@host/path)>

Parameters

<<http, ftp, or scp URL (e.g. scp://username:password@host/path)>	Specify the HTTP, FTP or scp URL. For example, scp://user:pass@host/pathtoimage

Example

```
amnesiac (config) # cmc upgrade fetch scp://user:pass@server/path/to/image
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups,"

cmc upgrade timeout

Description

Configures a time-out period for upgrades.

Syntax

cmc upgrade timeout <minutes>

Parameters

<minutes>	Specify to automatically stop upgrades that take longer than the time-out period..

Example

```
amnesiac (config) # cmc upgrade timeout 60
```

Product

CMC

Related Topics

"show cmc appliances," "show cmc groups,"

CMC Export Commands

This section describes the export commands for the CMC appliance.

export app_details

Description

Exports appliance information for CMC managed appliances to a remote email address or SCP/FTP location.

Syntax

export app_details [appliance <serial number>] [group <group>] report-format <options> {to-email <email-address> | to-file {<scp://username:password@hostname/path/filename> | <ftp://username:password@hostname/path/filename>}}

Parameters

appliance <serial number>	Specify the serial number of the target appliance. Use a comma to separate different appliance serial numbers if there is more than one target.
group <group>	Specify the name of the target group. Use a comma to separate different target groups if there is more than one target.
report-format <options>	Exports report type format information. Each report format has the following options: **html** - An HTML report that contains images. **csv** - A CSV report that includes actual statistical samples. **pdf** - A PDF report that contains images.
to-email <email-address>	Exports the report to the specified email address.
<to-file>	Specify an SCP/FTP URL. The exported file is always a compressed zip folder ending with a .zip extension. If the user is scheduling a recurring job to export reports to a URL, it is recommended that the user specify the URL as a directory name, and not a file name, to prevent overwriting of a previously exported file.

Example

```
amnesiac # export app_details appliance A16UV0052950,A16UV0052950 report-format html to-email
name@email.com

amnesiac # export app_details group Global report-format html to-file scp://username@servername/
path/to/filename

amnesiac # export app_details group Global report-format html to-file scp://username@servername/
path/to/directory/
```

Product

CMC

Related Topics

"Displaying CMC Data"

export statistics

Description

Exports statistical information for CMC managed appliances to a remote email address or SCP/FTP location.

Syntax

export statistics [appliance steelhead <serial number>] [group <group>] report-format <options> [granularity <options>] {period <options> | start-time <start-time> end-time <end-time>} report <report-name> [direction <direction>] [per-appliance] [port <port-number>] [qos-classes {all | default}] [data {sent | dropped}] [response-type <options>] [type {both | optimized | passthrough}] [units <size>] {to-email <email-address> | to-file {<scp://username:password@hostname/path/filename> | <ftp://username:password@hostname/path/filename>}}

Parameters

appliance steelhead <serial number>	Specify the serial number of the target appliance. Use a comma to separate different appliance serial numbers if there is more than one target appliance.
group <group>	Specify the name of the target group. Use a comma to separate different target groups if there is more than one target group.
report-format <options>	Specify report type format. Each report format has the following options: • **html** - Creates an HTML report that contains images. • **csv** - Creates a CSV report that includes actual statistical samples. • **pdf** - Creates a PDF report that contains images.
granularity <options>	Optionally, specify the granularity of the specified report. Each granularity format has the following options: • **300** - Export 5 minute samples. • **3600** - Export 1 hour samples. • **86400** - Export 1 day samples. For the best accuracy, Riverbed recommends that you do not specify this option. When you specify the granularity, data is gathered only from specified samples. This sampling can produce coarse reports if granularity is too low (such as one day) or very large data reports if granularity is too high (such as 5 minutes). If this option is not specified, the system automatically chooses the best combination for reporting.
period <options>	Specify the period for which to generate a report. Each period format has the following options: • **month** - Export last months statistics. • **week** - Export last week statistics. • **day** - Specify the day for the export. • **hour** - Specify the hour for the export. • **last_calendar_month** - Specify the last calendar month. • **last_calendar_week** - Specify the last calendar week. • **last_calendar_day** - Specify the last calendar day (yesterday).
start-time <start-time>	Specify the start time for reporting statistics in the format 'YYYY/MM/DD HH:MM:SS'.
end-time <end- time>	Specify the end time for reporting statistics in the following 'YYYY/MM/DD HH:MM:SS'.
report <report- name>	Specify the report names that you want to export. Use a comma to separate the different report names. For a complete list of report names available, see the CLI help.
direction <direction>	Specify the direction of traffic to include in statistics for various reports such as Throughput and BW Optimization reports. Choices are: • **in** - WAN-to-LAN traffic • **out** - LAN-to-WAN traffic • **both** - bidirectional traffic
per-appliance	Specify one graph per appliance. This option creates a report graph for each specified appliance in the **appliance steelhead** parameter and for each appliance that is part of the group specified by the **group** parameter.
port <port-number>	Specify the port that you want to create a report about. Use a comma to separate the list of ports if there is more than one port.
qos-classes {all | default}	Accepts QoS classes for which QoS reports need to be exported. The options are **all** and **default**. This option is only required for QoS reports.

data {sent | dropped}	Specifies data for QoS reports. The data options are **sent** and **dropped**.
response-type <options>	Specify response types for NFS. The response-type options are: **all**, **local**, **remote**, and **delayed**.
type <options>	Specify traffic type for the Traffic Summary report. The type options are: • **optimized** - optimized traffic • **passthrough** - passthrough traffic • **both** - both optimized and passthrough traffic
units <size>	Specify statistics size. Use this option for reports such as Connection Forwarding, QoS Stats (Sent/Dropped), and so on. The units options are: **bytes**, **bits**, **packets**.
to-email <email-address>	Exports the report to the specified email address.

to-file < scp://username:password@hostname/path/filename>	Specify a SCP/FTP URL. The exported file is always a compressed zip folder ending with a .zip extension. For example, if the user is scheduling a recurring job to export reports to a URL, it is recommended that the user specify the URL as a directory name, and not a file name, to prevent overwriting of a previously exported file.
	`amnesiac > #export statistics group Global report-format html to-file scp://username@servername/path/to/filename`
	`amnesiac > #export statistics group Global report-format html to-file scp//username@servername/path/to/directory`

Example

Per-Appliance Reporting

If the group Global contains appliances APP1 and APP2, the following example exports one Data Reduction report with separate graphs for both APP1 and APP2:

```
amnesiac # export statistics group Global period week report-format pdf report dataReduction per-
appliance to-email someone@emailaddr.com
```

The following example exports one Data Reduction report for both APP1 and APP2:

```
amnesiac # export statistics group Global period week report-format html report dataReduction to-
email someone@emailaddr.com
```

Per-Port(s) Reporting

The following example creates and exports four graphs in the Data Reduction Report: APP1 for port 21, APP1 for port 443, APP2 for port 21, and APP2 for port 443:

```
amnesiac # export statistics group Global period week report-format html report dataReduction per-
appliance port 21,443 to-email someone@emailaddr.com
```

Exporting a Report to a Remote File

The following example exports a report in PDF format to a remote file:

```
amnesiac > #export statistics group company1 report-format pdf to-file scp://username@servername/
path/to/dnsdata
Reports will be exported as a compressed file
```

Product

CMC

Related Topics

"Displaying CMC Data"

Displaying CMC Data

This section describes the **show** commands that are unique to the CMC appliance.

show cmc appliance

Description

Displays settings for the specified CMC appliance.

Syntax

show cmc appliance <serial number>

Parameters

<serial number >	Specify the serial number for the appliance.

Example

```
amnesiac (config) # show cmc appliance T30QK0006805E
Appliance T30QK0006805E (T30QK0006805E)

   Connected:                   false
   Version:
   Model:
   Parent Group:                Global
   Status:                      Unknown
   Reduction:                   Unavailable
   Comment:

   Optimization Policy:
   Networking Policy:
   Security Policy:
   System Policy:
   Branch Services Policy:

   Auto-configuration:          false
   Branch Managed:              false
   User-specified Address:
   Auto-registration Address:

   Disable Auto-Upgrade:        false
```

Product

CMC

Related Topics

"CLI Terminal Configuration Commands"

show cmc appliances

Description

Displays settings for all CMC appliances.

Syntax

show cmc appliances [detail]

Parameters

detail	Displays detailed information for all appliances.

Example

```
amnesiac (config) # show cmc appliances
```

Product

CMC

Related Topics

"CLI Terminal Configuration Commands"

show cmc autolicense status

Description

Displays the status of the CMC autolicense client operation.

Syntax

show cmc autolicense status

Parameters

None

Example

```
amnesiac >  show cmc autolicense status
Server: api.licensing.riverbed.com
Last attempt: Never
Successful: no
Status: Not yet attempted
```

Product

CMC

Related Topics

"CLI Terminal Configuration Commands"

show cmc backup appsnaps status

Description

Displays status of the managed appliance snapshots backup operation.

Syntax

show cmc backup appsnaps status

Parameters

None

Example

```
amnesiac (config) #show cmc backup appsnaps status
idle
```

Product

CMC

Related Topics

"CMC Configuration and Backup Commands"

show cmc backup config

Description

Displays list of backup files on the disk.

Syntax

show cmc backup config local {local | status}

Parameters

local	Displays detailed information for all appliances.
status	Displays status of the configuration backup operation.

Example

```
amnesiac > show cmc backup config local
amnesiac > show cmc backup config status
idle
```

Product

CMC

Related Topics

"CMC Configuration and Backup Commands"

show cmc backup server space

Description

Displays space usage on the backup server.

Syntax

show cmc backup server space

Parameters

None

Example

```
amnesiac > show cmc backup server space
Backup space usage information is unavailable
```

Product

CMC

Related Topics

"CMC Configuration and Backup Commands"

show cmc backup stats status

Description

Displays status of the statistics backup operation.

Syntax

show cmc backup stats status

Parameters

None

Example

```
amnesiac (config)  # show cmc backup stats status
idle
```

Product

CMC appliance

Related Topics

"CMC Configuration and Backup Commands"

show cmc email notify appliance

Description

Displays the CMC email notifications for appliances.

Syntax

show cmc email notify appliance

Parameters

None

Usage

None

Example

```
amnesiac >  show cmc email notify appliance
CMC Email Applicance Notification
Appliance State Notification:            no
Appliance Aggregate State Notification: no
        Aggregate Duration(seconds):    60
```

Product

CMC

Related Topics

"CMC Configuration and Backup Commands"

show cmc group

Description

Displays the specified CMC appliance group settings.

Syntax

show cmc group <group name>

Parameters

<group name>	Specify the group name.

Example

```
amnesiac (config) # show cmc group Global
Group Global
```

```
   Parent Group:
   Comment:

   Optimization Policy:
   Networking Policy:
   Security Policy:
   System Policy:

   Appliances:
      T24GK00008C48   10.1.11.0
```

Product

CMC

Related Topics

"CLI Terminal Configuration Commands"

show cmc groups

Description

Displays the specified CMC appliance group settings.

Syntax

show cmc groups [detail]

Parameters

detail	Displays detailed information for CMC groups.

Example

```
amnesiac > show cmc groups
Group Global
   Parent Group:
   Comment:
   Appliances:                 T24GK000XXXXX
```

Product

CMC

Related Topics

"CLI Terminal Configuration Commands"

show cmc monitored-port

Description

Displays the information on a monitored port.

Syntax

show cmc monitored-port <port number>

Parameters

<port number>	Specify the port number to monitor.

Example

```
amnesiac >  show cmc monitored-port 80
Port Number     Description
```

```
80              HTTP
```

Product

CMC

Related Topics

"CMC Configuration and Backup Commands"

show cmc op-history

Description

Displays the history of operations.

Syntax

show cmc op-history

Parameters

None

Example

```
amnesiac >  show cmc op-history
Date/Time           Operation      Status  User     Message

2013/07/11 13:31:24 Policy Push    success admin    Successfully pushed to all (1) attempted
appliance(s).
2013/07/11 13:30:53 Policy Push    success admin    Successfully pushed to all
```

Product

CMC

Related Topics

"CMC Configuration and Backup Commands"

show cmc restore appsnaps status

Description

Displays the status of the managed appliance snapshots restore operation.

Syntax

show cmc restore appsnaps status

Parameters

None

Example

```
amnesiac >  show cmc restore appsnaps status
idle
```

Product

CMC

Related Topics

"CMC Configuration and Backup Commands"

show cmc restore config status

Description

Displays the status of the configuration restore operation

Syntax

show cmc restore config status

Parameters

None

Example

```
amnesiac >  show cmc restore config status
idle
```

Product

CMC

Related Topics

"CMC Configuration and Backup Commands"

show cmc restore stats status

Description

Displays the status of the statistics restore operation.

Syntax

show cmc restore stats status

Parameters

None

Example

```
amnesiac >  show cmc restore stats status
idle
```

Product

CMC

Steelhead Mobile Controller Feature Commands

This section describes the Steelhead Mobile Controller (Mobile Controller) commands that are unique to the Mobile Controller appliance and includes commands up to Mobile Controller version 4.0.

Riverbed strongly recommends that you use the Mobile Controller GUI to configure the Mobile Controller appliance and Mobile Controller features.

- "Cluster Commands" on page 970
- "Policy Commands" on page 973
- "Endpoint Commands" on page 1022

- "Package Commands" on page 1023
- "Domain Command" on page 1025
- "Show Commands" on page 1025

Cluster Commands

This section describes the cluster commands.

cluster detach

Description

Detaches the Mobile Controller from an existing cluster.

Syntax

cluster detach

Parameters

None

Usage

Use this command to temporarily detach a Mobile Controller from a cluster.

Example

```
amnesiac (config) # cluster detach
```

Product

Steelhead Mobile Controller

Related Topics

"cluster join," "cluster remove," "aaa authentication login default"

cluster join

Description

Adds a Mobile Controller to a cluster.

Syntax

cluster join <hostname> [<port>]

Parameters

<hostname>	Specify the hostname of the Mobile Controller.
<port>	Optionally, specify a port number. The default port is 7870.

Example

```
amnesiac (config) # cluster join mobilecontroller1234
Sending cluster join action to host:mobilecontroller1234:7870
```

Product

Steelhead Mobile Controller

Related Topics

"cluster detach," "cluster remove," "aaa authentication login default"

cluster license checkout-count

Description

Configures the global count of cluster licenses that can be checked out.

Syntax

[no] cluster license checkout-count <number>

Parameters

<number>	Specify the global number of licenses to check out.

Usage

The **no** command option resets cluster license settings.

Example

```
amnesiac (config) # cluster license checkout-count 100
```

Product

Steelhead Mobile Controller

Related Topics

"show cluster licenses," "show cluster license settings"

cluster license high-threshold

Description

Configures the threshold percentage to check out more licenses.

Syntax

[no] cluster license high-threshold <percentage>

Parameters

<percentage>	Specify the numerical value representing percentage.

Usage

The **no** command option resets cluster license settings.

Example

```
amnesiac (config) # cluster license high-threshold 90
```

Product

Steelhead Mobile Controller

Related Topics

"show cluster licenses," "show cluster license settings"

cluster license initial-count

Description

Configures cluster-wide setting of initial number of licenses that can be checked out.

Syntax

[no] cluster license initial-count <number>

Parameters

<number>	Specify the number of licenses to check out.

Usage

The **no** command option resets cluster license settings.

Example

```
amnesiac (config) # cluster license initial-count 100
```

Product

Steelhead Mobile Controller

Related Topics

"show cluster licenses," "show cluster license settings"

cluster license low-threshold

Description

Configures the threshold percentage to check in unused licenses.

Syntax

[no] cluster license low-threshold <percentage>

Parameters

<percentage>	Specify the numerical value representing percentage.

Usage

The **no** command option resets cluster license settings.

Example

```
amnesiac (config) # cluster license low-threshold 70
```

Product

Steelhead Mobile Controller

Related Topics

"show cluster licenses," "show cluster license settings"

cluster remove

Description

Removes the Mobile Controller from the cluster.

Syntax

cluster remove <hostname> [port <port>]

Parameters

<hostname>	Specify the hostname of the Mobile Controller.
<port>	Optionally, specify a port number. The default port is 7870.

Usage

Removes a remote host from the cluster.

Example

```
amnesiac (config) # cluster remove mobilecontroller1234
```

Product

Steelhead Mobile Controller

Related Topics

"cluster join," "cluster detach," "aaa authentication login default"

Policy Commands

This section describes the Mobile Controller policy commands.

delete policy id

Description

Deletes the specified policy from the Mobile Controller.

Syntax

delete policy id <id>

Parameters

<id>	Specify the policy ID number.

Example

```
amnesiac (config) # delete policy id 1
```

Product

Steelhead Mobile Controller

Related Topics

"show policy list"

policy assignment adpath

Description

Configures policy assignment by Active Directory path.

Syntax

[no] policy assignment adpath <ad path> policy_id <policy id>

Parameters

<ad path>	Specify the Active Directory path.
policy_id <policy id>	Specify the policy ID number.

Usage

The **no** command option removes the policy assignment by Active Directory path.

Example

```
amnesiac (config) # no policy assignment adpath //path policy_id 1
```

Product

Steelhead Mobile Controller

Related Topics

"show policy assignments adpath"

policy assignment depid

Description

Configures policy assignment by deployment ID.

Syntax

[no] policy assignment depid <deploy id> policy_id <policy id>

Parameters

depid <deploy-id>	Specify the deployment ID.
policy_id <policy id>	Specify the policy ID number.

Usage

The **no** command option removes the policy assignment.

Example

```
amnesiac (config) # policy assignment depid 2566 policy_id 1
```

Product

Steelhead Mobile Controller

Related Topics

"show policy assignments depid"

policy assignment removeall-adpth

Description

Removes all the Active Directory path assignments.

Syntax

policy assignment adpath removeall-adpath

Parameters

None

Example

```
amnesiac (config) # policy assignment removeall-adpth
```

Product

Steelhead Mobile Controller

Related Topics

"show policy assignments adpath"

policy assignment removeall-depid

Description

Removes all the deployment ID assignments

Syntax

policy assignment removeall-depid

Parameters

None

Example

```
amnesiac (config) # policy assignment removeall-depid
```

Product

Steelhead Mobile Controller

Related Topics

"show policy assignments depid"

policy id advanced

Description

Configures advanced policy assignment settings.

Syntax

[no] policy id <id> advanced {nat-port <port-number> | service-port <port-number>}

Parameters

<id>	Specify the policy ID number.
nat-port <port-number>	Specify the in-path NAT port number.
service-port <port-number>	Specify the service port number.

Usage

The **no** command option disables the specified port setting.

Example

```
amnesiac (config) # policy id 1 advanced nat-port 7801
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id branch-warming enable

Description

Enables branch warming for a specified policy.

