riverbed®

Riverbed® Command-Line Interface Reference Manual

SteelHead™ CX/GX - RiOS Version 9.9
SteelHead EX - Version 5.5
SteelCentral™ Controller for SteelHead - Version 9.9
SteelHead Interceptor - Version 7.1
SteelCentral Controller for SteelHead Mobile - Version 6.0
SteelHead (in the cloud) - Version 9.9

December 2018

riverbed®

Riverbed Technology
680 Folsom Street
San Francisco, CA 94107
www.riverbed.com

Part Number
712-00002-27

Contents

Welcome

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.

This guide includes relevant information about these products:

- Riverbed Optimization System (RiOS)
- Riverbed SteelHead CX (SteelHead CX)
- Riverbed SteelHead EX (SteelHead EX)
- Riverbed SteelHead (in the cloud) (SteelHead-c)
- Riverbed SteelHead (virtual edition) (SteelHead-v)
- Riverbed SteelHead SaaS (SteelHead SaaS)
- Riverbed SteelHead Interceptor (Interceptor)
- Riverbed SteelCentral Controller for SteelHead (SCC or Controller)
- Riverbed SteelCentral Controller for SteelHead Mobile (Mobile Controller)

This manual provides you with command descriptions, syntax, parameters, usage guidelines, examples, and related commands information.

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, CLI parameters, and REST API properties appear in **bold** typeface.

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

< >	Values that you specify appear in angle brackets: **interface <ip-address>**
[ ]	Optional keywords or variables appear in brackets: **ntp peer <ip-address> [version <number>]**
{ }	Elements that are part of a required choice appear in braces: **{<interface-name> | ascii <string> | hex <string>}**
|	The pipe symbol separates alternative, mutually exclusive elements of a choice. The pipe symbol is used in conjunction with braces or brackets; the braces or brackets group the choices and identify them as required or optional: **{delete <filename> | upload <filename>}**

Documentation and release notes

The most current version of all Riverbed documentation can be found on the Riverbed Support site at https://support.riverbed.com.

See the Riverbed Knowledge Base for any 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 at https://support.riverbed.com.

Each software release includes release notes. The release notes list new features, known issues, and fixed problems. To obtain the most current version of the release notes, go to the Software and Documentation section of the Riverbed Support site at http://www.riverbed.com/services/index.html.

Examine the release notes before you begin the installation and configuration process.

Contacting Riverbed

This section describes how to contact departments within Riverbed.

- **Technical support** - 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** - Need help with planning a migration or implementing a custom design solution? Contact Riverbed Professional Services. Email proserve@riverbed.com or go to http://www.riverbed.com/services/index.html.
- **Documentation** - Have suggestions about Riverbed's online documentation or printed materials? Send comments to techpubs@riverbed.com.

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@ip-address
   ```
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 2017 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, Controller, SteelHead Interceptor, and SteelHead Mobile product family.

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.

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 # config 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.

2

User Mode Commands

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

User mode commands allow you to enter enable mode, display system data, and perform standard networking tasks. Monitor users can enter 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 User Guide*.

To enter user mode

- Connect to the CLI and enter the following:

```
login as: admin
Riverbed SteelHead
Last login: Wed Jan 20 13:02:09 2016 from 10.0.1.1
amnesiac >
```

System administration commands

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

enable

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

exit

Exits the CLI when in user mode; returns to enable mode when in configuration mode.

Syntax

exit

Parameters

None

Example

```
amnesiac > exit
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

ping

Sends 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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

ping6

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“ipv6 in-path-gateway”

slogin

Enables log in to another system securely using Secure Shell (SSH).

Syntax

slogin <username>@<hostname>.com [port <port-number>] [version {1 | 2}]

Parameters

<username>@<hostname>.com	Name of the user logging in to the other system and the hostname of the other system in the format <user>@<hostname>.com.
port <port-number>	Specifies the port number to which the SteelHead should connect to on the other system.
version 1	Specifies SSH protocol version 1.
version 2	Specifies SSH protocol version 2.

Usage

This command functions the same as the **ssh slogin** command.

Example

```
amnesiac > slogin jdoe@company.com
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“show ssh client,” “show ssh server”

ssh slogin

Enables log in to another system using Secure Shell (SSH).

Syntax

ssh slogin <username>@<hostname>.com [port <port-number>] [version {1 | 2}]

Parameters

<username>@<hostname>.com	Name of the user logging in to the other system and the hostname of the other system in the format <user>@<hostname>.com.
port <port-number>	Port number to which the SteelHead should connect to on the other system.
version 1	Specifies SSH protocol version 1.
version 2	Specifies SSH protocol version 2.

Usage

This command functions the same as the **slogin** command.

Example

```
amnesiac > ssh slogin jdoe@company.com
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show ssh client," "show ssh server"

---

stats export

Enables the export of statistics.

Syntax

stats export <format> <report-name> [filename <filename> | email <email-address>] [after <date> <time>] [before <date> <time>]

Parameters

<format>	File format for export. You can choose **csv** as a comma-separated format.
<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 ▪ **sharepoint** - SharePoint statistics ▪ **http_ss_bytes** - Stream splitting bytes ▪ **http_ss_sessions** - Stream splitting sessions ▪ **top-conversations** - Top conversations report ▪ **top-senders** - Top senders report ▪ **top-receivers** - Top receivers report ▪ **top-applications** - Top applications report
after <date>	Includes statistics collected after a specific date in the format yyyy/mm/dd.
<time>	Time in the format hh:mm:ss.
before <date>	Includes statistics collected before a specific date in the format yyyy/mm/dd.
email <email-address>	Specifies the address where the report is to be emailed.
filename <filename>	Specifies a filename for the new report.

Example

```
amnesiac > stats export csv ssl filename ssltest after 2014/03/01 01:00:00 before 2014/09/01 01:00:0
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“show stats bandwidth”

telnet

Logs in to another system using Telnet.

Syntax

telnet [**<telnet-options>**]

Parameters

<telnet-options>	Telnet command option. Specify one of the following options: ▪ **close** - Closes the current connection. ▪ **logout** - Forcibly logs out the remote user and closes the connection. ▪ **display** - Displays operating parameters. ▪ **mode** - Try to enter line or character mode ('mode ?' for more). ▪ **open** - Connects to a site. ▪ **quit** - Exits Telnet. ▪ **send** - Transmits special characters ('send ?' for more). ▪ **set** - Sets operating parameters ('set ?' for more). ▪ **unset** - Unset operating parameters ('unset ?' for more). ▪ **status** - Prints status information. ▪ **toggle** - Toggles operating parameters ('toggle ?' for more). ▪ **slc** - Changes state of special characters ('slc ?' for more). ▪ **z** - Suspends Telnet. ▪ **!** - Invokes a subshell. ▪ **environ** - Changes environment variables ('environ ?' for more). ▪ **?** - Prints help information.

Example

```
amnesiac > telnet display
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“show terminal”

terminal

Sets terminal settings.

Syntax

[no] terminal {length <lines> | type <terminal-type> | width <number-of-characters>}

Parameters

terminal-length <lines>	Sets the number of lines. The valid range is from 0 to 1024. 0 disables paging.
terminal-type <terminal-type>	Sets the terminal type.
terminal-width <number-of-characters>	Sets the number of characters for the width.

Usage

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

Example

```
amnesiac > terminal width 1024
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

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

traceroute

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

traceroute6

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

SCC, Interceptor, SteelHead CX, SteelHead-v, SteelHead-c

Related Commands

"ipv6 in-path-gateway"

Displaying system data

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

---

show access inbound rules

Displays the 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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"ACL management commands"

---

show access status

Displays the secure network access status.

Syntax

show access status

Parameters

None

Example

```
amnesiac > show access status
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"ACL management commands"

show admission

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 autodiscovery (CBAD) table.

Usage

After performing a model upgrade, 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Configuration file commands"

show alarm

Displays the status of the specified alarm. For detailed information about alarms, see the *SteelHead User Guide*.

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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

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

show alarms

Displays the status of all alarms. For detailed information about alarms, see the *SteelHead User 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
----------------------------------------
.
.
.
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

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

show application

Displays detailed information about a configured application.

Syntax

show application <name>

Parameters

<name>	Name of the application. Enter ? at the system prompt to view a list of predefined applications.

Example

```
amnesiac > show application Applejuice-GUI
Application 'Applejuice-GUI' configuration details:
   Description:           Represents the traffic between a host running an AppleJuice GUI and a
   host running the AppleJuice Core
   Application Group:     Standard Bulk
   Category:              File Transfer
   Business Criticality:  Low Criticality
   Application Protocol:  Applejuice-GUI
   Transport Protocol:    any
   Traffic Type:          any
   Local Subnet:          0.0.0.0/0
   Local Port:            any
   Remote Subnet:         0.0.0.0/0
   Remote Port:           any
   DSCP:                  any
   VLAN:                  any
   Tags:                  Standard Bulk, File Transfer, Low Criticality
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"application"

show applications

Displays detailed information about all configured applications.

Syntax

show applications

Parameters

None

Example

```
amnesiac > show applications
ACA-Services                          Business Critical, Networking, Highest Criticality
ACI                                   Business Critical, Networking, Medium Criticality
ACR-NEMA                              Business Bulk, File Transfer, High Criticality
Acrobat.com                           Standard Bulk, Web Services, Highest Criticality
Active-Directory-Protocol            Business Critical, Networking, Highest Criticality, Active
Directory Suite
ActiveSync                            Business Critical, Networking, Medium Criticality
AD-Backup                             Business Bulk, Networking, Highest Criticality, Active
Directory Suite
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"application"

show app-prot

Displays the details of the specified application protocol.

Syntax

show app-prot <app-prot-name>

Parameters

<app-prot-name>	Application protocol name. Enter ? at the system prompt to view a list of predefined application protocols. The application protocol names are case sensitive.

Usage

Use the **show app-prot** command to view all the configured application protocols.

Example

```
amnesiac > show app-prot Xbox-Live
Name:         Xbox-Live
Description:  Browsing Xbox and Xbox Live web pages
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"application," "show app-prots"

show app-prots

Displays all the configured application protocols.

Syntax

show app-prots

Parameters

None

Usage

Use the **show app-prot** command to view a particular application protocols.

Example

```
amnesiac > show app-prots
Application Protocols
-----------------------------------
12306.cn
126.com
2345.com
39.net
3COM-TSMUX
4399.com
4Shared
56.com
914CG
about.com
ACA-Services
ACI
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“application,” “show app-prot”

---

show appstats

Displays the application statistics configuration.

Syntax

show appstats

Parameters

None

Example

```
amnesiac # show appstats
Application Statistics:
  Enabled:    no
  Resolution: 300
  Rollup:     AVERAGE
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“appstats enable”

show apptag

Displays the details of the specified application tag.

Syntax

show apptag "<name>"

Parameters

"<name>"	Name of the application tag. The application tag name is case sensitive and you must enclose it in quotation marks.

Example

```
amnesiac > show apptag "Business Bulk"
Built-in:      True
   Applications:  NetBIOS-Session-service, SharePoint-Online, NovaBACKUP, PRINTSRV, OFTPS, Zabbix,
FASP, Panda, Eset, McAfee, Rsync, Akamai-NetSession, SharePoint, ACR-NEMA, Google-Drive, Kaspersky,
GPFS, BJNP, AD-DRS, SkyDrive, GSIFTP, AD-Description:  Browsing Xbox and Xbox Live web pages
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“application”

show apptags

Displays all the configured application tags.

Syntax

show apptags

Parameters

None

Example

```
amnesiac > show apptags
Tags
----------------------
Business Bulk
Business Critical
Business Productivity
Business Standard
Business VDI
Business Video
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“application,” “show apptag”

show authentication policy

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:     no limit
      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
Maximum characters can occur consecutively in password: 4
Prevent dictionary words in password:                   yes
Minimum days before password change allowed:            no limit
User passwords expire:                                  60 days
Warn user of an expiring password:                      7 days before
User accounts with expired passwords lock:              305 days
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Account control management commands”

show bootvar

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 2016-02-07 19:24:24 root@test:repository
Partition 2:
rbtsh/linux Columbia #2 2016-02-13 17:30:17 root@test:repository
Last boot partition: 1
Next boot partition: 1
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"hardware watchdog enable," "image boot"

---

show cascade shark

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"cascade shark enable," "user shark"

---

show cli

Displays the 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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"CLI terminal configuration commands"

---

show clock

Displays the 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: 2013/10/18
Zone: America North United_States Pacific
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"Host setup commands"

show cmc

Displays SCC-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 2013
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SteelCentral Controller for SteelHead commands"

show connection

Displays information about a single connection.

Syntax

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

Parameters

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

Example

```
amnesiac > show connection srcip 10.11.62.56 srcport 36433 dstip 10.11.60.9 dstport 7810
Type:                 Optimized (RIOS + SCPS)
Optimization policy:  SDR,LZ
Encrypted Peering (SSL SH-SH): no
Source:               10.5.148.60:49994
Destination:          172.217.3.228:443
Application:          HTTP
Reduction:            0%
Client Side:          yes
Since:                2016/03/18 17:24:00
Peer Appliance:       10.5.148.244:7810
Inner Local:          10.5.150.16:11188
Outer Local:          10.5.150.16:7801
Outer Remote:         10.5.148.60:49994
WAN Visibility Mode:  Correct Addressing

TCP Congestion Algorithm: New Reno
Dst Hostname:         www.company.com

SCPS Terminate:       OFF
SCPS Initiate:        WAN side

LAN Side Statistics
 Bytes:              59956
 Packets:            58
 Retransmitted:      0
 Fast Retransmitted: 0
 Timeouts:           0
 Congestion Window:  5

WAN Side Statistics:
 Bytes:              62015
 Packets:            49
 Retransmitted:      0
 Fast Retransmitted: 0
 Timeouts:           0
 Congestion Window:  0
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“System administration and service commands”

show connections

Displays the connections running through the appliance.