Syntax

[no] policy id <id> branch-warming enable

Parameters

<id>	Specify the policy ID number.

Usage

Branch warming requires Steelhead Mobile v3.0 or later.

You must also enable branch warming on the Steelhead appliance. For detailed information, see the Management Console online help or the *Steelhead Appliance Management Console User's Guide*.

The **no** command option disables branch warming.

Example

```
amnesiac (config) # policy id 1 branch-warming enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id cifs enable

Description

Configures CIFS settings for a specified policy.

Syntax

[no] policy id <id> cifs {applock |clear-read-resp | dw-throttling | mac-qpath-sqsh | secure-sig-opt | smb1-bckwd-comp} enable

Parameters

<id>	Specify the policy ID number.
applock	Enables CIFS latency optimizations to improve read and write performance for Microsoft Word and Excel documents when multiple users have the file open.
clear-read-resp	Increases performance for deployments with high bandwidth, low-latency links.
dw-throttling	Enables the CIFS dynamic throttling mechanism that replaces the current static buffer scheme. If you enable CIFS dynamic throttling, it is activated only when there are sub-optimal conditions on the server-side causing a backlog of write messages; it does not have a negative effect under normal network conditions. The **no** command option disables the dynamic throttling mechanism.
mac-qpath-sqsh	Enables Mac-specific CIFS query path squash.
secure-sig-opt	Enables optimization of connections with security signatures.
smb1-bckwd-comp	Enables CIFS SMBv1 backward-compatibility mode.

Usage

The **no** command option disables CIFS settings.

For detailed information about CIFS, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 cifs dw-throttling enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id citrix enable

Description

Enables Citrix optimization support on the specified policy.

Syntax

[no] policy id <id> citrix enable

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option disables Citrix optimization support.

For detailed information about CIFS, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 citrix enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id citrix ica

Description

Configures Citrix ICA settings on the specified policy.

Syntax

[no] policy id <id> citrix ica port <port-number>

Parameters

<id>	Specify the policy ID number.
port <port>	Specify the ICA optimization port number.

Usage

The **no** command option disables Citrix ICA support.

For detailed information about CIFS, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 citrix ica port 1494
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id citrix secure-ica enable

Description

Enables Citrix secure ICA support on the specified policy.

Syntax

[no] policy id <id> citrix secure-ica enable

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option disables Citrix secure ICA support.

For detailed information about CIFS, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 citrix secure-ica enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id citrix session reliability port

Description

Configures the Citrix session reliability port on the specified policy.

Syntax

[no] policy id <id> citrix session reliability port <port>

Parameters

<id>	Specify the policy ID number.
port <port>	Specify the port number.

Usage

The **no** command option disables Citrix session reliability support.

For detailed information about CIFS, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 citrix session reliability port 2598
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id connection lan receive buf-size

Description

Sets the LAN receive buffer size for high-speed TCP on the specified policy.

Syntax

[no] policy id <id> connection lan receive buf-size <bytes>

Parameters

<id>	Specify the policy ID number.
<bytes>	Specify the LAN receive buffer size. The default value is 32768.

Usage

To support high-speed TCP, you must increase your LAN buffer size to 1 MB.

The **no** command option resets the buffer size to the default value.

For detailed information about high-speed TCP, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 connection lan receive buf-size 1000000
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id connection lan send buf-size

Description

Configures LAN send buffer settings for high-speed TCP on the specified policy.

Syntax

[no] policy id <id> connection lan send buf-size <bytes>

Parameters

<id>	Specify the policy ID number.
<bytes>	Specify the LAN send buffer size. The default value is 81920.

Usage

For detailed information about high-speed TCP, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) #policy id 1 connection lan send buf-size 1000000
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id connection wan receive def-buf-size

Description

Sets the WAN receive buffer size for high-speed TCP on the specified policy.

Syntax

[no] policy id <id> connection wan receive def-buf-size <bytes>

Parameters

<id>	Specify the policy ID number.
<bytes>	Specify the WAN receive buffer size. The default value is 262140.

Usage

To configure your WAN buffer, you must increase the WAN buffers to twice Bandwidth Delay Product (BDP) or 10 MB. To calculate the BDP WAN buffer size:

Bandwidth = 155000000 Mbps
Delay = 100 ms

For a link of 155 Mbps and 100 ms round-trip delay, set the WAN buffers to

```
2 * 155000000 * 0.1 / 8 = 3875000
```

To calculate the BDP for a link

```
bandwidth * delay / 8 / MTU = X
```

If X is greater than the default (256 KB), enable HS-TCP with the correct buffer size.

The **no** command option resets the buffer size to the default.

For detailed information about high-speed TCP, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 connection wan receive def-buf-size 3875000
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id connection wan send def-buf-size

Description

Sets the WAN send buffer size for high-speed TCP on the specified policy.

Syntax

[no] policy id <id> connection wan send def-buf-size <bytes>

Parameters

<id>	Specify the policy ID number.
<bytes>	Specify the WAN send buffer size. The default value is 262140.

Usage

To configure your WAN buffer, you must increase the WAN buffers to twice Bandwidth Delay Product (BDP) or 10 MB. To calculate the BDP WAN buffer size:

Bandwidth = 155000000 Mbps
Delay = 100 ms

For a link of 155 Mbps and 100 ms round-trip delay, set the WAN buffers to

```
2 * 155000000 * 0.1 / 8 = 3875000
```

To calculate the BDP for a link

```
bandwidth * delay / 8 / MTU = X
```

If X is greater than the default (256 KB), enable HS-TCP with the correct buffer size.

The **no** command option resets the buffer size to the default.

For detailed information about high-speed TCP, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 connection wan send def-buf-size 3875000
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id endpoint controller add

Description

Adds the Mobile Controller to the policy.

Syntax

policy id <id> endpoint controller add <controller name> port <port>

Parameters

<id>	Specify the policy ID number.
<controller name>	Specify the Mobile Controller name.
port <port>	Optionally, specify the port number.

Usage

The **no** command option removes the Mobile Controller from the policy.

Example

```
amnesiac (config) # policy id 1 endpoint controller add smc1.example.com port 1234
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id endpoint controller randomize

Description

Configures random ordering of Mobile Controllers when connecting.

Syntax

policy id <id> endpoint controller randomize

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option disables the randomize feature.

Example

```
amnesiac (config) # policy id 1 endpoint controller randomize
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id endpoint controller remove

Description

Removes the Mobile Controller from the policy.

Syntax

policy id <id> endpoint controller remove <controller name>

Parameters

<id>	Specify the policy ID number.
<controller name>	Specify the Mobile Controller name.

Example

```
amnesiac (config) # policy id 1 endpoint controller remove smc.example.com
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id endpoint controller remove-all

Description

Removes all Mobile Controllers from the policy.

Syntax

policy id <id> endpoint controller remove-all

Parameters

<id>	Specify the policy ID number.

Example

```
amnesiac (config) # policy id 1 endpoint controller remove-all
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id endpoint datastore-size

Description

Configures the data store size on the endpoint client.

Syntax

policy id <id> endpoint datastore-size

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option disables the data store size.

Example

```
amnesiac (config) # policy id 1 endpoint datastore-size
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id endpoint dis-chksum-offl

Description

Disables checksum off-loading for TCP/IP operations.

Syntax

[no] policy id <id> endpoint dis-chksum-offl

Parameters

<id>	Specify the policy ID number or name.

Usage

Requires a client reboot.

Example

```
amnesiac (config) # policy id 1 endpoint dis-chksum-offl
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id endpoint kickoff

Description

Configures the service to kick off the connections of the specified process.

Syntax

[no] policy id <id> endpoint kickoff <process name>

Parameters

<id>	Specify the policy name or number.
<process name>	Specify the kickoff process name.

Usage

The **no** command option disables the kickoff process.

For detailed information about the kickoff feature, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 endpoint kickoff testkickoff
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id endpoint max-log-files

Description

Sets the maximum number of log files.

Syntax

[no] policy id <id> endpoint max-log-files <value>

Parameters

<id>	Specify the policy name or number.
<value>	Specify the number of log files.

Usage

The **no** command option disables the maximum number of log files.

Example

```
amnesiac (config) # policy id 1 endpoint max-log-files 10
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id endpoint max-log-size

Description

Sets the maximum size of the log files.

Syntax

[no] policy id <id> endpoint max-log-size <number of kilobytes>

Parameters

<id>	Specify the policy name or number.
<number of kilobytes>	Specify the number of kilobytes.

Usage

The **no** command option disables the maximum log size.

Example

```
amnesiac (config) # policy id 1 endpoint max-log-size 500
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id endpoint override-opt

Description

Allows the user to modify optimization settings on the endpoint client.

Syntax

[no] policy id <id> endpoint override-opt

Parameters

<id>	Specify the policy name or number.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # policy id 1 endpoint override-opt
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id endpoint show-tray-icon

Description

Displays the client in the system tray.

Syntax

[no] policy id <id> show-tray-icon

Parameters

<id>	Specify the policy name or number.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # policy id 1 endpoint show-tray-icon
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id ftp port

Description

Configures FTP settings on the specified policy.

Syntax

[no] policy id <id> ftp port <port>

Parameters

<id>	Specify the policy ID number.
port <port>	Specify the port number.

Usage

The **no** command option removes the FTP port from the list.

Example

```
amnesiac (config) # policy id 1 ftp port 259
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id http add-cookie

Description

Enables cookies in the HTTP optimization process on the specified policy.

Syntax

[no] policy id <id> http add-cookie

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option disallows cookies.

For detailed information about HTTP optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 http add-cookie
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id http enable

Description

Enables HTTP protocol optimization support on the specified policy.

Syntax

[no] policy id <id> http enable

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option disables HTTP protocol optimization support.

For detailed information about HTTP optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 http enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id http insrt-keep-aliv

Description

Adds the keep-alive option to the HTTP optimization on the specified policy.

Syntax

[no] policy id <id> http insrt-keep-aliv

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option disallows the insertion of the keep alive option.

For detailed information about HTTP optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 http insrt-keep-aliv
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id http metadata-resp max-time

Description

Configures the maximum time metadata response settings on the specified policy.

Syntax

[no] policy id <id> http metadata-resp max-time <seconds>

Parameters

<id>	Specify the policy ID number.
<seconds>	Specify the number of seconds.

Usage

The **no** command option disables the maximum response time settings.

For detailed information about HTTP optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 http metadata-resp max-time 120
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id http metadata-resp min-time

Description

Configures the minimum time for metadata response settings on the specified policy.

Syntax

[no] policy id http metadata-resp min-time <seconds>

Parameters

<id>	Specify the policy ID number.
<seconds>	Specify the number of seconds.

Usage

The **no** command option disables the minimum response time settings.

For detailed information about HTTP optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 http metadata-resp min-time 20
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id http metadata-resp mode

Description

Configures the object caching mode for the HTTP optimization cache.

Syntax

[no] policy id <id> http metadata-resp mode {all | use-list | none}

Parameters

<id>	Specify the policy ID number.
all	Cache all allowable objects.
use-list	Cache objects matching the extension list.
none	Do not cache any object.

Usage

The **no** command option resets the HTTP optimization caching mode to the default mode.
For detailed information about HTTP optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 http metadata-resp mode all
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id http prefetch extension

Description

Configures prefetch extensions on the specified policy.

Syntax

[no] policy id <id> http prefetch extension <extension>

Parameters

<id>	Specify the policy ID number.
<extension>	Specify extensions to prefetch. Default extensions are css, gif, jpg, js, and png.

Usage

The **no** command option removes the configured prefetch extension.
For detailed information about HTTP optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 http prefetch extension png
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id http prefetch tag attribute

Description

Configures the tag attributes to prefetch on the specified policy.

Syntax

[no] policy id <id> http prefetch tag <tag> attribute <attribute>

Parameters

<id>	Specify the policy ID number.
<tag >	Specify the tag to add or modify.
<attribute>	Specify the tag attribute.

Usage

The **no** command option disables the HTTP prefetch option.

For detailed information about HTTP optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 http prefetch tag body attribute background
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id http strip-compress

Description

Configures HTTP strip compression options.

Syntax

[no] policy id <id> http strip-compress

Parameters

<id>	Specify the policy ID number.

Usage

Removes the Accept-Encoding lines from the HTTP headers that contain gzip or deflate. These Accept-Encoding directives allow Web browsers and servers to send and receive compressed content rather than raw HTML.

The **no** command option disables the HTTP strip compression.

For detailed information about HTTP optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 http strip-compress
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id http server-subnet

Description

Configures HTTP optimization for a subnetwork on the specified policy.