Syntax

show connections [<type>] [brief | full] | filter {<filter-string> | application <app-name>}| sort-by <state> | path-selection [full] | path-selection site-name <site-name> [full] | path-selection uplink-name <uplink-name> [site-name <site-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	Specifies a brief report.	
full	Specifies a full report.	
filter <string> | filter application <app-name>	Filters the list according to the string or application. For example, to filter by IP address (such as **srcip** or **destip**), the filter string is the IP address.	
sort-by <state>	Sorts results by the following states: ▪ **state -** Sorts connections by state. ▪ **srcip** - Sorts connections by source IP address. ▪ **srcport** - Sorts connections by source port. ▪ **destip** - Sorts connections by destination IP address. ▪ **destport** - Sorts connections by destination port. ▪ **application** - Sorts connections by application, such as HTTP. ▪ **peerip** - Sorts connections by peer IP address. ▪ **peerport** - Sorts connections by peer port. ▪ **reduction** - Sorts connections by percent of reduction in bandwidth. ▪ **bytes_in** - Sorts connections by total number of bytes in. ▪ **bytes_out** - Sorts connections by total number of bytes out. ▪ **starttime** - Sorts connections by start time. ▪ **interface** - Sorts 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 site-name <site-name> [full]	Displays a list of connections using path selection to the specified site.
path-selection uplink-name <uplink-name> [site-name <site-name>] [full]	Displays a list of connections using path selection over the specified uplink or, optionally, to the specified site over the uplink.

Example

```
amnesiac > show connections all

T   Source                Destination           App       Rdn   Since
-------------------------------------------------------------------------------
RS  10.5.132.136:51632    10.5.160.235:445      SMB-UNS   6%    2016/01/20 14:21:59
-------------------------------------------------------------------------------
                                          All    V4     V6
-----------------------------------------------------------
Established optimized:                    1      1      0

  RiOS only (O):                          0      0      0
  SCPS only (SO):                         0      0      0
  RiOS+SCPS (RS):                         0      0      0
  TCP Proxy (TP):                         0      0      0
  Web Proxy only (WP):                    0      0      0
  Web Proxy=SCPS (WS):                    0      0      0


Half-opened optimized (H):                0      0      0
Half-closed optimized (C):                0      0      0
Establishing (E):                         0      0      0

Passthrough:                              0      0      0

  Passthrough intentional (PI):           0      0      0
  Passthrough unintentional (PU):         0      0      0

Forwarded (F):                            0      0      0
Discarded (not shown):                    0
Denied    (not shown):                    0
-----------------------------------------------------------
Total:                                    1      1      0
Error:                                    1      1      0
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“System administration and service commands,” “Path selection commands”

show datastore

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Data store replication and protection commands”

---

show datastore branchwarming

Displays the current branch warming settings.

Syntax

show datastore branchwarming

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Data store replication and protection commands”

---

show datastore disk

Displays the current data store disk configuration.

Syntax

show datastore disk

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Data store replication and protection commands”

---

show datastore disklayout

Displays the current data store disk layout status.

Syntax

show datastore disklayout

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Data store replication and protection commands”

---

show datastore sdr-policy

Displays the data store SDR policy.

Syntax

show datastore sdr-policy

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Data store replication and protection commands”

show datastore sync

Displays the 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Data store replication and protection commands”

show datastore write-q-prior

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Data store replication and protection commands”

show disk state

Displays the disk status.

Syntax

show disk state

Parameters

None

Usage

Use this command to display disk status reports on SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore disk”

---

show dns cache

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“DNS cache commands”

---

show dns forwarders

Displays a list of all the forwarders.

Syntax

show dns forwarders

Parameters

None

Example

```
amnesiac > show dns forwarders
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“DNS cache commands”

show dns interfaces

Displays a list of all the interfaces.

Syntax

show dns interfaces

Parameters

None

Example

```
amnesiac > show dns interfaces
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“DNS cache commands”

show dns settings

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“DNS cache commands”

show domain

Displays the domain settings.

Syntax

show domain {configuration | settings [kerberos {realm | enctype} | dc-list] | status}

Parameters

configuration	Displays domain configuration.
settings	Displays domain settings.
kerberos realm	Displays the Kerberos KDCs for all configured realms.
kerberos enctype	Displays the configured Kerberos encryption type.
dc-list	Displays the current list of domain controllers.
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

amnesiac > show domain settings kerberos realm
Realm             KDCs
-----             ----
TEST.AUTH         dc1
                  dc2
                  dc3

amnesiac > show domain settings
Log level                       : 0
Max log size (KB)               : 25000
Password refresh interval (Day) : 0
Disable IPv6 Lookups            : yes
Use default domain              : yes
Ignore trusted domains          : no
Max winbind children allowed    : 0
Enable tdb mmap                 : yes
Domain controller list          : il-vcs268
Kerberos settings               : yes

amnesiac > show domain settings kerberos enctype
Enctype: arcfour-hmac-md5
```

Product

SteelHead CX, SteelHead EX, SteelHead-v

Related Commands

“DNS cache commands,” “domain settings”

show domain-label

Displays entries in the specified domain label.

Syntax

show domain-label <domain-label>

Parameters

<domain-label>	Domain label name.

Usage

The entries in the specified domain label are listed. Domain labels are used in in-path rules to match traffic to the specified domain.

Example

```
amnesiac (config) # show domain-label d1
Domains in domain label 'd1':
     *.dynamics.com
```

Product

SteelHead CX, SteelHead EX, SteelHead-v

Related Commands

"In-path and virtual in-path support commands," "domain-label," "show domain-labels"

show domain-labels

Displays all configured domain labels.

Syntax

show domain-labels

Parameters

None

Usage

Displays all the configured domain labels. Domain labels are used within in-path rules to match traffic to the specified domain.

Example

```
amnesiac (config) # show domain-labels
Domain label: Office
Domain label: Box
```

Product

SteelHead CX, SteelHead EX, SteelHead-v

Related Commands

"In-path and virtual in-path support commands," "domain-label," "show domain-label"

show email

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

Passthrough Rule email
  Enabled: Yes
  Notify-time : 7 day(s)
  No recipients configured.

Autosupport emails
  Enabled: no
  Recipient:
    autosupport@eng.riverbed.com
  Mail hub:
    eng.riverbed.com
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"Notification commands"

---

show failover

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, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Data store replication and protection commands"

---

show flow

Displays detailed information for a single flow.

Syntax

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

Parameters

srcip <source-ip-address>	Specifies the source IP address.
srcport <source-port>	Specifies the source port.
dstip <destination-ip-address>	Specifies the destination IP address.
dstport <destination-port>	Specifies the destination port.
protocol <protocol-name>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show flows”

show flows

Displays a list of flows.