Syntax

[no] policy id <id> http server-subnet <subnet> [force-nego-ntlm {yes |no}] [obj-pref-table {yes |no}] [gratuitous-401 {yes |no}] [insert-cookie {yes |no}] [insrt-keep-aliv {yes |no}] [parse-prefetch {yes |no}] [reuse-ntlm {yes |no}] [strip-auth-hdr {yes |no}] [strip-compress {yes |no}] [url-learning {yes |no}]

Parameters

<id>	Specify the policy ID number.
<subnet>	Specify the HTTP server subnet. Use the format X.X.X.X/<0-32>.
force-nego-ntlm {yes | no}	In the case of negotiated Kerberos and NTLM authentication, specify to force NTLM. Kerberos is less efficient over the WAN, because the client must contact the domain controller to answer the server authentication challenge and tends to be employed on a per-request basis. Riverbed recommends enabling **strip-auth-hdr** with this option. This setting is disabled by default.
obj-pref-table {yes | no}	Specify to enable the Object Prefetch Table, which stores HTTP object prefetches from HTTP GET requests for cascading style sheets, static images, and Java scripts in the Object Prefetch Table. When the browser performs If-Modified-Since (IMS) checks for stored content or sends regular HTTP requests, the client-side Mobile Client responds to these IMS checks and HTTP requests, reducing round trips across the WAN.
gratuitous-401 {yes | no}	Specify to prevent a WAN round trip by issuing the first 401 containing the realm choices from the client-side Steelhead appliance. Riverbed recommends enabling **strip-auth-hdr** along with this option. This option is most effective when the Web server is configured to use per-connection NTLM authentication or per-request Kerberos authentication. If the Web server is configured to use per-connection Kerberos authentication, enabling this option might cause additional delay.
insert-cookie {yes | no}	Specify to add a cookie to HTTP applications that do not already have one. HTTP applications frequently use cookies to monitor sessions. The Mobile Client uses cookies to distinguish one user session from another. If an HTTP application does not use cookies, the Mobile Client inserts one so that it can track requests from the same client. This setting is disabled by default.
insrt-keep-alive {yes | no}	Specify to use the same TCP connection to send and receive multiple HTTP requests and responses, as opposed to opening new ones for every single request and response. Enable this option when using the URL Learning or Parse and Prefetch features with HTTP v1.0 or HTTP v1.1 applications using the Connection Close method. This setting is disabled by default.
parse-prefetch {yes | no}	Specify to allow an unauthenticated connection to serve prefetched objects, as long as the connection belongs to a session whose base connection is already authenticated. This option is most effective when the Web server is configured to use per-connection NTLM or Kerberos authentication.
reuse-ntlm {yes | no}	Specify to allow an unauthenticated connection to serve prefetched objects, as long as the connection belongs to a session whose base connection is already authenticated. This option is most effective when the Web server is configured to use per-connection NTLM or Kerberos authentication.
strip-auth-hdr {yes | no}	Specify to remove all credentials from the request on an already authenticated connection. This works around Internet Explorer behavior that re-authorizes connections that have been previously authorized. This option is most effective when the Web server is configured to use per-connection NTLM authentication. If the Web server is configured to use per-request NTLM authentication, enabling this option might cause authentication failure.

strip-compress {yes | no}	Specify **yes** to enable this feature; specify **no** to disable it. Removes the accept-encoding lines from the HTTP compression header. An accept-encoding directive compresses content rather than using raw HTML. Enabling this option improves the performance of the Mobile Client data-reduction algorithms. This setting is enabled by default.
url-learning {yes | no}	Specify to enable URL Learning, which learns associations between a base URL request and a follow-on request. This parameter stores information about which URLs have been requested and which URLs have generated a 200 OK response from the server. This option fetches the URLs embedded in style sheets or any JavaScript associated with the base page and located on the same host as the base URL. URL Learning works best with content that is not dynamic and does not contain session-specific information. URL Learning is enabled by default. Your system must support cookies and persistent connections to benefit from URL Learning. If your system has cookies turned off and depends on URL rewriting for HTTP state management, or is using HTTP v1.0 (with no keep-alives), you can force the use of cookies by using the Add Cookie option and force the use of persistent connections using the Insert Keep Alive option.

Usage

For detailed information about HTTP optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 http server-subnet 10.10.10.10/24 url-learning no
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id in-path rule auto-discover

Description

Adds an auto-discovery rule to a policy.

Syntax

policy id <id> in-path rule auto-discover [scraddr <subnet>] [dstaddr <subnet>] [dstport <port>] |[optimization {normal | sdr-only | sdr-m |compr-only | none}] | [preoptimization {ssl | none}] | [latency-opt {citrix | http | outlook-anywhr |normal | none}] | [neural-mode {always | dynamic | never | tcphints}] | [wan-visibility {correct | port | full {wan-vis-opt fwd-reset | none}] | [description <description>] | [rulenum <rulenum>]

Parameters

<id>	Specify the policy ID number.
srcaddr <subnet>	Specify the source subnet, in the format XXX.XXX.XXX.XXX/XX.
dstaddr <subnet> dstport <port>	Specify the destination subnet and port. For the subnet address, use the format XXX.XXX.XXX.XXX/XX. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
optimization {normal | sdr-only | sdr-m |compr-only | none}	Specify an optimization policy: • **normal** - The normal optimization policy is the default. The normal process performs LZ compression and SDR. • **sdr-only** - Specify this option to turn off LZ compression. • **sdr-m** - Performs data reduction entirely in memory, which prevents the Mobile Client from reading and writing to and from the disk. Enabling this option can yield high LAN-side throughput, because it eliminates all disk latency. • **compr-only** - Specify this option to turn off SDR but perform LZ compression. • **none** - Specify this option to turn off LZ compression and SDR.
preoptimization {ssl |oracle-forms | oracle-forms+ssl | none}	Specify a preoptimization policy: • **ssl** - Specify to enable SSL preoptimization processing for traffic via SSL secure ports. • **oracle-forms** - Specify oracle-forms to enable preoptimization processing for the Oracle Forms browser plug-in. • **oracle-forms+ssl** - Specify to enable preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side Mobile Client. • **none** - Preoptimization processing is set to **none** by default. If SSL or Oracle Forms preoptimization processing is turned on and you want to turn it off for a port, specify **none**.
latency-opt {citrix | http | normal |outlook-anywhr | none}	Specify a latency-optimization policy: • **citrix** - Always use Citrix optimization on connections matching this rule. Citrix optimizations are ICA/CGP over SSL optimizations. For Citrix latency optimization to work, set the preoptimization policy to the **preoptimization ssl** option. • **http** - Perform HTTP optimization on connections matching this rule. • **normal** - Perform HTTP optimization on ports 80, 8080, and (with SSL preoptimization) 443. This is the default setting. • **outlook-anywhr** - Always use Outlook-Anywhere optimization on the connection. • **none** - Do not perform latency optimization on connections matching this rule.

neural-mode {always | dynamic | never | tcphints}	Enables neural framing in the Mobile Client. Enabling neural framing makes your WAN more efficient by gathering data to select the optimal packet framing boundaries for SDR. If you specify a neural mode, your network experiences a trade-off between the compression and SDR performance, and the latency added to the connection. For different types of traffic, one algorithm might be better than others. Specify one of the following modes: • **always** - Always use the Nagle algorithm. This is the default setting (always wait 6 ms). All data is passed to the codec, which attempts to coalesce consume calls (if needed) to achieve better fingerprinting. A timer (6 ms) backs it up and causes leftover data to be consumed. Neural heuristics are computed in this mode but are not used. • **dynamic** - Dynamically adjust the Nagle parameters. The Mobile Client picks the best algorithm to use by learning which algorithm is best and adapting if the traffic characteristic changes. • **never** - Never use the Nagle algorithm. All the data is immediately encoded without waiting for timers to fire or application buffers to fill past a specified threshold. Neural heuristics are computed in this mode but are not used. • **tcphints** - Base setting on TCP hints. If data is received from a partial frame packet or a packet with the TCP PUSH flag set, the encoder encodes the data instead of immediately coalescing it. Neural heuristics are computed in this mode but are not used. To configure neural framing for an FTP data channel, define an in-path rule with the destination port 20 and set its optimization policy. To configure neural framing for a MAPI connection, define an in-path rule with the destination port 7830 and set its optimization policy.

wan-visibility {correct | port |full [wan-vis-opt fwd-reset | none]}	Enables WAN visibility, which pertains to how packets traversing the WAN are addressed. There are three types of WAN visibility modes: correct addressing, port transparency, and full address transparency. You configure WAN visibility on the client-side Mobile Client (where the connection is initiated). The server-side Steelhead appliance must also support WAN visibility. • **correct** - Turns WAN visibility off. Correct addressing uses Mobile Client IP addresses and port numbers in the TCP/IP packet header fields for optimized traffic in both directions across the WAN. This is the default setting. • **port** - Preserves your server port numbers in the TCP/IP header fields, for optimized traffic in both directions across the WAN. Traffic is optimized, while the server port number in the TCP/IP header field appears to be unchanged. Routers and network monitoring devices deployed in the WAN segment between the communicating Mobile Clients can view these preserved fields. Use port transparency if you want to manage and enforce QoS policies that are based on destination ports. If your WAN router is following traffic classification rules written in terms of client and network addresses, port transparency enables your routers to use existing rules to classify the traffic without any changes. Port transparency enables network analyzers deployed within the WAN to monitor network activity and to capture statistics for reporting by inspecting traffic according to its original TCP port number. Port transparency does not require dedicated port configurations on your Mobile Clients. **Note:** Port transparency provides only server port visibility. It does not provide client and server IP address visibility, nor does it provide client port visibility. • **full** - Preserves your client and server IP addresses and port numbers in the TCP/IP header fields for optimized traffic, in both directions across the WAN. It also preserves VLAN tags. Traffic is optimized, while these TCP/IP header fields appear to be unchanged. Routers and network monitoring devices deployed in the WAN segment between the communicating Mobile Clients can view these preserved fields. If both port transparency and full address transparency are acceptable solutions, port transparency is preferable. Port transparency avoids potential networking risks that are inherent to enabling full address transparency. For details, see the *Steelhead Appliance Deployment Guide*. However, if you must see your client or server IP addresses across the WAN, full transparency is your only configuration option.
description <description>	Specify a description of the rule.
rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**. The rule is inserted into the list at the specified position. For example, if you specify **rulenum** as **3**, the new rule will be #3, the old rule #3 becomes #4, and subsequent rules, if any, also move down the list. Specify **start** for the rule to be the first rule and **end** for the rule to be the last rule. If you do not specify a rule number, the rule is added to the end of the list.

Usage

For detailed information about in-path rules, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 in-path rule auto-discover srcaddr 10.10.10.1/24 port 2121 dstaddr
10.24.24.24.1/24 rulenum 2
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id in-path rule deny

Description

Adds an in-path rule that rejects connection requests on the specified policy.

Syntax

[no] policy id <id> in-path rule deny [scraddr <subnet>] [dstaddr <subnet>] [dstport <port>] | [rulenum <rulenum>] | [description <description>]

Parameters

<id>	Specify the policy ID number.
srcaddr <subnet>	Specify the source subnet for this rule: for example, 1.2.3.4/32
dstaddr <subnet> **dstport <port>**	Specify the destination subnet and port for this rule. For the subnet address, use the format XXX.XXX.XXX.XXX/XX. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**. The rule is inserted into the list at the specified position. For example, if you specify **rulenum** as 3, the new rule will be #3, the old rule #3 becomes #4, and subsequent rules, if any, also move down the list. Specify start for the rule to be the first rule and end for the rule to be the last rule. If you do not specify a rule number, the rule is added to the end of the list.
description <description>	Specify a description of the rule.

Usage

The Mobile Client automatically intercepts traffic on all IP addresses (**0.0.0.0**) and ports (**all**) and optimizes according to default settings.

Specify deny rules for traffic you want to reject and return a message to the client that the request has been denied.

The **no** command option disables the rule. The **no** command option syntax is **no in-path rule <rulenum>.**

For detailed information about in-path rules, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 in-path rule deny srcaddr 10.0.0.1/24 dstaddr 10.0.0.2/24 rulenum
5 description test
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id in-path rule discard

Description

Adds an in-path rule that drops connections on the specified policy.

Syntax

[no] policy id <id> in-path rule discard [scraddr <subnet>] [dstaddr <subnet>] [dstport <port>] | [rulenum <rulenum>] | [description <description>]

Parameters

<id>	Specify the policy ID number.
srcaddr <subnet>	Specify the source subnet for this rule, in the format XXX.XXX.XXX.XXX/XX.
dstaddr <subnet> **dstport <port>**	Specify the destination subnet and port for this rule. For the subnet address, use the format XXX.XXX.XXX.XXX/XX. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**. The rule is inserted into the list at the specified position. For example, if you specify **rulenum** as 3, the new rule will be #3, the old rule #3 becomes #4, and subsequent rules, if any, also move down the list. Specify start for the rule to be the first rule and end for the rule to be the last rule. If you do not specify a rule number, the rule is added to the end of the list.
description <description>	Specify a description of the rule.

Usage

The Mobile Client automatically intercepts traffic on all IP addresses (**0.0.0.0**) and ports (**all**) and optimizes according to default settings.

Specify discard rules for traffic that you want to drop silently instead of optimizing or passing through.

The **no** command option disables the rule. The **no** command option has the following syntax, **no in-path rule <rulenum>.**

For detailed information about in-path rules, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 in-path rule discard srcaddr 10.0.0.2/24 dstaddr 10.0.0.1/24 port
1234 rulenum 2
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id in-path rule edit rulenum auto-discover

Description

Edits an auto-discovery rule on the specified policy.

Use the auto-discovery process to determine if a remote Mobile Client is able to optimize the connection attempting to be created by this SYN packet. By default, auto-discovery is applied to all IP addresses and ports that are not secure, interactive, or default Riverbed ports. Defining in-path rules modifies this default setting.

Syntax

policy id <id> in-path rule edit rulenum <rulenum> auto-discover [scraddr <subnet>] [dstaddr <subnet>] [dstport <port>] [preoptimization {ssl | oracle-forms+ssl | oracle-forms | none}] [optimization {normal | sdr-only | compr-only | none}] [latency-opt {http | outlook-anywhr | normal | none}] [neural-mode {always | dynamic | never | tcphints}] [wan-visibility correct | port | full {wan-vis-opt fwd-reset | none}] | [description <description>] | [rule-enable {true | false}]

Parameters

<id>	Specify the policy ID number.
rulenum <rulenum>	Specify the rule number to edit: **1-N** or **start** or **end**.
srcaddr <subnet>	Specify the source subnet in the format XXX.XXX.XXX.XXX/XX.
dstaddr <subnet> dstport <port>	Specify the destination subnet and port. For the subnet address, use the format XXX.XXX.XXX.XXX/XX. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
optimization {normal | sdr-only | sdr-m |compr-only | none}	Specify an optimization policy: • **normal** - The **normal** optimization policy is the default. The normal process performs LZ compression and SDR. • **sdr-only** - Specify this option to turn off LZ compression. • **sdr-m** - Performs data reduction entirely in memory, which prevents the Mobile Client from reading and writing to and from the disk. Enabling this option can yield high LAN-side throughput, because it eliminates all disk latency. • **compr-only** - Specify this option to turn off SDR but perform LZ compression. • **none** - Specify this option to turn off LZ compression and SDR.
preoptimization {ssl |oracle-forms | oracle-forms+ssl | none}	Specify a preoptimization policy: • **ssl** - Specify **ssl** to enable SSL preoptimization processing for traffic via SSL secure ports. • **oracle-forms** - Specify **oracle-forms** to enable preoptimization processing for the Oracle Forms browser plug-in. • **oracle-forms+ssl** - Specify to enable preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side Mobile Client. • **none** - Preoptimization processing is set to **none** by default. If SSL or Oracle Forms preoptimization processing is turned on and you want to turn it off for a port, specify **none**.
latency-opt {citrix | http | normal |outlook-anywhr | none}	Specify a latency-optimization policy: • **citrix** - Always use Citrix optimization on connections matching this rule. Citrix optimizations are ICA/CGP over SSL optimizations. For Citrix latency optimization to work, set the preoptimization policy to the **preoptimization ssl** option. • **http** - Perform HTTP optimization on connections matching this rule. • **normal** - Perform HTTP optimization on ports 80, 8080, and (with SSL preoptimization) 443. This is the default setting. • **outlook-anywhr** - Always use Outlook-Anywhere optimization on the connection. • **none** - Do not perform latency optimization on connections matching this rule.

neural-mode {**always** | **dynamic** | **never** | **tcphints**}	Enables neural framing in the Mobile Client. Enabling neural framing makes your WAN more efficient by gathering data to select the optimal packet framing boundaries for SDR. If you specify a neural mode, your network experiences a trade-off between the compression and SDR performance, and the latency added to the connection. For different types of traffic, one algorithm might be better than others. Specify one of the following modes: • **always** - Always use the Nagle algorithm. This is the default setting (always wait 6 ms). All data is passed to the codec, which attempts to coalesce consume calls (if needed) to achieve better fingerprinting. A timer (6 ms) backs it up and causes leftover data to be consumed. Neural heuristics are computed in this mode but are not used. • **dynamic** - Dynamically adjust the Nagle parameters. The Mobile Client picks the best algorithm to use by learning, which algorithm is best and adapting if the traffic characteristic changes. • **never** - Never use the Nagle algorithm. All the data is immediately encoded without waiting for timers to fire or application buffers to fill past a specified threshold. Neural heuristics are computed in this mode but are not used. • **tcphints** - Base setting on TCP hints. If data is received from a partial frame packet or a packet with the TCP PUSH flag set, the encoder encodes the data instead of immediately coalescing it. Neural heuristics are computed in this mode but are not used. To configure neural framing for an FTP data channel, define an in-path rule with the destination port 20 and set its optimization policy. To configure neural framing for a MAPI connection, define an in-path rule with the destination port 7830 and set its optimization policy.

wan-visibility {correct | port |full [wan-vis-opt fwd-reset | none]}	Enables WAN visibility, which pertains to how packets traversing the WAN are addressed. There are three types of WAN visibility modes: correct addressing, port transparency, and full address transparency. You configure WAN visibility on the client-side Mobile Client (where the connection is initiated). The server-side Steelhead appliance must also support WAN visibility. • **correct** - Turns WAN visibility off. Correct addressing uses Mobile Client IP addresses and port numbers in the TCP/IP packet header fields for optimized traffic in both directions across the WAN. This is the default setting. • **port** - Preserves your server port numbers in the TCP/IP header fields for optimized traffic, in both directions across the WAN. Traffic is optimized while the server port number in the TCP/IP header field appears to be unchanged. Routers and network monitoring devices deployed in the WAN segment between the communicating Mobile Clients can view these preserved fields. Use port transparency if you want to manage and enforce QoS policies that are based on destination ports. If your WAN router is following traffic classification rules written in terms of client and network addresses, port transparency enables your routers to use existing rules to classify the traffic without any changes. Port transparency enables network analyzers deployed within the WAN to monitor network activity and to capture statistics for reporting by inspecting traffic according to its original TCP port number. Port transparency does not require dedicated port configurations on your Mobile Clients. **Note:** Port transparency provides only server port visibility. It does not provide client and server IP address visibility, nor does it provide client port visibility. • **full** - Preserves your client and server IP addresses and port numbers in the TCP/IP header fields for optimized traffic, in both directions across the WAN. It also preserves VLAN tags. Traffic is optimized, while these TCP/IP header fields appear to be unchanged. Routers and network monitoring devices deployed in the WAN segment between the communicating Mobile Clients can view these preserved fields. If both port transparency and full address transparency are acceptable solutions, port transparency is preferable. Port transparency avoids potential networking risks that are inherent to enabling full address transparency. For details, see the *Steelhead Appliance Deployment Guide*. However, if you must see your client or server IP addresses across the WAN, full transparency is your only configuration option. If you specify **full**, further specify one of the following options: • **wan-vis-opt fwd-reset** - Enables full address transparency and also sends a reset between the probe response and inner SYN. The reset ensures that the packet header uses the same IP address and port numbers as the initial client and server connection. Because the reset creates a fresh inner connection, you can use full transparency in systems with firewalls that perform stateful packet inspection to track the connection state. • **none** - Specify to set the WAN visibility option to none. **Important:** Enabling full address transparency requires symmetrical traffic flows between the client and server. Should any asymmetry exist on the network, enabling full address transparency might yield unexpected results, up to and including loss of connectivity. For detailed information about how to configure WAN visibility, see the *Steelhead Appliance Management Console User's Guide* and the *.
description <description>	Specify a description of the rule.

Usage

The **in-path rule auto-discover** command adds an auto-discovery rule.

When you edit a rule of the same type (for example, **in-path rule auto-discover** to **in-path rule edit auto-discover**), the parameters you specify in the edit command are applied and the other parameters remain the same as the default value or the previously configured value of the **in-path rule auto-discover** command. However, if you change the rule type (for example, **in-path rule auto-discover** to **in-path rule edit fixed-target**), the parameters you specify in the edit command are applied and the rest of the parameters are reset to the default of the new rule type (in this example, resets to in-path fixed-target rules).

For detailed information about in-path rules, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 in-path rule edit rulenum 2-3 auto-discover srcaddr 10.0.0.1/24
dstaddr 10.0.0.2/24 preoptimization ssl optimization normal latency-opt http neural-mode always wan-
visibility correct
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id in-path rule edit rulenum deny

Description

Edits an in-path rule that rejects connection requests on the specified policy.

Syntax

policy id <id> in-path rule edit rulenum <rulenum> deny [scraddr <subnet>] [dstaddr <subnet>] [dstport <port>] | [description <description>] [rule-enable {true | false}]

Parameters

<id>	Specify the policy ID number.
rulenum <rulenum>	Specify the rule number to edit: **1-N** or **start** or **end**.
srcaddr <subnet>	Specify the source subnet for this rule: for example, **1.2.3.4/32**
dstaddr <subnet> **dstport <port>**	Specify the destination subnet and port for this rule. For the subnet address, use the format XXX.XXX.XXX.XXX/XX. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
description <description>	Specify a description of the rule.
rule-enable [true | false]	Enables or disables an in-path rule. Specify **true** to enable this rule, **false** to disable this rule.

Usage

Use the **policy id in-path edit rulenum deny** command to edit an in-path rule that rejects connection requests.

For detailed information about in-path rules, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 in-path edit rulenum 2-3 deny srcaddr 10.0.0.1/24 dstaddr 10.0.0.2/
24 rule-enable true
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id in-path rule edit rulenum discard

Description

Edits an in-path rule that drops connections on the specified policy.

Syntax

[no] policy id <id> in-path rule edit rulenum <rulenum> discard [scraddr <subnet>] [dstaddr <subnet>] [dstport <port>] | [description <description>] [rule-enable {true | false}]

Parameters

<id>	Specify the policy ID number.
rulenum <rulenum>	Specify the rule number to edit: **1-N** or **start** or **end**.
srcaddr <subnet>	Specify the source subnet, for this rule in the format XXX.XXX.XXX.XXX/XX.
dstaddr <subnet> **dstport <port>**	Specify the destination subnet and port for this rule. For the subnet address,, use the format XXX.XXX.XXX.XXX/XX. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
description <description>	Specify a description of the rule.
rule-enable [true | false]	Enables or disables an in-path rule. Specify **true** to enable this rule, **false** to disable this rule.

Usage

Use the **in-path rule discard** command to add an in-path rule that drops connections.

For detailed information about in-path rules, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 in-path rule edit rulenum 2 discard srcaddr 10.0.0.1/24 dstaddr
10.0.0.2/24 description example rule-enable true
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id in-path rule edit rulenum enable

Description

Enables a single in-path rule on the specified policy.

Syntax

policy id <id> in-path rule edit rulenum <rule number> enable

Parameters

<id>	Specify the policy ID number.
rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**.

Usage

For detailed information about in-path rules, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 in-path rule edit rulenum 3 enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id in-path rule edit rulenum fixed-target

Description

Edits a fixed-target in-path rule on the specified policy.

Syntax

policy acceleration id <id> in-path rule edit rulenum <rulenum> fixed-target [target-addr <addr>] [target-port <port>] [dstaddr <subnet>] [dstport <port>] [scraddr <subnet>] | [backup-addr <addr>] [backup-port <port>] | [optimization {normal | sdr-only |sdr-m | compr-only | none}] | [preoptimization {ssl |oracle-forms |oracle-forms+ssl | none}] | [latency-opt {citrix | http | normal| outlook-anywhr | none}] | [neural-mode {always | dynamic | never | tcphints}] | [description <description>] | rule-enable [true | false]

Parameters

<id>	Specify an existing policy on the local Mobile Controller.
rulenum <rulenum>	Specify the rule number to edit: 1-N or start or end.
target-addr <addr> target-port <port>	Specify the fixed-target appliance address. For the network address, use the format XXX.XXX.XXX.XXX. For the port, you can specify a single port (number), a port label, or all to specify all ports.
backup-addr <addr> backup-port <port>	Specify a backup appliance for this rule (if any). For the network address, use the format XXX.XXX.XXX.XXX. For the port, you can specify a single port (number), a port label, or all to specify all ports.
dstaddr <subnet> dstport <port>	Specify the destination subnet and port. For the subnet address,, use the format XXX.XXX.XXX.XXX/XX. For the port, you can specify a single port (number), a port label, or all to specify all ports.
srcaddr <subnet>	Specify the source subnet,: for example, 1.2.3.4/32
optimization {normal | sdr-only | sdr-m | compr-only | none}	Specify an optimization policy: • **normal** - The **normal** optimization policy is the default. The normal process performs LZ compression and SDR. • **sdr-only -** Specify this option to turn off LZ compression. • **sdr-m -** Performs data reduction entirely in memory, which prevents the Mobile Client from reading and writing to and from the disk. Enabling this option can yield high LAN-side throughput, because it eliminates all disk latency. • **compr-only** - Specify this option to turn off SDR but perform LZ compression. • **none -** Specify this option to turn off LZ compression and SDR.
preoptimization {ssl |oracle-forms | oracle-forms+ssl | none}	Specify a preoptimization policy: • **ssl** - Specify **ssl** to enable SSL preoptimization processing for traffic via SSL secure ports. • **oracle-forms** - Specify **oracle-forms** to enable preoptimization processing for the Oracle Forms browser plug-in. • **oracle-forms+ssl** - Specify to enable preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side Mobile Client. • **none** - Preoptimization processing is set to **none** by default. If SSL or Oracle Forms preoptimization processing is turned on and you want to turn it off for a port, specify **none**.
latency-opt {citrix | http | normal |outlook-anywhr | none}	Specify a latency-optimization policy: • **citrix** - Always use Citrix optimization on connections matching this rule. Citrix optimizations are ICA/CGP over SSL optimizations. For Citrix latency optimization to work, set the preoptimization policy to the **preoptimization ssl** option. • **http** - Perform HTTP optimization on connections matching this rule. • **normal** - Perform HTTP optimization on ports 80, 8080, and (with SSL preoptimization) 443. This is the default setting. • **outlook-anywhr** - Always use Outlook Anywhere optimization on the connection. • **none** - Do not perform latency optimization on connections matching this rule.

neural-mode {always | dynamic | never | tcphints}	Enables neural framing in the Mobile Client. Enabling neural framing makes your WAN more efficient by gathering data to select the optimal packet framing boundaries for SDR. If you specify a neural mode, your network will experience a trade-off between the compression and SDR performance, and the latency added to the connection. For different types of traffic, one algorithm might be better than others. Specify one of the following modes: • **always -** Always use the Nagle algorithm. This is the default setting (always wait 6 ms). All data is passed to the codec, which attempts to coalesce consume calls (if needed) to achieve better fingerprinting. A timer (6 ms) backs it up and causes leftover data to be consumed. Neural heuristics are computed in this mode but are not used. • **dynamic -** Dynamically adjust the Nagle parameters. The Mobile Client picks the best algorithm to use by learning, which algorithm is best and adapting if the traffic characteristic changes. • **never -** Never use the Nagle algorithm. All the data is immediately encoded without waiting for timers to fire or application buffers to fill past a specified threshold. Neural heuristics are computed in this mode but are not used. • **tcphints -** Base setting on TCP hints. If data is received from a partial frame packet or a packet with the TCP PUSH flag set, the encoder encodes the data instead of immediately coalescing it. Neural heuristics are computed in this mode but are not used. To configure neural framing for an FTP data channel, define an in-path rule with the destination port 20 and set its optimization policy. To configure neural framing for a MAPI connection, define an in-path rule with the destination port 7830 and set its optimization policy.
description <description>	Specify a description of the rule.
rule-enable [true | false]	Enables or disables an in-path rule. Specify **true** to enable this rule, **false** to disable this rule.

Usage

The **in-path rule fixed-target** command adds a fixed-target in-path rule.

When you edit a rule of the same type (for example, **in-path rule fixed-target** to **in-path rule edit fixed-target**), the parameters you specify in the edit command are applied and the other parameters remain the same as the default value or the previously configured value of the **in-path rule fixed-target** command. However, if you change the rule type (for example, **in-path rule fixed-target** to **in-path rule edit auto-discover**), the parameters you specify in the edit command are applied and the rest of the parameters are reset to the default of the new rule type (in this example, resets to in-path auto-discover rules).

For detailed information about in-path rules, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 in-path rule edit rulenum 1 fixed-target srcaddr 10.0.0.1/24 rule-
enable true
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id in-path rule edit pass-through

Description

Edits a pass-through in-path rule on the specified policy.

Syntax

[no] policy id <id> in-path rule edit rulenum <rulenum> pass-through [scraddr <subnet>] [dstaddr <subnet> dstport <port>] | [description <description>]

Parameters

<id>	Specify the policy ID number.
rulenum <rulenum>	Specify the rule number to edit: 1-N or start or end.
srcaddr <subnet>	Specify the source subnet, for this rule, for example, 1.2.3.4/32.
dstaddr <subnet> dstport <port>	Specify the destination subnet and port. For the subnet address,, use the format XXX.XXX.XXX.XXX/XX. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
description <description>	Specify a description of the rule.

Usage

Use the **in-path rule pass-through** command to add a pass-through in-path rule.
For detailed information about in-path rules, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 in-path rule edit rulenum 25 pass-through srcaddr 10.10.10.1/24
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id in-path rule fixed-target

Description

Adds a fixed-target in-path rule on the specified policy.

Syntax

[no] policy id <id> in-path rule fixed-target [target-addr <addr>] [target-port <port>] [dstaddr <subnet>] [dstport <port>] [scraddr <subnet>] | [backup-addr <addr>] [backup-port <port>] | [optimization {normal | sdr-only |sdr-m | compr-only | none}] | [preoptimization {ssl |oracle-forms | oracle-forms+ssl |none}] | [latency-opt {citrix | http | normal| outlook-anywhr | none}] | [neural-mode {always | dynamic | never | tcphints}] | [description <description>] | rule-enable [true | false] | [rulenum <rulenum>]

Parameters

<id>	Specify the policy ID number.
target-addr <addr> target-port <port>	Specify the fixed target appliance address. For the network address, use the format XXX.XXX.XXX.XXX. For the port, you can specify a single port (number), a port label, or all to specify all ports.
backup-addr <addr> backup-port <port>	Specify a backup appliance for this rule (if any). For the network address, use the format XXX.XXX.XXX.XXX. For the port, you can specify a single port (number), a port label, or all to specify all ports.
dstaddr <subnet> dstport <port>	Specify the destination subnet and port. For the subnet address, use the format XXX.XXX.XXX.XXX/XX. For the port, you can specify a single port (number), a port label, or all to specify all ports.
srcaddr <subnet>	Specify the source subnet, for example, 1.2.3.4/32.
optimization {normal | sdr-only | sdr-m | compr-only | none}	Specify an optimization policy: • **normal** - The **normal** optimization policy is the default. The normal process performs LZ compression and SDR. • **sdr-only -** Specify this option to turn off LZ compression. • **sdr-m -** Performs data reduction entirely in memory, which prevents the Mobile Client from reading and writing to and from the disk. Enabling this option can yield high LAN-side throughput, because it eliminates all disk latency. • **compr-only** - Specify this option to turn off SDR but perform LZ compression. • **none -** Specify this option to turn off LZ compression and SDR.
preoptimization {ssl |oracle-forms | oracle-forms+ssl | none}	Specify a preoptimization policy: • **ssl** - Specify **ssl** to enable SSL preoptimization processing for traffic via SSL secure ports. • **oracle-forms** - Specify **oracle-forms** to enable preoptimization processing for the Oracle Forms browser plug-in. • **oracle-forms+ssl** - Specify to enable preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side Mobile Client. • **none** - Preoptimization processing is set to none by default. If SSL or Oracle Forms preoptimization processing is turned on and you want to turn it off for a port, specify none.
latency-opt {citrix | http | normal |outlook-anywhr | none}	Specify a latency-optimization policy: • **citrix** - Always use Citrix optimization on connections matching this rule. Citrix optimizations are ICA/CGP over SSL optimizations. For Citrix latency optimization to work, set the preoptimization policy to the **preoptimization ssl** option. • **http** - Perform HTTP optimization on connections matching this rule. • **normal** - Perform HTTP optimization on ports 80, 8080, and (with SSL preoptimization) 443. This is the default setting. • **outlook-anywhr** - Always use Outlook Anywhere optimization on the connection. • **none** - Do not perform latency optimization on connections matching this rule.

neural-mode {always | dynamic | never | tcphints}	Enables neural framing in the Mobile Client. Enabling neural framing makes your WAN more efficient by gathering data to select the optimal packet framing boundaries for SDR. If you specify a neural mode, your network will experience a trade-off between the compression and SDR performance, and the latency added to the connection. For different types of traffic, one algorithm might be better than others. Specify one of the following modes: • **always -** Always use the Nagle algorithm. This is the default setting (always wait 6 ms). All data is passed to the codec, which attempts to coalesce consume calls (if needed) to achieve better fingerprinting. A timer (6 ms) backs it up and causes leftover data to be consumed. Neural heuristics are computed in this mode but are not used. • **dynamic -** Dynamically adjust the Nagle parameters. The Mobile Client picks the best algorithm to use by learning, which algorithm is best and adapting if the traffic characteristic changes. • **never -** Never use the Nagle algorithm. All the data is immediately encoded without waiting for timers to fire or application buffers to fill past a specified threshold. Neural heuristics are computed in this mode but are not used. • **tcphints -** Base setting on TCP hints. If data is received from a partial frame packet or a packet with the TCP PUSH flag set, the encoder encodes the data instead of immediately coalescing it. Neural heuristics are computed in this mode but are not used. To configure neural framing for an FTP data channel, define an in-path rule with the destination port 20 and set its optimization policy. To configure neural framing for a MAPI connection, define an in-path rule with the destination port 7830 and set its optimization policy.
description <description>	Specify a description of the rule.
rule-enable [true | false]	Enables or disables an in-path rule. Specify **true** to enable this rule, **false** to disable this rule.
rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**. The rule is inserted into the list at the specified position. For example, if you specify **rulenum** as **3**, the new rule will be #3, the old rule #3 becomes #4, and subsequent rules, if any, also move down the list. Specify **start** for the rule to be the first rule and **end** for the rule to be the last rule. If you do not specify a rule number, the rule is added to the end of the list.