Syntax

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

Parameters

all	Displays information about all flow types.	
<sub-type>	**destip <ip-address>**	Displays a list of flows filtered by destination IP address.
	destport <port>	Displays a list of flows filtered by destination port.
	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 site-name <site-name> [full]	Displays a list of flows using path selection to the specified site. The **full** option displays detailed information about the flows using path selection. Path selection statistics are only reported if path selection is enabled.
	path-selection uplink-name <uplink-name> [site-name <site-name>] [full]	Displays a list of flows using path selection over the specified uplink or, optionally, to the specifed site over the uplink.
	srcip <ip-address>	Displays a list of flows filtered by source IP address.
	srcport <port>	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-address>	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-address>	Displays a list of flows filtered by source IP address.
	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 site-name <site-name> [full]	Displays a list of flows using path selection to the specified site. The **full** option displays detailed information about the flows using path selection. Path selection statistics are only reported if path selection is enabled.
	path-selection uplink-name <uplink-name> [site-name <site-name>] [full]	Displays a list of flows using path selection over the specified uplink or, optionally, to the specified site over the uplink.
filter <string> | filter application <app-name>	Filters the list according to the string or application. 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. ▪ **application** - Sort connections by application. ▪ **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	Specifies a brief flow list.	
debug	Displays debug information with each flow.	
full	Displays 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“packet-mode enable,” “show flow,” “Path selection commands”

show hardware error-log

Displays intelligent platform management interface (IPMI) system event log entries.

Syntax

show hardware error-log {all | new}

Parameters

all	Displays all IPMI SEL entries.
new	Displays 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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“clear hardware error-log”

---

show hardware nic slots

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

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“hardware nic slot”

---

show hardware spec

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“clear hardware error-log”

show hardware watchdog

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

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller

Related Commands

“hardware watchdog enable”

show hosts

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“Host setup commands”

show host-label

Displays information about the specified host label.

Syntax

show host-label <name> [detailed]

Parameters

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

Example

```
amnesiac # show host-label rvbd detailed

Subnets:
23.61.194.0/24

Host www.riverbed.com:
184.25.56.107/32, 184.25.56.140/32
Resolved: 2016/01/25 11:35:36

Next scheduled resolve: 2016/01/26 11:35:31
```

Product

SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Interceptor

Related Commands

“Host label commands”

show host-labels

Displays all host label names.

Syntax

show host-labels [refresh-intvl]

Parameters

<refresh-intvl>	Displays the hostname DNS refresh interval.

Example

```
amnesiac # show host-label refresh-intvl
Hostname DNS refresh interval: 1440 minutes
```

Product

SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Interceptor

Related Commands

“Host label commands”

show images

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"License and hardware upgrade commands"

show info

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show connection"

show in-path

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“In-path and virtual in-path support commands”

---

show in-path ar-circbuf

Displays the asymmetric routing table.

Syntax

show in-path ar-circbuf

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Asymmetric route detection commands”

---

show in-path asym-route-tab

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 SteelHeads going from client to server but bypass both SteelHeads on the return path.

- **bad SYN/ACK** - Server-Side Asymmetry: Packets traverse both SteelHeads going from client to server but bypass the server-side SteelHead on the return path.
- **no SYN/ACK** - Client-Side Asymmetry: Packets traverse both SteelHeads going from client to server but bypass the client-side SteelHead on the return path.
- **probe-filtered (not-AR)** - Probe-Filtered: Occurs when the client-side SteelHead sends out multiple SYN+ frames and does not get a response.
- **probe-filtered (not-AR)** - SYN-Rexmit: Occurs when the client-side SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Asymmetric route detection commands”

show in-path bundles

Displays bundle information.

Syntax

show in-path bundles [failover-state]

Parameters

failover-state	Displays bundle link failover details.

Example

```
amnesiac > show in-path bundles
 ID   Bundle Name       Bundle interfaces
---- ----------------- -------------------
 1    bundle 1          inpath0_0,inpath0_1

amnesiac > show in-path bundles failover-state
Bundle Name  Interface   Link Status  Backup Interface  Time of Failover
-----------  ----------  -----------  ----------------  -------------------
b1           inpath0_0   Up           -                 -
b1           inpath0_1   Down         inpath3_0         2015/05/14 11:15:37
b1           inpath3_0   Up           -                 -
b1           inpath3_1   Up           -                 -
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“in-path bundle”

show in-path cdp

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Asymmetric route detection commands”

---

show in-path cf-timer

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Asymmetric route detection commands”

---

show in-path drop-when-flap

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Asymmetric route detection commands”

show in-path gre-egress-tbl

Displays the GRE tunnel egress table.

Syntax

show in-path gre-egress-tbl

Parameters

None

Usage

This command reports egress statistics about GRE-tunneled paths for the path selection feature. The command output displays GRE sources along with the number of packets and bytes received from those senders.

Example

```
amnesiac > show in-path gre-egress-tbl
source        destination   packets count    bytes count    last-rcvd(seconds ago)
10.11.4.99    10.11.6.126   21869334         23696065976    0
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“path-selection rule site application”

show in-path hw-assist rules

Displays the hardware assist rules.

Syntax

show in-path hw-assist rules

Parameters

None

Usage

On SteelHeads and SteelHead Interceptors 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 connections.

You can also configure rules for bypassing specific TCP connections. By automatically bypassing these connections, you can decrease the workload on the local SteelHeads.

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

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)
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“in-path hw-assist rule,” “in-path hw-assist edit-rule,” “in-path hw-assist move-rule rulenum”

---

show in-path lsp

Displays whether link state propagation is enabled.

Syntax

show in-path lsp

Parameters

None

Usage

When LSP is enabled, if the LAN interface drops the link, then the WAN also drops the link.

Example

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

Product

Interceptor, SteelHead CX, SteelHead-v, SteelHead-c

Related Commands

“in-path lsp enable”

---

show in-path mac-except-locl

Displays whether nonlocal peer SteelHead MAC has been configured for simplified routing. For detailed information, see the *SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“WAN visibility (transparency) commands”

---

show in-path mac-match-vlan

Displays in-path settings if VLAN IDs are used in simplified routing table lookups for WAN visibility. For detailed information, see the *SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“WAN visibility (transparency) commands”

---

show in-path macmap-except

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“WAN visibility (transparency) commands”

---

show in-path macmap-tables

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

Syntax

show in-path macmap-tables

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“WAN visibility (transparency) commands”

---

show in-path neighbor

Displays connection forwarding settings. For detailed information about connection forwarding alarms, see the *SteelHead User 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Asymmetric route detection commands,” “Connection forwarding”

---

show in-path neighbor-detail

Displays connection forwarding settings. For detailed information, see the *SteelHead User 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Asymmetric route detection commands,” “Connection forwarding”

---

show in-path neighbor advertiseresync

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Asymmetric route detection commands”

show in-path peer-probe-cach

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“in-path peer-probe-cach”

show in-path peering auto

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“in-path peering auto”

show in-path peering disc-outer-acpt

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“in-path peering rule”

show in-path peering-gre

Displays whether or not enhanced IPv4 generic routing encapsulation (GRE) tunneled auto-discovery is enabled.

Syntax

show in-path peering-gre

Parameters

None

Example

```
amnesiac # show in-path peering-gre
Enhanced IPv4 GRE tunneled Auto-Discovery Enabled:   yes
```

Related Commands

“in-path peering-gre enable”

show in-path peering-ipv6

Displays whether or not enhanced IPv6 auto-discovery is enabled.