Usage

Defining a fixed-target rule uses a specified remote Steelhead appliance as an optimization peer.

You must specify at least one remote target Steelhead appliance to optimize (and, optionally, which ports and backup Steelhead appliances), and add rules to specify the network of servers, ports, port labels, and out-of-path Steelhead appliances to use.

The Mobile Client automatically intercepts traffic on all IP addresses (**0.0.0.0**) and ports (**all**) and optimizes according to default settings.

Specify fixed-target rules to set out-of-path Mobile Clients near the target server that you want to optimize.

For detailed information about in-path rules, see the *Steelhead Appliance Management Console User's Guide*.

The **no** command option disables the rule. The **no** command option has the following syntax, **no in-path rule <rulenum>.**

Example

```
amnesiac (config) # policy id 1 in-path rule fixed-target srcaddr 10.0.0.1/24 optimization sdr-only
rulenum 1 rule-enable true
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id in-path rule move

Description

Moves an in-path rule in the rule list on the specified policy.

Syntax

policy id <id> in-path rule move rulenum <rulenum> to <rulenum>

Parameters

<id>	Specify the policy ID number.
<rulenum>	Specify the rule number or **start** or **end**.

Usage

For detailed information about in-path rules, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 in-path rule move rulenum 2 to 1
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id in-path rule pass-through

Description

Adds a pass-through in-path rule on the specified policy. Allows the SYN packet to pass through the Mobile Client unoptimized. No optimization is performed on the TCP connection initiated by this SYN packet. You define pass-through rules to exclude subnets from optimization. Traffic is also passed through when the Mobile Client is in bypass mode. (Pass through of traffic might occur because of in-path rules or because the connection was established before the Mobile Client was put in place or before the Mobile Client service was enabled.)

Syntax

[no] policy id <id> in-path rule pass-through [scraddr <subnet>] [dstaddr <subnet> dstport <port>] | [rulenum <rulenum>] | [description <description>]

Parameters

<id>	Specify the policy ID number.
srcaddr <subnet>	Specify the source subnet for this rule: for example, **1.2.3.4/32**
dstaddr <subnet> dstport <port>	Specify the destination subnet and port. For the subnet address, use the format XXX.XXX.XXX.XXX/XX. For the port, you can specify a single port (number), a port label, or **all** to specify all ports.
rulenum <rulenum>	Specify the order in which the rule is consulted: **1-N** or **start** or **end**. The rule is inserted into the list at the specified position. For example, if you specify **rulenum** as 3, the new rule will be 3, the old rule 3 becomes 4, and subsequent rules also move down the list. Specify **start** for the rule to be the first rule and **end** for the rule to be the last rule. If you do not specify a rule number, the rule is added to the end of the list.
description <description>	Specify a description of the rule.

Usage

The Mobile Client automatically intercepts traffic on all IP addresses (**0.0.0.0**) and ports (**all**) and optimizes according to default settings.

Specify pass-through rules for traffic that you want to pass through to its destination without optimization by the Riverbed system.

The **no** command option disables the rule. The **no** command option has the following syntax, **no in-path rule <rulenum>.**

For detailed information about in-path rules, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # in-path rule pass-through srcaddr 10.10.10.1 rulenum 25
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id mapi enable

Description

Enables MAPI optimization and features on the specified policy.

Syntax

[no] policy id <id> mapi enable

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option disables MAPI optimization settings.

For detailed information about MAPI optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 mapi enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id mapi encrypted enable

Description

Enables MAPI Exchange encrypted optimization settings on the specified policy.

Syntax

[no] policy id <id> mapi encrypted enable

Parameters

<id>	Specify the ID number.

Usage

The **no** command option disables MAPI optimization settings.

For detailed information about MAPI optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # no policy id 1 mapi encrypted enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id mapi mac enable

Description

Enables MAPI Exchange MAC settings on the specified policy.

Syntax

[no] policy id <id> mapi mac enable

Parameters

<id>	Specify the ID number.

Usage

The **no** command option disables MAPI optimization settings.

For detailed information about MAPI optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # no policy id 1 mapi mac enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id mapi outlook-anywhr auto-detect

Description

Enables Outlook Anywhere auto-detection on the specified policy.

Syntax

[no] policy id <id> protocol mapi outlook-anywhr auto-detect

Parameters

<id>	Specify the policy ID number.

Usage

For detailed information about the Outlook Anywhere auto-detection, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 mapi outlook-anywhr auto-detect
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id mapi outlook-anywhr enable

Description

Enables Outlook Anywhere optimization on the specified policy.

Syntax

[no] policy id <id> mapi outlook-anywhr enable

Parameters

<id>	Specify the policy ID number.

Usage

Enables Outlook Anywhere latency optimization. Outlook Anywhere is a feature of Microsoft Exchange Server 2007 and 2010 that allows Microsoft Office Outlook 2003, 2007, and 2010 clients to connect to their Exchange servers over the Internet using the RPC over HTTP(S) Windows networking component. By default, this feature is disabled.

To use this feature, you must also enable HTTP Optimization. If you are using Outlook Anywhere over HTTPS, you must enable the secure inner channel, and the Microsoft Internet Information Server (IIS) SSL certificate must be installed on the server-side Mobile Client.

For detailed information about Outlook Anywhere, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 mapi outlook-anywhr enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id mapi port-remap enable

Description

Enables MAPI port remapping.

Syntax

[no] policy id <id> mapi port-remap enable

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option disables the port remapping feature.

For detailed information about the MAPI optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 mapi port-remap enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id nfs enable

Description

Enables the NFS protocol settings on the specified policy.

Syntax

[no] policy id <id> nfs enable

Parameters

<id>	Specify the policy ID number.

Usage

The NFS optimizer provides latency optimization improvements for NFS operations primarily by prefetching data, storing it on the client Mobile Client for a short amount of time, and using it to respond to client requests.

The **no** command option disables the NFS optimizer.

For detailed information about the NFS protocol settings, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 nfs enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id notes enable

Description

Enables Lotus Notes optimization.

Syntax

[no] policy id <id> notes enable

Parameters

<id>	Specify the policy on the Mobile Controller.

Usage

The **no** command option disables Lotus Notes optimization.

For detailed information about the Lotus Notes optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 notes enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id notes port

Description

Configures a port for Lotus Notes optimization.

Syntax

[no] policy id <id> notes port

Parameters

<id>	Specify the policy on the Mobile Controller.
<port>	Specify the port number.

Usage

The **no** command option disables the Lotus Notes port for optimization.

For detailed information about the Lotus Notes optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 notes port 1234
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id oracle-forms enable

Description

Configures preoptimization processing for the Oracle Forms browser plug-in.

Syntax

[no] policy id <id> oracle-forms enable

Parameters

<id>	Specify the policy on the Mobile Controller.

Usage

The **no** command option disables Oracle Forms optimization.

For detailed information about the Oracle Forms optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 oracle-forms enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id probe-tcp-opt

Description

Configures the TCP probing option for optimization.

Syntax

[no] policy id <id> probe-tcp-opt <probe tcp option value>

Parameters

<id>	Specify the policy on the Mobile Controller.
<probe tcp option value>	Specify the TCP probe value.

Usage

The **no** command option disables TCP optimization.

For detailed information about TCP probing, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 probe-tcp-opt 2
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id smb2 enable

Description

Enables optimization of SMB2 traffic for native SMB2 clients and servers on the specified policy. SMB2 allows access across disparate networks. It is the default mode of communication between Windows Vista and Windows 7 clients and Windows Server 2008 and Windows Server 2008r2 servers.

Syntax

[no] policy id <id> smb2 enable

Parameters

<id>	Specify the policy on the Mobile Controller.

Usage

For detailed information about SMB2 optimization, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 smb2 enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id ssl backend no-byp-hs-fail

Description

Configures the SSL backend server to bypass the connection if the handshake fails.

Syntax

[no] policy id <id> ssl backend no-byp-hs-fail

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option disables the SSL bypass feature.

For detailed information about SSL, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 ssl backend no-byp-hs-fail
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id ssl enable

Description

Configures SSL for the policy.

Syntax

[no] policy id <id> ssl enable

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option disables SSL support.

For detailed information about SSL, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 ssl enable
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id ssl fallback-no-enc

Description

Configures fallback to no encryption on the inner channel.

Syntax

[no] policy id <id> ssl fallback-no-enc

Parameters

<id>	Specify the policy ID number.

Usage

Specifies that the system optimizes but does not encrypt the connection when it is unable to negotiate a secure, encrypted inner channel connection with the peer. This is the default setting.

Enabling this option requires an optimization service restart.

Riverbed strongly recommends enabling this setting on both the Mobile Client and the server-side Steelhead appliances.

This option applies only to non-SSL traffic and is unavailable when you select s**sl-only** as the traffic type in the **policy id ssl traffic-type** command.

The **no policy id <id> ssl fallback-no-enc enable** command configures the system to not trust all preconfigured peering certificates.

Disable this setting to pass through connections that do not have a secure encrypted inner channel connection with the peer. Use caution when disabling this setting, because doing so specifies that you strictly do not want traffic optimized between non-secure systems. Consequently, when this setting is disabled, connections might be dropped.

For detailed information about SSL, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 ssl fallback-no-enc
amnesiac (config) # service restart
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id ssl sfe-mode

Description

Configures SSL safe mode.

Syntax

[no] policy id <id> ssl sfe-mode

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option resets SSL safe mode.

For detailed information about SSL, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 ssl sfe-mode
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id ssl traffic-type

Description

Configures the SSL traffic type for the policy.

Syntax

[no] policy id <id> ssl traffic-type [ssl-only | ssl-and-secure-protocols | all]

Parameters

<id>	Specify the policy ID number.
<type>	Specify one of the following traffic types: • **ssl-only** - The Mobile Client and the server-side Steelhead appliance authenticate each other and then encrypt and optimize all SSL traffic; for example, HTTPS traffic on port 443. This is the default setting. • **ssl-and-secure-protocols** - The Mobile Client and the server-side Steelhead appliance authenticate each other and then encrypt and optimize all traffic traveling over the following secure protocols: Citrix, SSL, SMB-signed, and encrypted MAPI. SMB-signing, MAPI encryption, or Secure ICA encryption must be enabled on both the Mobile Client and server-side Steelhead appliances when securing SMB-signed traffic, encrypted MAPI traffic, or encrypted Citrix ICA traffic (RiOS v7.0). Enabling this option requires an optimization service restart. • **all** - The Mobile Client and the server-side Steelhead appliance authenticate each other and then encrypt and optimize all traffic. Only the optimized traffic is secure; pass-through traffic is not. Enabling this option requires an optimization service restart.

Usage

The **no** command option resets the traffic type.

For detailed information about SSL, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 ssl traffic-type all
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

policy id ssl trust-all

Description

Configures a trust relationship with all preconfigured peering certificates.

Syntax

[no] policy id <id> ssl trust-all

Parameters

<id>	Specify the policy ID number.

Usage

The **no** command option configures the system to not trust all preconfigured peering certificates.

For detailed information about SSL, see the *Steelhead Appliance Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 ssl trust-all
```

Product

Steelhead Mobile Controller

Related Topics

"show policy id"

Endpoint Commands

This section describes the Mobile Controller commands for endpoint clients.

endpoint info clearall

Description

Clears all endpoint statistics.

Syntax

endpoint info clearall

Parameters

None

Example

```
amnesiac (config) # endpoint info clearall
```

Product

Steelhead Mobile Controller

Related Topics

"endpoint info showall," "endpoint info threshold"

endpoint info showall

Description

Shows all endpoint information.

Syntax

endpoint info showall

Parameters

None

Example

```
amnesiac (config) # endpoint info showall
```

Product

Steelhead Mobile Controller

Related Topics

"endpoint info threshold," "endpoint info threshold"

endpoint info threshold

Description

Configures the duration, in seconds, to keep unused endpoint data.

Syntax

endpoint info threshold <seconds>

Parameters

<seconds>	Specify the number of seconds.

Example

```
amnesiac (config) # endpoint info threshold 10
```

Product

Steelhead Mobile Controller

Related Topics

"endpoint info showall," "endpoint info showall"

Package Commands

This section describes the Mobile Controller package commands.

package assignment adpath

Description

Configures package assignment by Active Directory path.

Syntax

[no] package assignment adpath <ad path> package_id <package-id>

Parameters

<ad path>	Specify the Active Directory path.
package_id <package-id>	Specify the package ID.

Usage

The **no** command option removes the package assignment by Active Directory path.

Example

```
amnesiac (config) # package assignment adpath //path package_id 1
```

Product

Steelhead Mobile Controller

Related Topics

"show package assignments adpath"

package assignment depid

Description

Configures package assignment by deployment ID.

Syntax

[no] package assignment depid <deploy id> package_id <package-id>

Parameters

depid <depid>	Specify the deployment ID.
package_id <package-id>	Specify the package ID.

Usage

The **no** command option removes the package assignment by deployment ID.

Example

```
amnesiac (config) # package assignment depid 2566 package_id 1
```

Product

Steelhead Mobile Controller

Related Topics

"show package assignments depid"

package assignment removeall-adpath

Description

Removes all Active Directory path assignments.

Syntax

package assignment removeall-adpath

Parameters

None

Example

```
amnesiac (config) # package assignment removeall-adpath
```

Product

Steelhead Mobile Controller

Related Topics

"show package assignments adpath"

package assignment removeall-depid

Description

Removes all package deployment ID assignments.

Syntax

package assignment remove-all-depid

Parameters

None

Example

```
amnesiac (config) # package assignment removeall-depid
```

Product

Steelhead Mobile Controller

Related Topics

"show package assignments depid"

Domain Command

This section describes Mobile Controller **domain** command.

ip fqdn override (Mobile Controller)

Description

Enables the Steelhead Mobile Client to override the fully qualified domain name.

Syntax

[no] ip fqdn override <domain name>

Parameters

<domain name>	Specify the override domain name.

Usage

If set, the fully qualified domain name always refers to the override value.

This command should be used sparingly and very carefully. If the override string has an error in it, the Steelhead Mobile Client will not be able to connect to the Mobile Controller until you change this override value.

To change the override domain name value

1. On your endpoint client machine, click the Riverbed icon in your tool bar to open the Steelhead Mobile Client window.
2. Click Settings.
3. Under Configure Steelhead Mobile Controllers, click **Configure** to open the Configure Steelhead Mobile Controller window.
4. Click **Override the controller list** and click **New**.
5. Type a new hostname in the **Hostname or IP Address** text box and click **OK**.
6. Click **Apply** to apply your changes.

Example

```
amnesiac (config) # ip fqdn override thisisatest
```

Product

Steelhead Mobile Controller

Related Topics

"show hosts"

Show Commands

This section describes the Mobile Controller **show** commands.

show cluster licenses

Description

Displays cluster licenses.

Syntax

show cluster licenses

Parameters

None

Example

```
amnesiac (config) # show cluster licenses

Member (Hostname:Port)  Licenses Installed  Licenses In Use Licenses Available
-----------------------------------------  ------------------  ---------------

example.example.com (localhost):7870        1000      0              100
example1.example1.com:          7870        1000      0              100

Summary:
Licenses Installed: 2000
Licenses Free: 1800
```

Product

Steelhead Mobile Controller

Related Topics

"cluster license checkout-count"

show cluster license settings

Description

Displays cluster license settings.

Syntax

show cluster license settings

Parameters

None

Example

```
amnesiac (config) # show cluster license settings
Global initial count of licenses to checkout:    100
Global count of licenses to checkout:            100
Threshold percentage to checkin unused licenses: 70
Threshold percentage to checkout more licenses:  90
```

Product

Steelhead Mobile Controller

Related Topics

"cluster join," "cluster remove," "cluster detach"

show cluster members

Description

Displays the Mobile Controllers in a cluster.