Syntax

show in-path peering-ipv6

Parameters

None

Example

```
amnesiac > show in-path peering-ipv6
Enhanced IPv6 Auto-Discover Enabled: yes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“in-path peering-ipv6 enable”

show in-path peering oobtransparency

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"WAN visibility (transparency) commands," "in-path peering oobtransparency mode"

---

show in-path peering rules

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"in-path peering rule"

---

show in-path probe-caching

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

Syntax

show in-path probe-caching

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"WAN visibility (transparency) commands"

---

show in-path probe-ftp-data

Displays whether or not FTP connections are probed to learn VLAN information. For detailed information, see the *SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“in-path probe-ftp-data”

show in-path probe-mapi-data

Displays whether or not MAPI data connections are probed to learn VLAN information. For detailed information, see the *SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“in-path simplified routing”

show in-path rules

Displays information about one or more in-path rules.

Syntax

show in-path rules [detail <rule-number> | all | default]

Parameters

detail	Displays detailed information about the in-path rule.
<rule-number>	Rule number to display. Valid values are from 1 to 65534.
all	Displays detailed information for all in-path rules.
default	Displays detailed information for the system-generated default in-path rule.

Example - SteelHead

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

```
ID Type Source Addr        Port  Destination Addr   Port  VLAN p P O L N W K C w
--- ---- ------------------ ----- ------------------ ----- ---- - - - - - - - - -
  1 pass all-ip             all   all-ip             Secure
                                                          all  T - - - - - - A N
  2 pass all-ip             all   all-ip             Interactive
                                                          all  T - - - - - - A N
  3 pass all-ip             all   all-ip             RBT-Proto
                                                          all  T - - - - - - A N
  4 auto all-ip             all   all-ip             all   all  T N F F A C N A N
def auto all-ip             all   all-ip             all   all  T N F F A C N A A

4 user-defined rule(s)

(p) Protocol:               T=TCP U=UDP A=Any
(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 O=Outlook-anywhere
                            C=Citrix E=Exchange-Auto 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
Rules marked with * are disabled.
(C) Cloud Acceleration:     A=Auto
                            P=Passthru
(w) Web Proxy               A=Auto
                            F=Force
                            N=None
```

Example - SteelHead Interceptor

```
amnesiac (config) # show in-path rules detail 5
Rule Number: 5
Creation date: 12/15/16-13:38:33
Created by: admin, logged in from: ip: 10.34.51.71 name: user-w7.nbttech.com
        Type                : pass-through
        Send periodic email : no
        Source ip           : all-ip
        Destination ip      : all-ip
        Destination port    : all
        Vlan                : all
        Hit count           : 0
        Last hit time       : Never
        Counter clear time  : Never
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“In-path and virtual in-path support commands”

---

show in-path send-storeid

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“in-path send-storeid enable”

---

show in-path simplified routing

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Simplified routing support commands”

---

show in-path vlan-conn-based

Displays whether or not the VLAN connection-based mapping is in use. For detailed information, see the *SteelHead Deployment Guide*.

Syntax

show in-path vlan-conn-based

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“WAN visibility (transparency) commands”

---

show interfaces

Displays the running state settings and statistics.

Syntax

show interfaces [**<interface-name>**] [**brief | configured**]

Parameters

<interface-name>	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 vary 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>>
.
.
.
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“interface”

show interfaces mtu-override

Displays whether or not the MTU override setting is enabled.

Syntax

show interfaces mtu-override

Parameters

None

Example

```
amnesiac # show interfaces mtu-override
MTU sync override enabled: yes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"interface mtu-override enable"

show ip

Displays the IP settings.

Syntax

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

Parameters

flow-export	Displays NetFlow export settings.
destination <ip-address> <port>	Displays the destination IP address and NetFlow collector port.
destination-hostname <hostname> <port>	Displays the destination hostname and NetFlow collector port.
filter	Displays filters for the NetFlow collector.
flow-setting	Displays NetFlow settings.
in-path route <interface>	Displays in-path route settings for the specified interface, such as **inpath0_0**, and **inpath1_1**.
in-path-gateway <interface>	Displays in-path gateway settings for the specified interface, such as **inpath0_0** and **inpath1_1**.
static	Displays configured in-path routes.
security	Displays IPSec settings.
peers	Displays IPSec connections with peer 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

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Data flow analyzer support commands," "Host setup commands"

show limit bandwidth

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Host setup commands”

show limit connection

Displays the connection limit setting.

Syntax

show limit connection

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Host setup commands”

show logging

Displays logging and logging filter settings.

Syntax

show logging [**filter** | **facility**]

Parameters

filter	Displays per-process logging configuration information.
facility	Displays the logging facility configuration.

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

amnesiac > show logging facility
System Messages: local0
User Messages: local0
PerProcess Filter: local0
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"Logging commands"

show nettest

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Network test commands"

show ntp

Displays Network Time Protocol (NTP) settings.

Syntax

show ntp [**all**]

Parameters

all	Displays 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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, Mobile Controller, SteelHead-c

Related Commands

“Host setup commands”

show ntp active-peers

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

SCC, Interceptor, SteelHead CX, SteelHead-v, SteelHead-c, SteelHead EX

Related Commands

“Host setup commands”

---

show ntp authentication

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

SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Host setup commands”

show out-of-path

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Out-of-path support"

show packet-mode ip-channels

Displays information about the setup of IP channels between SteelHead 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 ▪ **srcport** - Port of the originating SteelHead ▪ **destip** - IP address of the destination SteelHead ▪ **destport** - Port of the destination SteelHead ▪ **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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

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

show packet-mode status

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 CX, SteelHead EX, SteelHead-v, SteelHead-c,

Related Commands

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

show path-selection channels

Displays the path-selection channel states.

Syntax

show path-selection channels [site <name>] [uplink <name>]

Parameters

site <name>	Displays the channel information associated with paths to the specified site.
uplink <name>	Displays the channel information associated with paths to the specified uplink.

Example

```
amnesiac  >show path-selection channels uplink MPLS site Bangalore
Channel ID:              5
  Status:                Up
  Interface:             inpath0_0
  Gateway IP:            172.16.113.1
  Neighbor IP:           172.16.113.12
  Active for:
     Local Uplink:       MPLS
     Remote Peer(s):     172.16.110.2, 172.16.112.2
     Remote Site:        Bangalore

     Local Uplink:       MPLS
     Remote Peer(s):     172.16.113.1(*)
     Remote Site:        Default-Site

  Probe Timeout:         2 seconds
  Probe Threshold:       2

*The IP address represents the local gateway probed because the corresponding site does not have
any configured peers.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Interceptor

Related Commands

"path-selection channel"

show path-selection interface stats

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Path selection commands"

show path-selection rules

Displays configured path-selection rules.

Syntax

show path-selection rules

Parameters

None

Example

```
amnesiac > show path-selection rules
Pos  Site  App  Uplink 1 Name  Uplink1 DSCP  Uplink 2 Name  Uplink 2 DSCP  Uplink 3 Name  Uplink3 DSCP   Default
                                                                                                      Action
1    Any   Any  None           Preserve      None           Preserve       None           Preserve       Relay
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"path-selection rule site application"

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: drop
Reflect path for probe responses:                    yes
Reflect path for optimized connection setup packets: yes
Bypass non-local transparency node packets:          no
Decrement IP TTL:                                    yes
Enable TCP MSS adjustment                            yes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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 CX, SteelHead EX, SteelHead-v, SteelHead-c, Interceptor

Related Commands

“Path selection commands”

---

show path-selection-transit-bypass status

Displays whether or not transit site bypass rules for path selection are enabled.

Syntax

show path-selection-transit-bypass status

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX

Related Commands

“path-selection-transit-bypass enable”

show peer version

Displays the peer protocol version settings.

Syntax

show peer version

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Peering commands”

show peers

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Peering commands”

show perf-test

Displays test results to verify optimization and disk-usage performance on a SteelHead-v.

Syntax

show perf-test test <test-name>

Parameters

test <test-name>	Specifies the name of the test.

Usage

Use the **perf-test run** command to run the performance test. Test results indicate the set of SteelHead-v models that can properly function at the performance levels measured in the tests.

Example

```
amnesiac > show perf-test test optimize_simulate
  Test: optimize_simulate
  Status: done
  Models: (VCX) 255U 255L 255M 255H 555L 555M 555H 755L 755M 755H 1555L 1555M
   Subtest: mixed_traffic
    Status: done
    Value: 239.060 Mbps
    Models: (VCX) 255U 255L 255M 255H 555L 555M 555H 755L 755M 755H 1555L 1555M
```

Product

SteelHead-v

Related Commands

“perf-test run”

show perf-tests

Displays test results to verify optimization and disk-usage performance on a SteelHead-v.

Syntax

show perf-test

Parameters

None

Usage

Use the **perf-test run** command to run the performance test. Test results indicate the set of SteelHead-v models that can properly function at the performance levels measured in the tests.

Example

```
amnesiac > show perf-tests
```

Product

SteelHead-v

Related Commands

“perf-test run”

show prepop

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	Displays all information for the prepopulation share or the specified share.
configuration shares	Displays configuration of the prepopulation share or the specified share.
stats shares	Displays prepopulation statistics for all shares or the specified share.
status shares	Displays status for the prepopulation shares or the specified share.
remote-path <remote-path>	Specifies the remote path of the share to be displayed. Use the format `'\\server\share'`.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“CIFS prepopulation support commands”

show prepop log dry-run

Displays the dry run log for a prepopulated share.

Syntax

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

Parameters

remote-path <remote-path>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“CIFS prepopulation support commands”

show prepop log sync

Displays the prepopulation synchronization log for the prepopulated share.

Syntax

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

Parameters

remote-path <remote-path>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“CIFS prepopulation support commands”

show prepop share policy

Displays policy information.

Syntax

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

Parameters

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

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“CIFS prepopulation support commands”

show protocol cifs

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"CIFS, SMB, SMB2, and SMB3 support commands"

show protocol cifs applock

Displays CIFS applock settings.

Syntax

show protocol cifs applock

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"CIFS, SMB, SMB2, and SMB3 support commands"

show protocol cifs ext-dir-cache

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"CIFS, SMB, SMB2, and SMB3 support commands," "protocol cifs ext-dir-cache enable"

show protocol cifs nosupport client

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“CIFS, SMB, SMB2, and SMB3 support commands”

---

show protocol cifs nosupport server

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“CIFS, SMB, SMB2, and SMB3 support commands”

---

show protocol cifs oopen

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, sldwg, sldprt, txt, vsd, xls
Extensions to always deny:
ldb, mdb
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“CIFS, SMB, SMB2, and SMB3 support commands”

---

show protocol cifs smb signing status

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“CIFS, SMB, SMB2, and SMB3 support commands”

---

show protocol cifs spoolss

Displays CIFS print spool subsystem settings.

Syntax

show protocol cifs spoolss

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol cifs spoolss enable”

---

show protocol citrix

Displays Citrix status.

Syntax

show protocol citrix [cdm | smallpkts | auto-msi]

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.
auto-msi	Displays whether Citrix autonegotiate multi-stream ICA is enabled or not.

Example

```
amnesiac > show protocol citrix
Citrix optimization enabled:                        yes
Citrix SecureICA enabled:                           yes
Citrix ICA port:                                    1494
Citrix Session Reliability (CGP) port:              2598
Citrix Multi-Port ICA enabled:                      no
Citrix Multi-Stream ICA auto-negotiation enabled:   yes
Citrix small packets optimization:                  no

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

amnesiac > show protocol citrix auto-msi
Citrix Multi-Stream ICA auto-negotiation enabled: yes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Citrix support commands”

show protocol connection

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“High-speed TCP and satellite optimization commands”

show protocol domain-auth restricted-krb

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol domain-auth restricted-krb enable"

show protocol domain-auth credentials location

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Windows domain authentication delegation commands"

show protocol domain-auth delegation auto-mode

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Windows domain authentication delegation commands"

---

show protocol domain-auth delegation delegate-user

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Windows domain authentication delegation commands"

---

show protocol domain-auth delegation rules

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Windows domain authentication delegation commands"

---

show protocol domain-auth oneway-trust

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Windows domain authentication delegation commands"

---

show protocol domain-auth replication replicate-user

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol domain-auth auto-conf replication"

---

show protocol eos

Displays Exchange Optimization Services settings.

Syntax

show protocol eos

Parameters

None

Example

```
amnesiac > show protocol eos
MAPI over HTTP Optimization Enabled:                    yes
MAPI over HTTP Bandwidth-Only Optimization Enabled:     yes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol eos moh enable”

---

show protocol fcip rules

Displays Fiber Channel over IP (FCIP) 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“FCIP support commands”

---

show protocol fcip settings

Displays Fiber Channel over IP (FCIP) optimization settings.

Syntax

show protocol fcip settings

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“FCIP support commands”

show protocol ftp

Displays FTP settings.

Syntax

show protocol ftp

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“FTP support commands”

show protocol http

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“HTTP support commands”

show protocol http auto-config selection

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
Stream Splitting:            no
Sharepoint FPSE:             no
Sharepoint WebDAV:           no
Sharepoint FSSHTTP:          yes
HTTP2:                       yes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol http auto-config selection”

---

show protocol http metadata-resp

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“HTTP support commands”

show protocol http prefetch extensions

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“HTTP support commands”

show protocol http prefetch tags

Displays HTTP prefetched 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“HTTP support commands”

show protocol http prepop

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

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

show protocol http prepop status

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

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

show protocol http prepop verify-svr-cert

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol http prepop verify-svr-cert enable”

show protocol http server-table

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol http server-table”

show protocol mapi

Displays messaging application programming interface (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 Encryption NTLM Bypass:    no
MAPI 2k7 Force NTLM Auth:       yes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol mapi enable"

show protocol ms-sql

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"MS-SQL blade support commands"

show protocol ms-sql rules

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
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"MS-SQL blade support commands"

---

show protocol nfs

Displays NFS server and volume settings.

Syntax

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

Parameters

server <name>	Displays information for the NFS server specified by name.
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 file system ID.
servers	Displays settings for NFS servers.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"NFS support commands"

---

show protocol notes

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Lotus Notes commands"

---

show protocol oracle-forms

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Oracle forms support commands"

---

show protocol saas identity o365 status

Displays whether or not SaaS identity tracking for Office 365 is enabled.

Syntax

show protocol saas identity o365 status

Parameters

None

Example

```
amnesiac (config) # show protocol saas identity o365 status
Saas Identity tracking enabled for Office 365: yes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol saas identity o365 enable”

show protocol smb2

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

Syntax

show protocol smb2 {status | signing status}

Parameters

status	Displays whether or not the SMB2 protocol is enabled or disabled.
signing status	Displays whether SMB2 signing is enabled (yes or no) and which SMB2 signing mode is configured (transparent or delegation).