Syntax

show cluster members

Parameters

None

Example

```
amnesiac (config) # show cluster members
Member (Hostname:Port)   Version   Model  Health          LI      LIU     LA
sf-c2.example.com:7870   4.0.0     8500   Connected,      1000    6       100
                                          Synched
sf-c3.example.com:7870   4.0.0     8500   Connected       1000    4       100

LI:  Licenses Installed
LIU: Licenses In Use
LA:  Licenses Available
```

Product

Steelhead Mobile Controller

Related Topics

"cluster join," "cluster remove," "cluster detach"

show package assignments adpath

Description

Displays package Active Directory path assignments.

Syntax

show package assignments adpath

Parameters

None

Example

```
amnesiac # show package assignments adpath
#Assignment ID          Policy ID   Policy Name
--------------------   ---------   -----------
load-test-client-0     10          Policy[10]
```

Product

Steelhead Mobile Controller

Related Topics

"package assignment adpath"

show package assignments depid

Description

Displays package ID assignments.

Syntax

show package assignments depid

Parameters

None

Example

```
amnesiac # show package assignments depid
```

```
#Assignment ID          Policy ID   Policy Name
--------------------   ---------   -----------
load-test-client-0     10          Policy[10]
```

Product

Steelhead Mobile Controller

Related Topics

"package assignment depid"

show package list

Description

Displays current package list.

Syntax

show package list

Parameters

None

Example

```
amnesiac # show package list
Package Name   Version    Package ID
------------   --------   ----------------
Default        2.1.0.27   1784341108700150
```

Product

Steelhead Mobile Controller

Related Topics

"package assignment adpath," "package assignment removeall-adpath," "package assignment removeall-depid"

show policy assignments adpath

Description

Displays policy Active Directory path assignments.

Syntax

show policy assignments adpath

Parameters

None

Example

```
amnesiac # show policy assignments adpath
#Assignment ID          Policy ID   Policy Name
--------------------   ---------   -----------
load-test-client-0     10          Policy[10]
```

Product

Steelhead Mobile Controller

Related Topics

"policy assignment adpath"

show policy assignments depid

Description

Displays policy assignments by assignment ID.

Syntax

show policy assignments depid

Parameters

None

Example

```
amnesiac # show policy assignments depid
#Assignment ID          Policy ID   Policy Name
--------------------   ---------   -----------
load-test-client-0     10          Policy[10]
```

Product

Steelhead Mobile Controller

Related Topics

"package assignment depid"

show policy default

Description

Displays the default policy ID and name.

Syntax

show policy default

Parameters

None

Example

```
amnesiac (config) # show policy default

Policy ID   Policy Name
---------   -----------
1           Initial
```

Product

Steelhead Mobile Controller

show policy id

Description

Displays policy settings.

Syntax

show policy id <id> {branch-warming | cifs | citrix | connection | endpoint | ftp | http | in-path | mapi | nfs | notes | probe-tcp-opt | smb2 | ssl}

Parameters

<id>	Specify the policy ID number.
branch-warming	Displays branch-warming settings for the specified policy.
cifs	Displays CIFs protocol settings for the specified policy.
citrix	Displays Citrix protocol settings for the specified policy.
connection	Displays LAN and WAN connection settings for the specified policy.
endpoint	Displays endpoint settings for the specified policy.
ftp	Displays FTP protocol settings for the specified policy.
http	Displays HTTP protocol settings for the specified policy.
in-path	Displays in-path settings for the specified policy.
mapi	Displays MAPI protocol settings for the specified policy.
nfs	Displays NFS optimization settings for the specified policy.
notes	Displays Lotus Notes protocol settings for the specified policy.
probe-tcp-opt	Displays probe TCP settings for the specified policy.
smb2	Displays SMB2 protocol settings for the specified policy.
ssl	Displays SSL protocol settings for the specified policy.

Example

```
amnesiac(config) # show policy id 1 branch-warming
Enable Branch Warming: no
```

Product

Steelhead Mobile Controller

Related Topics

"Policy Commands"

show policy list

Description

Displays a list of policies, with policy ID and name.

Syntax

show policy list

Parameters

None

Example

```
amnesiac (config) # show policy list

Policy ID          Policy Name
---------------    -----------
1                  Initial
47769969272552     Addressing1
47769969272553     Addressing2
128953441101573    gw241
128953441101574    gw242
```

Product

Steelhead Mobile Controller

Related Topics

"policy id ssl enable"

show protocol ssl ca

Description

Displays settings for the signing certificate authority (CA).

Syntax

show policy ssl ca <certificate_name> certificate [raw | text]

Parameters

<certificate_name>	Specify CA certificate name.
raw	Specify raw PEM format.
text	Specify text format.

Example

```
amnesiac (config) # show protocol ssl ca Wells_Fargo certificate text
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 971282334 (0x39e4979e)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US, O=Wells Fargo, OU=Wells Fargo Certification Authority, CN=
Wells Fargo Root Certificate Authority
        Validity
            Not Before: Oct 11 16:41:28 2000 GMT
            Not After : Jan 14 16:41:28 2021 GMT
        Subject: C=US, O=Wells Fargo, OU=Wells Fargo Certification Authority, CN
=Wells Fargo Root Certificate Authority
        Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
            RSA Public Key: (2048 bit)
                Modulus (2048 bit):
                    00:d5:a8:33:3b:26:f9:34:ff:cd:9b:7e:e5:04:47:
<this is partial output>
```

Product

Steelhead Mobile Controller

Related Topics

"policy id ssl enable"

show protocol ssl cas

Description

Displays the CA certificates.

Syntax

show protocol ssl cas

Parameters

None

Example

```
amnesiac > show protocol ssl cas ca Actalis certificate text
  Name  (Issued To)
  AC_RaEDz_CerticE1mara_S.A.  (AC Ra<C3><AD>z Certic<C3><A1>mara S.A.)
  AOL_Time_Warner_1  (AOL Time Warner Root Certification Authority 1)
  AOL_Time_Warner_2  (AOL Time Warner Root Certification Authority 2)
  AddTrust_Class_1  (AddTrust Class 1 CA Root)
  AddTrust_External  (AddTrust External CA Root)
  AddTrust_Public  (AddTrust Public CA Root)
  AddTrust_Qualified  (AddTrust Qualified CA Root)
  America_Online_1  (America Online Root Certification Authority 1)
  America_Online_2  (America Online Root Certification Authority 2)
  Autoridad_de_Certificacion_Firmaprofesional_CIF_A62634068  (Autoridad de Certi
ficacion Firmaprofesional CIF A62634068)
  Baltimore_CyberTrust  (Baltimore CyberTrust Root)
  COMODO  (COMODO Certification Authority)
  COMODO_ECC  (COMODO ECC Certification Authority)
  Certisign_Autoridade_Certificadora_AC1S  ()
  Certisign_Autoridade_Certificadora_AC2  ()
  Certisign_Autoridade_Certificadora_AC3S  ()
  Certisign_Autoridade_Certificadora_AC4  ()
  Certplus_Class_1_Primary  (Class 1 Primary CA)
  Certplus_Class_2_Primary  (Class 2 Primary CA)
  Certplus_Class_3P_Primary  (Class 3P Primary CA)
<<partial listing>>
```

Product

Steelhead Mobile Controller

Related Topics

"policy id ssl enable"

show protocol ssl chain-cert

Description

Displays the CA certificates.

Syntax

show protocol ssl chain-cert {ca | cert <cert data>}

Parameters

ca	Specify the certificate name
cert <cert data>	Specify the certificate in PEM format.

Example

```
amnesiac # show protocol ssl chain-cert ca Coast_Bank
CA "Coast_Bank" added to chain.
```

Product

Steelhead Mobile Controller

Related Topics

"policy id ssl enable"

show protocol ssl signing certificate

Description

Displays SSL signing status.

Syntax

show protocol SSL signing certificate <cr>| [raw | text]

Parameters

raw	Specify raw PEM format.
text	Specify text format.

Example

```
amnesiac (config) # show protocol ssl signing certificate
Issued To:
  Common Name:       examle.lab.example.com
  Email:             examplet@example.com
  Organization:      Riverbed Technology, Inc.
  Locality:          San Francisco
  State:             California
  Country:           --
  Serial Number:     xx-xx-xx-xx-xx-xx
Issued By:
  Common Name:       examle.lab.example.com
  Email:              examplet@example.com
  Organization:      Riverbed Technology, Inc.
  Locality:          San Francisco
  State:             California
  Country:           --
Validity:
  Issued On:         Apr 13 16:38:14 2010 GMT
  Expires On:        Apr 12 16:38:14 2015 GMT
Fingerprint:
  SHA1:              xx:XX:XX:XX:XX:XX:XX:
Extensions:
  X509v3 Subject Key Identifier:  XX:XX:XX:XXX:XXX
:3E:69:58:35:50
```

Product

Steelhead Mobile Controller

Related Topics

"policy id ssl enable"

Cloud Steelhead Feature Commands

This section describes the commands unique to Cloud Steelhead and includes commands up to Cloud Steelhead version 1.3. You can use the command-line to perform basic cloud configuration tasks, display configuration information, and check status. Some commands require information available only from the Riverbed Cloud Portal. Riverbed strongly recommends that you use the Cloud Steelhead GUI to configure the Cloud Steelhead appliance. This section also contains:

- "Displaying Cloud Steelhead Information"

For detailed information about the Cloud Steelhead, see the *Riverbed Cloud Services Deployment Guide*.

discovery enable

Description

Enables the Discovery Agent on the CSH.

Syntax

[no] discovery enable

Parameter

None

Usage

The Discovery Agent is a software package that you install on the client or server in the optimized Riverbed cloud.

When a client Steelhead connects to a server in the cloud, the Discovery Agent redirects any auto-discovery probe request to a CSH in its optimization group. Then, the client Steelhead discovers and starts peering and optimizing with the CSH. After the auto-discovery process completes, the connection is terminated locally on the Steelhead without going over the WAN.

When a client in the cloud connects to a server, the Discovery Agent redirects any TCP connection to a CSH in its optimization group. The CSH sends an auto-discovery probe, discovers the remote Steelhead, and starts peering and optimizing with it.

Configure Discovery Agent settings before you enable discovery.

The Discovery Agent provides auto-discovery, transparency, failure detection, and load balancing. For details, see the *Riverbed Cloud Services Deployment Guide*.

The **no** command option disables the Discovery Agent on the CSH.

Example

```
amnesiac (config) # discovery enable
```

Product

CSH

Related Topics

“show discovery”

discovery local

Description

Specifies the local node configuration in the Discovery Agent.

Syntax

discovery local [node-id <id>] [node-key <key>] [discovery-type {riverbed-portal | local-portal url <portal URL>}] [refresh-time <time>]

Parameters

node-id <id>	Specify the local client ID.
node-key <key>	Specify the local client key.
discovery-type {riverbed-portal | local-portal url <portal URL>}	Specify the portal with which the Discovery Agent should communicate. The default value is **riverbed-portal**. You can use your own local portal by specifying the **local-portal url** option and typing the URL of the local portal.
refresh time <time>	Specify the refresh time in seconds for the Discovery Agent. The time must be between 300 and 3600 seconds. The default value is 300 seconds.

Usage

The **riverbed-portal** parameter does not take a URL. This is valid:

```
amnesiac (config) # discovery local discovery-type local-portal url MY_URL
```

This is not valid:

```
amnesiac (config) # discovery local discovery-type riverbed-portal url MY_URL
```

Example

```
amnesiac (config) # discovery local refresh-time 400
```

Product

CSH

Related Topics

"show discovery"

in-path agent-intercept

Description

Configures the agent intercept mode.

Syntax

in-path agent-intercept [heartbeat port <IP port>] [keepalive count <int>] [keepalive interval <int>] [server-nat-mode<mode>]

Parameters

heartbeat port <IP port>	Specify the IP port that transmits a regular heartbeat.
keepalive count <int>	Specify a value for the keepalive count. This is the total number of acknowledgements (ACKs) for which the CSH waits before it reports that the Discovery Agent is down.
keepalive interval <int>	Specify the time interval in seconds between keep-alive messages of the CSH for heartbeat connection with the Discovery Agent.
server-nat-mode <mode>	Specify the transparency mode for client connections: **safe-transparent**, **restricted-transparent** (default), or **non-transparent**. You configure the transparency mode in the CSH and it transmits it to the Discovery Agent. There are three transparency modes: **safe-transparent** - If the client is behind a NAT device, the client connection to the application server is non-transparent—the application server sees the connection as a connection from the CSH IP address and not the client IP address. All connections from a client that is not behind a NAT device are transparent and the server sees the connection as a connection from the client IP address instead of the CSH IP address. **restricted-transparent** - All client connections are transparent with the following restrictions: If the client connection is from a NATed network, the application server detects the private IP address of the client. You can use this mode only if there is no conflict between the private IP address ranges (there are no duplicate IP addresses) and ports. This is the default mode. **non-transparent** - All client connections are non-transparent—the application server detects the connections from the server-side Steelhead IP address and not the client IP address. Riverbed recommends that you use this mode as the last option.

Usage

There is a constant keep-alive connection between the CSH and the Discovery Agent.

Example

```
amnesiac (config) # in-path agent-intercept heartbeat port 8081
```

Product

CSH

Related Topics

"show in-path agent-intercept"

in-path agent-intercept enable

Description

Enables the agent intercept mode.

Syntax

[no] in-path agent-intercept enable

Parameters

None

Usage

You must map the in-path intercept feature between the Amazon Web Services (AWS) appliance public IP address and private IP address. You must restart the CSH for this command to take effect.

The **no** command option disables the in-path intercept mode on the CSH.

Example

```
amnesiac (config) # in-path agent-intercept enable
```

Product

CSH

Related Topics

"show in-path agent-intercept"

in-path agent-intercept keepalive non-zero

Description

Enables keep-alive, non-zero, in the agent intercept mode. The keep-alive feature checks for peer connectivity status and provides network activity to prevent disconnection due to inactivity.

Syntax

[no] in-path agent-intercept keepalive non-zero

Parameters

None

Usage

There is a constant keep-alive connection between the CSH and the Discovery Agent.

The **no** command option disables the keep-alive non-zero feature in the in-path intercept mode on the server.

Example

```
amnesiac (config) # in-path agent-intercept keepalive non-zero
```

Product

CSH

Related Topics

"show in-path agent-intercept"

ip addrmap

Description

Creates a new IP address map between the public IP address of the server to its private IP address in AWS.

Syntax

[no] ip addrmap public-addr <public IP address> private-addr <private IP address>

Parameters

public-addr <public IP address>	Specify the public IP address of the server.
private-addr <private IP address>	Specify the private IP address of the server.

Usage

The **no** command option deletes a map entry from the public to private IP address map table. The **no ip addrmap** command does not allow the parameter **private-addr**.

Example

```
amnesiac (config) # ip addrmap public-addr 10.0.62.164 private-addr 10.0.62.165
amnesiac (config) # no ip addrmap public-addr 10.10.10.1
```

Product

CSH

Related Topics

"show ip addrmap"

ip addrmap enable

Description

Enables the IP address mapping between the public IP address of the server and its private IP address in Amazon Web Services (AWS).

Syntax

[no] ip addrmap enable

Parameters

None

Usage

The CSH must know the IP address mapping between the public and private IP addresses of the server so that it can recognize the connection coming from the server and optimize it.

You must restart the CSH for this command to take effect.

The **no** command option disables the IP address mapping between the public IP address of the server and its private IP address in AWS.

Example

```
amnesiac (config) # ip addrmap enable
```

Product

CSH

Related Topics

"show ip addrmap"

license client fetch

Description

Forces the license client to update immediately.

Syntax

license client fetch

Parameters

None

Usage

If there is a change in your account (such as if Riverbed has given you an extra license), and the change will be updated whenever the license client runs next, but you want to force it to run immediately, then you can use the **license client fetch** command.

Example

```
amnesiac # license client fetch
```

Product

CSH

Related Topics

"show license-client"

license client init

Description

Uses the one-time-token you provide to retrieve a license for the CSH.

Syntax

[no] license client init <one-time-token>

Parameters

<one-time-token>	Specify the one-time token that the CSH uses to retrieve the license.

Usage

The license client is part of the CSH software. It communicates with the license server. It has two main functions:

- It periodically contacts the license server and checks out and renews the license.
- It enables you to query available features, licenses and other metadata such as serial number.

You can configure the license client to communicate with the license server at the company headquarters or the local license server.

If the **no license client init** command is used without specifying a license token, all licenses are removed.

Example

```
amnesiac (config) # license client init "8c163d46-39b2-427d-9b3e-4f0c5317effb"
```

Product

CSH

Related Topics

"show in-path agent-intercept"

license server (Cloud Steelhead)

Description

Adds a license server.