Example

```
amnesiac > show protocol smb2 status
SMB2 Enabled: yes
SMB3 Enabled: yes
DFS Enabled: yes

amnesiac > show protocol smb2 signing status
SMB2 Signing Enabled:                yes
Mode Type:                           delegation
SMB2 Signing End-to-End Kerberos:    yes
End-to-End Kerberos Downgrad Support: yes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol smb2 signing enable,” “protocol smb2 signing mode-type,” “protocol smb2 signing native-krb enable”

show protocol snapmirror

Displays the filer configuration settings for one or all filers.

Syntax

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

Parameters

filer <name>	Specifies the name of the filer.
volume <volume-name>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“SnapMirror support commands”

show protocol snapmirror stats

Displays statistics for SnapMirror selective optimization.

Syntax

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

Parameters

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

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SnapMirror support commands"

show protocol snapmirror settings

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SnapMirror support commands"

show protocol ssl hsm safenet

Displays the connection configurations between the Hardware Security Module (HSM) and the SteelHead appliance.

Syntax

show protocol ssl hsm safenet

Parameters

None

Usage

This command displays the SafeNet HSM devices registered on the SteelHead and the HSM partitions assigned to the SteelHead and their corresponding slot number.

Example

```
amnesiac (config) # show protocol ssl hsm safenet

Registered Safenet HSM device list:
 Server: sv-safenet1    HTL required: no
Connected Safenet HSM server info:
The following Luna SA Slots/Partitions were found:

Slot    Serial #        Label
====    ========        =====
 1      469809010       par01
 2      469809011       par02
```

Product

SteelHead CX

Related Commands

“protocol ssl hsm slot”

show protocol ssl hsm server-cert

Displays a server certificate with a private key on the Hardware Security Module (HSM).

Syntax

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

Parameters

name <name>	Specifies the server certificate name.
certificate	Displays a server certificate with private keys.
certificate raw	Displays a server certificate with private keys in raw PEM format.
certificate text	Displays a server certificate with private keys with full details.

Example

```
amnesiac # show protocol ssl hsm server-cert name hsmservercert
```

Product

SteelHead CX

Related Commands

“protocol ssl hsm server-cert import-cert”

show protocol ssl hsm server-certs

Displays server certificates with private keys on the Hardware Security Module (HSM).

Syntax

show protocol ssl hsm server-certs

Parameters

None

Usage

The system checks every 5 minutes to see if all the private keys were loaded. An SSL alarm is enabled on the user interface if the server-side SteelHead can’t import the private key corresponding to the proxy certificate from the HSM. Check that the server-side SteelHead can access the HSM device and that the private key exists on the HSM server.

Example

```
amnesiac # show protocol ssl hsm server-certs
HSM Server Certificates:
Name              (Issued To)        Key Accessible
pq-ssl-test       (pq-ssl-test)      Yes
rsa1024           (johndoe)          Yes
rsa2048           (*.*.*)            Yes
10.34.42.36       (10.34.42.36)      No
```

Product

SteelHead CX

Related Commands

“protocol ssl hsm server-cert import-cert”

show qos bandwidth

Displays QoS bandwidth settings.

Syntax

show qos bandwidth

Parameters

None

Example

```
amnesiac > show qos bandwidth

Uplink: wan1_1 (up/down : 1000000/1000000 Kbps)
Site Name      Outbound BW (Kbps)    Inbound BW (Kbps)
-----------  --------------------  -------------------
DefaultSite               1000000              1000000


Uplink: wan1_0 (up/down : 1000000/1000000 Kbps)
Site Name      Outbound BW (Kbps)    Inbound BW (Kbps)
-----------  --------------------  -------------------
DefaultSite               1000000              1000000
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos profile class-params”

show qos control-packets dscp

Displays the global differentiated services code point (DSCP) marking.

Syntax

show qos control-packets dscp

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos control-packets”

show qos profile

Displays the specified profile configuration.

Syntax

show qos profile <name> [rules]

or

show qos profiles

Parameters

<name>	QoS profile name.
rules	Displays the rules of the QoS profile.

Usage

The **show qos profiles** command shows information about all the configured QoS profiles.

Example

```
amnesiac > show qos profile Default

 Class Name        Priority  Min BW   Max BW  Climit   Queue  Parent  OB Queue   IB Queue   DSCP
                                                                       Length     Length

 RealTime             1         10      100     0       SFQ                     1024      Preserve
 Interactive          2         20      100     0       SFQ                     1024      Preserve
 BusinessCritical     3         20      100     0       SFQ                     1024      Preserve
 Normal               4         40      100     0       SFQ                     1024      Preserve
 Low Priority         5         9       100     0       SFQ                     1024      Preserve
 Best Effort          6         1       100     0       SFQ                     1024      Preserve

QoS Type      Site Associated
------------  -----------------
Inbound QoS   Local, DefaultSite
Outbound QoS  Local, DefaultSite
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos profile rule”

show qos settings

Displays QoS configured settings.

Syntax

show qos settings

Parameters

None

Example

```
amnesiac > show qos settings

Outbound Shaping:  Disabled
Inbound Shaping:   Disabled
```

```
DSCP Marking:      Disabled

Outbound Shaping:
Interface    State
-----------  --------
wan0_1       Disabled
wan0_0       Disabled
primary      Disabled
wan1_0       Disabled
wan1_1       Disabled

Inbound Shaping:
Interface    State
-----------  --------
wan1_0       Disabled
wan1_1       Disabled
wan0_1       Disabled
wan0_0       Disabled
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos dscp-marking enable,” “qos inbound shaping enable,” “qos outbound shaping enable”

---

show stats protocol snapmirror

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>	Specifies the name of the filer.
volume <volume-name>	Specifies the volume name.
total	Displays the total bytes transferred instead of throughput.
interval <time-interval>	Specifies 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">	Specifies the start time to collect SnapMirror statistics. Use the format "yyyy/mm/dd hh:mm:ss" (enclosed in quotation marks).
end-time <"yyyy/mm/dd hh:mm:ss">	Specifies the end time to stop collecting SnapMirror statistics. Use the format "yyyy/mm/dd hh:mm:ss" (enclosed in quotation marks).