Syntax

[no} license server <hostname> [priority <number>] [port <number>]

Parameters

<hostname>	Specify the hostname of the computer that contains the license server.
priority <number>	Specify the order in which the license server is added. 0 is the highest priority and 9 is the lowest priority. The default priority is 9.
port <number>	Optionally, specify the port number on which the license server is listening. The default is port 80.

Usage

The license server provides licenses to CSHs.

The **no** command option deletes the license server specified.

The default license server is the server hosted at Riverbed headquarters.

The **no license server <hostname> priority** command resets the priority in which the specified license server is added to the default value (9 is the lowest priority).

The **no license server <hostname> port** command resets the license server port to the default port.

Example

```
amnesiac (config) # license server MyLicenseServer
amnesiac (config) # show license-servers
Server Name                         Port                Priority
---------------                     ---------------     ---------------
MyLicenseServer                     80                  0
```

Product

CSH

Related Topics

"show license-servers (Cloud Steehead)"

Displaying Cloud Steelhead Information

This section describes the **show** commands for displaying Cloud Steelhead information.

show discovery

Description

Displays whether the Discovery Agent is enabled or disabled on the CSH.

Syntax

show discovery {settings | info]

Parameters

settings	Displays the Discovery Agent settings such as the client ID and client key.
info	Displays groups and nodes associated with the Discovery Agent in the Riverbed Cloud Portal.

Example

```
amnesiac (config) # show discovery
Enabled: no
```

Product

CSH

Related Topics

"discovery enable"

show in-path agent-intercept

Description

Displays the status of the in-path intercept feature.

Syntax

show in-path agent intercept

Parameters

None

Example

```
amnesiac (config) # show in-path agent-intercept
Enabled            : yes
Heartbeat port     : 7850
Keepalive count    : 3
Keepalive interval : 1
```

Product

CSH

Related Topics

"in-path agent-intercept"

show in-path agent intercept server-nat mode

Description

Displays the transparency mode for client connections.

Syntax

show in-path agent intercept server-nat mode

Parameters

None

Example

```
amnesiac (config) # show in-path agent intercept server-nat-mode
Server NAT mode : restricted-transparent
```

Product

CSH

Related Topics

"in-path agent-intercept"

show ip addrmap

Description

Displays the mapping between the public IP address and private IP address of the server in AWS.

Syntax

show ip addrmap [public-addr <public IP address>]

Parameters

public-addr <public IP address>	Displays the public IP address of the CSH.

Example

```
amnesiac (config) # show ip addrmap
IP address mapping: enabled
Public addr     Private addr
-----------     ------------
    10.0.62.164 10.0.62.165
```

Product

CSH

Related Topics

"ip addrmap enable", "ip addrmap"

show licenses

Description

Displays all of the CSH licenses.

Syntax

show licenses

Parameters

None

Example

```
amnesiac (config) # show licenses
Local: LK1-SH10BASE-0000-0037-1-3A45-F3C2-7AB2
   Index:        1
   Feature:      SH10BASE
   Valid:        yes
   Active:       yes
   Start date:
   End date:
```

Product

CSH

Related Topics

"license client fetch", "license client init" "license server (Cloud Steelhead)"

show license-client

Description

Displays details of the licenses retrieved by the CSH.

Syntax

show license-client

Parameters

None

Example

```
amnesiac (config) # show license-client
Serial Number: V78386326145
Status: Licensed
Reason: Appliance received valid license from the Portal.
Last Contact With: cloudportal.riverbed.com
Last Contact At: 04/29/2011 16:00
Renew Interval: 3 minutes
Client ID: 372938742-24397234-24387622def
```

In the above example, `Reason:` shows the result of the last communication with the Riverbed Cloud Portal.

Product

CSH

Related Topics

"license client fetch", "license client init"

show license-servers (Cloud Steehead)

Description

Displays the name, port number, and priority of the server that the CSH uses for licensing.

Syntax

show license-servers

Parameters

None

Example

```
amnesiac (config) # show license-servers
Server Name                              Port                Priority
---------------                          ---------------     ---------------
aws-cloud-df.riverbed.com                80                  5
```

Product

CSH

Related Topics

"license server (Cloud Steelhead)"

Steelhead Cloud Accelerator Commands

This section describes the commands unique to the Steelhead Cloud Accelerator. You can use the command-line to perform basic cloud configuration tasks, display configuration information, and check status. Some commands require information available only from the Riverbed Cloud Portal. Riverbed strongly recommends that you use the ESH GUI to configure the Enterprise Steelhead appliance.

in-path peering rule cloud-accel

Description

Configures in-path peering rules for the Steelhead Cloud Accelerator.

Syntax

[no] in-path peering rule cloud-accel {auto | pass} | [peer <peer ip-addr>]| [ssl-capability cap | in-cap | no-check] | [src <subnet>] | [dest <subnet> | dest-port <port>] | [rulenum <rulenum>] | [description <description>]

Parameters

cloud-accel	Use cloud acceleration in peering rules on a data center Steelhead appliance in a back-hauled deployment to configure which connections coming from a branch Steelhead appliance (with the SCA enabled but with redirect disabled) should be optimized with the SCA. Specify one of the following rules: • **auto** - The data center Steelhead appliance redirects to the cloud connections when the branch Steelhead appliance tries to optimize with the SCA. • **pass** - The data center Steelhead appliance does not redirect to the cloud connections when the branch Steelhead appliance tries to optimize with the SCA. If the branch Steelhead appliance does not have the SCA enabled, or if it is not trying to optimize the SCA connection, the value of this field is irrelevant on the data center Steelhead appliance.
peer <peer ip-addr>	Specify the in-path IP address of the probing Steelhead appliance. If more than one in-path interface is present on the probing Steelhead appliance, apply multiple peering rules, one for each in-path interface.
ssl-capability [cap | in-cap | no-check]	Specify one of the following options to determine how to process attempts to create secure SSL connections: • **no-check** - The peering rule does not determine whether the server Steelhead appliance is present for the particular destination IP address and port combination. This default rule catches any connection that did not match the first two default rules. The Steelhead appliance performs auto-discovery and does not optimize SSL. This rule always appears last in the list and you cannot remove it. • **cap (capable)** - The peering rule checks whether the server-side Steelhead appliance is present for the particular destination IP address and port combination. If the destination IP address and port are of an SSL server that is properly configured and enabled on the server-side Steelhead appliance, and if there is no temporary or short-lived error condition, the SSL-capable check is a success. The Steelhead appliance accepts the condition and, assuming all other proper configurations and that the peering rule is the best match for the incoming connection, optimizes SSL. The default peering rule with the SSL capable flag matches those connections to the destination IP/port combination for which there is an SSL server configuration added. The Steelhead appliance considers the SSL server a match even if it is defined on a port number that is not the standard port 443. For all connections that match, the Steelhead appliance performs both auto-discovery and SSL optimization. • **incap (incapable)** - If the destination IP address and port are not an SSL server that is properly configured and enabled on the server-side Steelhead appliance, or if there is a temporary or short-lived error condition, the SSL-capable check fails. The Steelhead appliance passes the connection through unoptimized without affecting connection counts. The default peering rule with the SSL incap flag matches any SSL connection to port 443 for which there is no SSL server configuration on the Steelhead appliance.
src <subnet>	Specify the source network for this rule.
dest <subnet>	Specify the destination network for this rule.
dest-port <port>	Specify the destination port for this rule. You can specify a port label, or **all** for all ports.
rulenum <rulenum>	Specify the rule number. The system evaluates the rules in numerical order starting with rule **1**. If the conditions set in the rule match, then the rule is applied. If the conditions set in the rule do not match, then the rule is not applied and the system moves on to the next rule. For example, if the conditions of rule **1** do not match, rule **2** is consulted. If rule **2** matches the conditions, it is applied, and no further rules are consulted. The type of a matching rule determines which action the Steelhead appliancee takes on the connection.
description <description>	Specify a description to facilitate communication about network administration.

Usage

You can provide increased optimization by deploying two or more Steelhead appliances back-to-back in an in-path configuration to create a serial cluster.

Appliances in a serial cluster process the peering rules you specify in a spill-over fashion. When the maximum number of TCP connections for a Steelhead appliance is reached, that appliance stops intercepting new connections. This allows the next Steelhead appliance in the cluster the opportunity to intercept the new connection, if it has not reached its maximum number of connections. The in-path peering rules and in-path rules tell the Steelhead appliance in a cluster not to intercept connections between themselves.

You configure peering rules that define what to do when a Steelhead appliance receives an auto-discovery probe from another Steelhead appliance.

You can deploy serial clusters on the client or server-side of the network.

Supported Models

Two-appliance serial clusters are supported for all Steelhead appliance *xx*20 and *xx*50 models, except the 250 model. The Steelhead appliances must be the same model running RiOS v5.5.3 or later or RiOS v5.0.8 or later.

The following Steelhead appliance models support serial clusters:

- 550 series, 1050 series, 2050, 5050, 6050, 7050, 1020, 2020, 3020, 3520, 5000, 5010, 5520, and 6020

These models can reach their specifications even while potentially passing through the LAN-side traffic for optimized connections for the other Steelhead appliance in the cluster.

When running a RiOS software version prior to v5.5.1, models 5520, 6020, and 6120 are qualified by Riverbed for serial clusters.

Important: For environments that want to optimize MAPI or FTP traffic which require all connections from a client to be optimized by one Steelhead appliance, Riverbed strongly recommends using the master and backup redundancy configuration instead of a serial cluster. For larger environments that require multi-appliance scalability and high availability, Riverbed recommends using the Interceptor appliance to build multi-appliance clusters. For details, see the *Interceptor Appliance Deployment Guide* and the *Interceptor Appliance User's Guide*.

Notes:

- When you combine two Steelhead appliances that have a bandwidth limit of 20 Mbps each, the serial cluster still has a limit of 20 Mbps.
- If the active Steelhead appliance in the cluster enters a degraded state because the CPU load is too high, it continues to accept new connections.

Preventing an Unknown (or Unwanted) Steelhead Appliance from Peering

To prevent an unknown Steelhead appliance from peering you must add a pass-through peering rule that passes through traffic from the unknown Steelhead appliance in the remote location. For detailed information, see the Management Console online help and the *Steelhead Appliance Deployment Guide*.

Example

This is an example of how to configure a cluster of three in-path appliances in a data center.

```
WAN----SH1----SH2----SH3----LAN

SH1 ip address is 10.0.1.1 on a /16
SH2 ip address is 10.0.1.2 on a /16
SH3 ip address is 10.0.1.3 on a /16
```

In this example, you configure each Steelhead appliance with in-path peering rules to prevent peering with another Steelhead appliance in the cluster, and with in-path rules to not optimize connections originating from other Steelhead appliances in the same cluster.

SH1 configuration:

```
SH1 > enable
SH1 # configure terminal
SH1 (config) # in-path peering rule pass peer 10.0.1.2 rulenum 1
SH1 (config) # in-path peering rule pass peer 10.0.1.3 rulenum 1
SH1 (config) # in-path rule pass-through srcaddr 10.0.1.2/32 rulenum 1
SH1 (config) # in-path rule pass-through srcaddr 10.0.1.3/32 rulenum 1
SH1 (config) # wr mem
SH1 (config) # show in-path peering rules
Rule  Type   Source Network     Dest Network       Port  Peer Addr
----- ------ ------------------ ------------------ ----- ---------------
    1 pass   *                  *                  *     10.0.1.3
    2 pass   *                  *                  *     10.0.1.2
  def auto   *                  *                  *     *
SH1 (config) # show in-path rules
Rule  Type Source Addr        Dest Addr          Port  Target Addr     Port
----- ---- ------------------ ------------------ ----- --------------- -----
    1 pass 10.0.1.3/32        *                  *     --              --
    2 pass 10.0.1.2/32        *                  *     --              --
  def auto *                  *                  *     --              --
```

SH2 configuration

```
SH2 > enable
SH2 # configure terminal
SH2 (config) # in-path peering rule pass peer 10.0.1.1 rulenum 1
SH2 (config) # in-path peering rule pass peer 10.0.1.3 rulenum 1
SH2 (config) # in-path rule pass-through srcaddr 10.0.1.1/32 rulenum 1
SH2 (config) # in-path rule pass-through srcaddr 10.0.1.3/32 rulenum 1
SH2 (config) # wr mem
SH2 (config) # show in-path peering rules
Rule  Type   Source Network     Dest Network       Port  Peer Addr
----- ------ ------------------ ------------------ ----- ---------------
    1 pass   *                  *                  *     10.0.1.3
    2 pass   *                  *                  *     10.0.1.1
  def auto   *                  *                  *     *
SH1 (config) # show in-path rules
Rule  Type Source Addr        Dest Addr          Port  Target Addr     Port
----- ---- ------------------ ------------------ ----- --------------- -----
    1 pass 10.0.1.3/32        *                  *     --              --
    2 pass 10.0.1.1/32        *                  *     --              --
  def auto *
                *                  *     --              --
```

SH3 configuration

```
SH3 > enable
SH3 # configure terminal
SH3 (config) # in-path peering rule pass peer 10.0.1.1 rulenum 1
SH3 (config) # in-path peering rule pass peer 10.0.1.2 rulenum 1
SH3 (config) # in-path rule pass-through srcaddr 10.0.1.1/32 rulenum 1
SH3 (config) # in-path rule pass-through srcaddr 10.0.1.2/32 rulenum 1
SH3 (config) # wr mem
SH3 (config) # show in-path peering rules
Rule  Type   Source Network     Dest Network       Port  Peer Addr
----- ------ ------------------ ------------------ ----- ---------------
SH1 (config) # show in-path rules
Rule  Type Source Addr        Dest Addr          Port  Target Addr     Port
----- ---- ------------------ ------------------ ----- --------------- -----
    1 pass 10.0.1.2/32        *                  *     --              --
    2 pass 10.0.1.1/32        *                  *     --              --
  def auto *                  *                  *     --              --
```

Product

SCA

Related Topics

“show in-path peering rules”

service cloud-accel enable

Description

Enables the cloud acceleration service.

Syntax

[no] service cloud-accel enable

Parameters

None

Usage

This command enables communication with the Riverbed Cloud Portal and also enables the cloud acceleration service. The **no** command option disables the cloud acceleration service.

Example

```
amnesiac (config) # service cloud-accel enable
```

Product

SCA

Related Topics

"show service cloud-accel"

service cloud-accel log-level

Description

Specifies the severity of the log message.

Syntax

service cloud-accel log-level <debug | info | notice | warning | error | critical>

Parameters

log-level <debug | info | notice | warning | error | critical>	Select the minimum severity level for the event log messages. The log contains all messages with this severity level or higher. Select one of the following levels from the drop-down list: • **debug** - Messages that help you debug a failure. • **info** - Informational messages that provide general information about system operations. • **notice** - Normal, but significant conditions, such as a configuration change. This is the default setting. • **warning** - Conditions that might affect the functionality of the appliance, such as authentication failures. • **error** - Conditions that probably affect the functionality of the appliance. • **critical** - Conditions that affect the functionality of the appliance.

Example

```
amnesiac (config) # service cloud-accel log-level info
```

Product

SCA

Related Topics

"show service cloud-accel"

service cloud-accel platforms enable

Description

Allows you to enable or disable cloud acceleration for a specific SaaS platform.

Syntax

[no] service cloud-accel platforms <appid> enable

Parameters

<appid>	Specify the Saas application for which you want to enable or disable cloud acceleration. This parameter can have one of the following values: • O365 for Office365 • SFDC for Salesforce.com.

Usage

The **no** command option disables cloud acceleration for the SaaS platform specified.

Example

```
amnesiac (config) # service cloud-accel platforms O365 enable
```

Product

SCA

Related Topics

"show service cloud-accel platforms," "show service cloud-accel platforms ip"

service cloud-accel portal refresh

Description

Instructs the Enterprise Steelhead appliance to contact the Riverbed Cloud Portal immediately and refresh its service details.

Syntax

service cloud-accel portal refresh

Parameters

None

Example

```
amnesiac (config) # service cloud-accel portal refresh
```

Product

SCA

Related Topics

"show service cloud-accel"

service cloud-accel redirect enable

Description

Enables redirection of connections through the Steelhead Cloud Accelerator.

Syntax

[no] service cloud-accel redirect enable

Parameters

None

Usage

Use this command to activate traffic redirection from the Enterprise Steelhead appliance to the Akamai network. This feature is enabled by default. There are two modes of proxy redirection:

- Direct mode - The Enterprise Steelhead appliance redirects traffic to the Akamai network.
- Backhauled mode - The Enterprise Steelhead appliance in the data center redirects traffic to the Akamai network. So, you must disable proxy redirection in the branch Enterprise Steelhead appliance and let the data center appliance redirect the traffic.

The **no** command option disables cloud acceleration redirection.

Example

```
amnesiac (config) # service cloud-accel redirect enable
```

Product

SCA

Related Topics

"show service cloud-accel"

service cloud-accel redirect log-level

Description

Sets the log-level for the cloud acceleration service.

Syntax

service cloud-accel redirect log-level

Parameters

port <port>	Specify the port number for UDP connections to the Akamai network.

Example

```
amnesiac (config) # service cloud-accel redirect port 65
```

Product

SCA

Related Topics

"show service cloud-accel"

service cloud-accel redirect port

Description

Specifies the destination port used to redirect connections through the Steelhead Cloud Accelerator.

Syntax

service cloud-accel redirect port <port>

Parameters

port <port>	Specify the port number for UDP connections to the Akamai network.

Usage

Use this command to specify a port number for the configurable outbound port for UDP connections to the Akamai network or leave the default value (9545) as it is. The Enterprise Steelhead appliance connected to the Akamai network uses this configurable UDP port over a wide range of IP addresses.

Example

```
amnesiac (config) # service cloud-accel redirect port 65
```

Product

SCA

Related Topics

"show service cloud-accel"

service cloud-accel redirect spill-over enable

Description

Specifies whether the Enterprise Steelhead appliance should continue to redirect new SaaS connections through the cloud when it reaches the Enterprise Steelhead appliance admission control.

Syntax

service cloud-accel redirect spill-over enable

Parameters

None

Usage

Use this command in a serial failover or serial cluster configuration that contains two Steelhead appliances connected back-to-back; if the first appliance is in admission control, you can configure it to let the SaaS connections spill over to the second appliance and ensure that the connections are optimized.

The default setting is disabled, so that when the Steelhead appliance reaches admission control, it redirects connections through the cloud, but the connections are not optimized.

You must enable this setting on the first Steelhead appliance in a serial failover or serial cluster configuration.

The **no** command option disables the cloud acceleration redirection when the Enterprise Steelhead appliance reaches its admission control.

Example

```
amnesiac (config) # service cloud-accel redirect spill-over enable
```

Product

SCA

Related Topics

"show service cloud-accel"

service cloud-accel register

Description

Registers the Enterprise Steelhead appliance using the appliance registration key you specify.

Syntax

[no] service cloud-accel register <key>

Parameters

<key>	Specify the appliance registration key

Usage

The appliance registration key enables the Enterprise Steelhead appliance to register with the Riverbed Cloud Portal.

The **no** command option deregisters the Enterprise Steelhead appliance. Deregistration cannot be reversed. If you deregister your Enterprise Steelhead appliance, you must register it again for it to participate in the cloud acceleration service.

Example

```
amnesiac (config) # service cloud-accel register ABCDEF12345
```

Product

SCA

Related Topics

"show service cloud-accel"

Displaying Steelhead Cloud Accelerator Information

This section describes the **show** commands for displaying Steelhead Cloud Accelerator information.

show service cloud-accel

Description

Displays the following information about the Steelhead Cloud Accelerator: whether it is enabled, its status, the hostname of the portal it is connected to, whether proxy redirection is enabled or disabled, the port to which it is connected, and its state.

Syntax

show service cloud-accel

Parameters

None

Example

```
gen-sh210 (config) # show service cloud-accel
  Enabled:             No
  Status:              Unregistered
  Portal:              cloudportal.riverbed.com:443 (HTTPS)
  Redirection:         Enabled
    Port:              9545
    State:             Inactive
```

Product

Steelhead Cloud Accelerator

Related Topics

"Steelhead Cloud Accelerator Commands"

show service cloud-accel platforms

Description

Displays details about the SaaS platforms that the Enterprise Steelhead appliance is optimizing.

Syntax

show service cloud-accel platforms

Parameters

None

Example

```
gen-sh210 (config) # show service cloud-accel platforms
SaaS Platform           App ID          Enabled
-------------           ------          ------
Office 365              O365            Yes
Salesforce.com          SFDC            Yes
```

Product

SCA

Related Topics

"Steelhead Cloud Accelerator Commands"

show service cloud-accel platforms ip

Description

Displays details about the server IP addresses that the Enterprise Steelhead appliance is optimizing. You can use this command to troubleshoot issues when connections to a certain SaaS service are not optimized through the cloud.

Syntax

show service cloud-accel platforms ip

Parameters

None

Example

```
gen-sh210 (config) # show service cloud-accel platforms ip
149 results found:
---------------------------------------------------------------------------

173.194.0.0/16          443:443
207.126.144.0/20        443:443
209.85.128.0/17         443:443
216.239.32.0/19         443:443
64.18.0.0/20            443:443
64.233.160.0/19         443:443
66.102.0.0/20           443:443
66.249.80.0/20          443:443
72.14.192.0/18          443:443
74.125.0.0/16           443:443
111.221.68.0/24         25:25
111.221.68.0/24         80:80
111.221.68.0/24         443:443
111.221.68.0/24         587:587
207.46.62.0/24          25:25
[partial output]
```

Product

SCA

Related Topics

"Steelhead Cloud Accelerator Commands"

show service cloud-accel statistics connections

Description

Displays details about the optimized SaaS connections.

Syntax

show service cloud-accel statistics connections

Parameters

None

Example

```
gen-sh210 (config) # show service cloud-accel statistics connections
CLNT-IP     SERV-IP  SRIP-EDGE-IP  TYPE  STATE  SRC-IP  DEST-IP    ESH ID
10.32.75.135:53894   157.56.232.198:443   204.132.143.51  Prefresh   Normal   10.32.3.35:63157
63.217.157.6:7827
70005
10.32.75.135:53893   157.56.232.198:443   204.132.143.51  Prefresh   Normal   10.32.3.35:63156
63.217.157.6:7827
70005
10.32.75.135:55443   173.194.79.189:443   69.22.131.51    Prefresh   Normal   10.32.3.35:63516
64.209.118.20:7827
70005
10.32.75.135:55442   173.194.79.189:443   204.132.143.51  Prefresh  Timed_Wait 10.32.3.35:63515
64.209.118.20:7827
   70005
[partial output]
```

Product

SCA

Related Topics

"Steelhead Cloud Accelerator Commands"

show service cloud-accel statistics devices

Description

Displays details about the SaaS platforms that the Enterprise Steelhead appliance is optimizing.

Syntax

show service cloud-accel statistics devices

Parameters

None

Example

```
gen-sh210 (config) # show service cloud-accel statistics devices
rbtpipe0_0:
  device: packets in, out    : 0 0
  device: bytes in, out      : 0 0
  device: malformed, no conn: 0 0
  device: invalid, dns fail : 0 0
  intfc: packets in, out     : 0 0
  intfc: bytes in, out       : 0 0
  intfc: malformed, no conn : 0 0
rbtpipe0_1:
  device: packets in, out    : 2370749 2447030
  device: bytes in, out      : 243796158 296371873
  device: malformed, no conn: 0 14
  device: invalid, dns fail : 0 28
  intfc: packets in, out    : 2564261 2487981
  intfc: bytes in, out      : 301226622 278001118
  intfc: malformed, no conn : 0 22
```

Product

SCA

Related Topics

"Steelhead Cloud Accelerator Commands"

CHAPTER 5 Troubleshooting

This chapter contains a table of commands to provide a quick reference for troubleshooting

Problem	Commands
General	"logging local"
	"show alarm," "show alarms"
	"show clock"
	"show history"
	"show logging"
	"show info"
	"show version"
Start, Stop, and Reboot	"reload"
	"restart"
	"service enable"
Connectivity	"show bootvar"
	"show connection," "show connections"
	"show flow," "show flows"
	"ping"
	"traceroute"
Data Store	"show datastore"

Problem	Commands
Optimization Service	"show in-path"
	"show in-path cdp"
	"show out-of-path"
	"show in-path rules"
	"show peers"
	"show service"
	"show wccp"
	"show licenses"
Hardware	"show stats cpu"
	"show stats memory"
	"show stats ecc-ram"
	"show stats fan"
	"show hardware error-log"
	"show hardware spec"
	"show history"
Protocol Specific	"show protocol cifs"
	"show protocol citrix"
	"show protocol ftp"
	"show protocol http"
	"show protocol http server-table"
	"show protocol mapi"
	"show protocol ms-sql"
	"show protocol nfs"
	"show protocol notes"
	"show protocol oracle-forms"
	"show protocol smb2"
	"show protocol snapmirror," "show protocol snapmirror stats," "show stats protocol snapmirror"
	"show protocol ssl"
	"show qos l7protocol"
PFS and Prepopulation	"show pfs status"
	"show pfs configuration"
	"show prepop"
	"pfs settings"

Problem	Commands
Asymmetric Routing and Failover	"show failover"
	"show in-path asym-route-tab"
	"show in-path neighbor"
	"show in-path neighbor advertiseresync"
	"show hardware error-log"
RAID	"show raid configuration"
	"show raid diagram"
	"show raid error-msg"
	"show raid info"
	"show report"
Upgrade and Boot	"show images"
	"show bootvar"
Collecting System Data for Riverbed Technical Support	"RiOS TCP Dump Commands"
	"debug generate dump"
	"file debug-dump delete"

APPENDIX A

Riverbed Ports

This appendix provides a reference to ports used by the system. It includes the following sections:

- "Granite Ports" on page 1059
- "Default Ports" on page 1060
- "Commonly Excluded Ports" on page 1060
- "Interactive Ports Forwarded by the Steelhead Appliance" on page 1060
- "Secure Ports Forwarded by the Steelhead Appliance" on page 1061

Granite Ports

The following table summarizes Steelhead EX+Granite default ports with the port label: Granite.

Default Ports	Description
7950	Data requests for data-blocks absent in Edge from the data center
7951	New data created at the Edge to the data center
7952	Prefetch data for which Granite has highest confidence (for example, file read ahead)
7953	Prefetch data for which Granite has medium confidence (for example, boot)
7954	Prefetch data for which Granite has lowest confidence (for example, prepopulation)
7970	Management information exchange between Edge and Core appliances

Default Ports

The following table summarizes Steelhead appliance default ports with the port label: RBT-Proto.

Default Ports	Description
7744	Data store synchronization port.
7800	In-path port for appliance-to-appliance connections.
7801	Network Address Translation (NAT) port.
7810	Out-of-path server port.
7820	Failover port for redundant appliances.
7850	Connection forwarding (neighbor) port.
7860	Interceptor appliance.
7870	Steelhead Mobile.

Note: Because optimization between Steelhead appliances typically takes place over a secure WAN, it is not necessary to configure company firewalls to support Steelhead-specific ports. If there are one or more firewalls between two Steelhead appliances, ports 7800 and 7810, must be passed through firewall devices located between the pair of Steelhead appliances. Also, SYN and SYN/ACK packets with the TCP option 76 must be passed through firewalls for auto-discovery to function properly. For the CMC, port 22 must be passed through for the firewall to function properly.

Commonly Excluded Ports

This section summarizes the ports that are commonly excluded from optimization in the Steelhead appliance.

If you have multiple ports that you want to exclude, create a port label and list the ports.

Application	Ports
PolyComm (video conferencing)	1503, 1720-1727, 3230-3253, 5060
Cisco IPTel	2000

Interactive Ports Forwarded by the Steelhead Appliance

A default in-path rule with the port label **Interactive** is automatically created in your system. This in-path rule automatically passes through traffic on interactive ports (for example, Telnet, TCP ECHO, remote logging, and shell).

Tip: If you do not want to automatically forward these ports, simply delete the **Interactive** rule in the Management Console.

The following table lists the interactive ports that are automatically forwarded by the Steelhead appliance.

Port	Description
7	TCP ECHO
23	Telnet
37	UDP/Time
107	Remote Telnet Service
179	Border Gateway Protocol
513	Remote Login
514	Shell
1494	Citrix
1718-1720	h323gatedisc
2000-2003	Cisco SCCP
2427	Media Gateway Control Protocol Gateway
2598	Citrix
2727	Media Gateway Control Protocol Call Agent
3389	MS WBT Server, TS/Remote Desktop
5060	SIP
5631	PC Anywhere
5900-5903	VNC
6000	X11

Secure Ports Forwarded by the Steelhead Appliance

A default in-path rule with the port label **Secure** is automatically created in your system. This in-path rule automatically passes through traffic on commonly secure ports (for example, ssh, https, and smtps).

Tip: If you do not want to automatically forward these ports, simply delete the **Secure** rule in the Management Console.

The following table lists the common secure ports that are automatically forwarded by the Steelhead appliance.

Type	Port	Description
ssh	22/tcp	SSH Remote Login Protocol
tacacs	49/tcp	TACACS+
kerberos	88	Kerberos
rtsps	322	rtsp over TLS/SSL

Type	Port	Description
https	443/tcp	http protocol over TLS/SSL
smtps	465/tcp	# SMTP over SSL (TLS)
nntps	563/tcp	nntp protocol over TLS/SSL (was snntp)
imap4-ssl	585/tcp	IMAP4+SSL (use 993 instead)
sshell	614/tcp	SSLshell
ldaps	636/tcp	ldap protocol over TLS/SSL (was sldap)
ftps-data	989/tcp	FTP protocol, data, over TLS/SSL
ftps	990/tcp	FTP protocol, control, over TLS/SSL
telnets	992/tcp	telnet protocol over TLS/SSL
imaps	993/tcp	imap4 protocol over TLS/SSL
pop3s	995/tcp	pop3 protocol over TLS/SSL (was spop3)
l2tp	1701/tcp	l2tp
pptp	1723/tcp	pptp
tftps	3713/tcp	TFTP over TLS
operations-manager	5723	Microsoft Operations Manager

The following table contains the uncommon ports automatically forwarded by the Steelhead appliance.

Type	Port	Description
nsiiops	261/tcp	IIOP Name Service over TLS/SSL
ddm-ssl	448/tcp	DDM-Remote DB Access Using Secure Sockets
corba-iiop-ssl	684/tcp	CORBA IIOP SSL
ieee-mms-ssl	695/tcp	IEEE-MMS-SSL
ircs	994/tcp	irc protocol over TLS/SSL
njenet-ssl	2252/tcp	NJENET using SSL
ssm-cssps	2478/tcp	SecurSight Authentication Server (SSL)
ssm-els	2479/tcp	SecurSight Event Logging Server (SSL)
giop-ssl	2482/tcp	Oracle GIOP SSL
ttc-ssl	2484/tcp	Oracle TTC SSL
groove	2492	GROOVE
syncserverssl	2679/tcp	Sync Server SSL
dicom-tls	2762/tcp	DICOM TLS
realsecure	2998/tcp	Real Secure
orbix-loc-ssl	3077/tcp	Orbix 2000 Locator SSL
orbix-cfg-ssl	3078/tcp	Orbix 2000 Locator SSL
cops-tls	3183/tcp	COPS/TLS

Type	Port	Description
csvr-sslproxy	3191/tcp	ConServR SSL Proxy
xnm-ssl	3220/tcp	XML NM over SSL
msft-gc-ssl	3269/tcp	Microsoft Global Catalog with LDAP/SSL
networklenss	3410/tcp	NetworkLens SSL Event
xtrms	3424/tcp	xTrade over TLS/SSL
jt400-ssl	3471/tcp	jt400-ssl
seclayer-tls	3496/tcp	securitylayer over tls
vt-ssl	3509/tcp	Virtual Token SSL Port
jboss-iiop-ssl	3529/tcp	JBoss IIOP/SSL
ibm-diradm-ssl	3539/tcp	IBM Directory Server SSL
can-nds-ssl	3660/tcp	Candle Directory Services using SSL
can-ferret-ssl	3661/tcp	Candle Directory Services using SSL
linktest-s	3747/tcp	LXPRO.COM LinkTest SSL
asap-tcp-tls	3864/tcp	asap/tls tcp port
topflow-ssl	3885/tcp	TopFlow SSL
sdo-tls	3896/tcp	Simple Distributed Objects over TLS
sdo-ssh	3897/tcp	Simple Distributed Objects over SSH
iss-mgmt-ssl	3995/tcp	ISS Management Svcs SSL
suucp	4031/tcp	UUCP over SSL
wsm-server-ssl	5007/tcp	wsm server ssl
sip-tls	5061/tcp	SIP-TLS
imqtunnels	7674/tcp	iMQ SSL tunnel
davsrcs	9802/tcp	WebDAV Source TLS/SSL
intrepid-ssl	11751/tcp	Intrepid SSL
rets-ssl	12109/tcp	RETS over SSL

Index