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“SnapMirror support commands”

show protocol srdf rules

Displays rules for isolating DIF headers within the Symmetrix Remote Data Facility (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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“SRDF support commands”

show protocol srdf settings

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SRDF support commands"

show protocol srdf symm

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

Syntax

show protocol srdf symm [id <symmetrix-id>] [base-rdf-group <rdf-number-base> | [rdf_group <rdf-group>] stats [brief] [live [interval <seconds>]]

Parameters

id <symmetrix-id>	Specifies a Symmetrix ID. The Symmetrix ID is an alphanumeric string that can contain hyphens and underscores (for example, a standard Symmetrix serial number: 000194900363). Do not use spaces or special characters.
base-rdf-group <rdf- number-base>	Specifies 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>	Specifies an RDF group number (0 to 254).
stats brief	Displays output with a minimum amount of detail.
stats live	Displays statistics that are periodically updated.
interval <seconds>	Specifies the time interval in which to refresh the statistics.

Usage

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

If the Symmetrix ID is omitted, the statistics for all Symmetrix IDs on this SteelHead are displayed.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“SRDF support commands”

---

show protocol ssl

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
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“SSL support commands”

---

show protocol ssl backend

Displays Secure Sockets Layer (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: 31536000 seconds
```

```
Bypass table maximum size:                              2300
Renegotiation with NULL certificates enabled:           no
Certificate chain caching enabled:                      no
SNI enabled:                                            no
Client TLSv1.2:                                         yes
Server TLSv1.2:                                         yes
Include proxy SAN in certificate selection:             no
Forward ALPN extension                                  yes
OCSP Stapling level                                      off
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

show protocol ssl backend bypass-table

Displays the list of bypassed servers.

Syntax

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

Parameters

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

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

show protocol ssl backend client cipher-strings

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.
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“SSL support commands”

show protocol ssl backend disc-table

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“SSL support commands”

show protocol ssl backend server cipher-strings

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

show protocol ssl ca certificate

Displays a CA certificate.

Syntax

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

Parameters

ca <ca-name>	Specifies the CA name.
certificate raw	Displays SSL CA certificate in raw format.
certificate text	Displays SSL CA certificate in 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:
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

show protocol ssl cas

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)
  .
  .
  .
```

Product

Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“SSL support commands”

show protocol ssl client-cer-auth

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

show protocol ssl client-side session-reuse

Displays client-side SSL connection reuse settings.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

show protocol ssl crl

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 an automatically discovered certificate authority (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 overridden 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

---

show protocol ssl expiring-certs

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

---

show protocol ssl midsession-ssl

Displays midsession SSL settings.

Syntax

show protocol ssl midsession-ssl

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

show protocol ssl proxy-support

Displays SSL proxy settings.

Syntax

show protocol ssl proxy-support

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol ssl proxy-support enable"

show protocol ssl server-cert name

Displays an SSL server certificate.

Syntax

show protocol ssl server-cert name <name>

Parameters

<name>	Server certificate name.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

show protocol ssl server-cert name certificate

Displays an SSL server certificate.

Syntax

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

Parameters

<name>	Server certificate name.
[raw | text]	Specifies the format type for the certificate.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

show protocol ssl server-cert name chain-cert

Displays a SSL server chain certificate.

Syntax

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

Parameters

<name>	Server certificate name.
<cert-name>	Certificate name.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

show protocol ssl server-cert name chain-certs

Displays the SSL server chain certificates.

Syntax

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

Parameters

<name>	Server certificate name.
<cert-name>	Certificate name.
certificate	Displays the certificate.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands"

show protocol ssl server-certs

Displays the SSL server certificate.

Syntax

show protocol ssl server-certs

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX

Related Commands

"SSL support commands"

show public-ip

Displays public IP addresses.

Syntax

show public-ip [interface <name>]

Parameters

interface <name>	Displays public IP addresses for an interface.

Example

```
amnesiac # show public-ip
1 public address configured for inpath0_0
1: 10.5.5.5:4500
1 public address configured for ipath0_1
1: 10.6.5.5:4500
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"interface"

show raid configuration

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"RAID commands"

show raid diagram

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"RAID commands"

show raid error-msg

Displays RAID error messages.

Syntax

show raid error-msg

Parameters

None

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"RAID commands"

show raid info

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"RAID commands"

show raid physical

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
.
.
.
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“RAID commands”

show report

Displays system details.

Syntax

show report {all | system | service}

Parameters

all	Displays a complete system detail report.
system	Displays system resources.
service	Displays 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show info," "show stats bandwidth"

---

show rps

Displays whether or not the Receive Packet Steering (RPS) feature is enabled.

Syntax

show rps

Parameters

None

Example

```
amnesiac > show rps
RPS enabled on SteelHead: no
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-c

Related Commands

"rps enable"

---

show scc

Displays settings for the SCC.

Syntax

show scc

Parameters

None

Usage

The SteelCentral Controller for SteelHead is required to manage the secure transport deployment. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac > show scc
Auto-registration:              Enabled
HTTPS connection (to the CMC):
        Status:                 Connected
        Hostname:               chief-cmc4
SSH connection (from the CMC):
        Status:                 Connected
        Hostname:               chief-cmc4 (10.1.16.92)
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"scc enable," "scc hostname"

---

show scep service

Displays SCEP service status.

Syntax

show scep service

Parameters

None

Example

```
amnesiac > show scep service
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"scep service restart"

---

show secure-peering

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
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Secure peering (secure inner channel) commands"

show secure-peering black-lst-peer

Displays self-signed black list peers in secure peering.

Syntax

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

Parameters

<ip-address>	IP address of the black list peer.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Secure peering (secure inner channel) commands"

show secure-peering black-lst-peers

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Secure peering (secure inner channel) commands"

show secure-peering ca

Displays a specified peering certificate authority (CA) certificate.

Syntax

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

Parameters

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

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Secure peering (secure inner channel) commands"

show secure-peering cas

Displays all configured secure peering CA certificates.

Syntax

show secure-peering cas

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Secure peering (secure inner channel) commands"

show secure-peering certificate

Displays a certificate.

Syntax

show secure-peering certificate [raw | text]

Parameters

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

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Secure peering (secure inner channel) commands"

show secure-peering cipher-strings

Displays the cipher strings used for peering.

Syntax

show secure-peering cipher-strings [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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Secure peering (secure inner channel) commands”

show secure-peering crl

Displays a certificate.

Syntax

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

Parameters

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

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Secure peering (secure inner channel) commands”

show secure-peering crl report ca

Displays a report of a secure-peering CRL certificate.

Syntax

show secure-peering crl report ca <string>

Parameters

<string>	Name of a secure peering CA certificate.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Secure peering (secure inner channel) commands"

show secure-peering gray-lst-peer

Displays self-signed gray list peers for the specified IP address.

Syntax

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

Parameters

<ip-address>	IP address of the gray list peer.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Secure peering (secure inner channel) commands"

show secure-peering gray-lst-peers

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Secure peering (secure inner channel) commands"

show secure-peering mobile-trust

Displays trusted SteelCentral Controller for SteelHead Mobile entities that can sign certificates for SteelHead Mobile product family clients.

Syntax

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

Parameters

<cert-name>	Certificate name.
certificate raw	Displays the certificate in raw format.
certificate text	Displays the certificate in text format.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Secure peering (secure inner channel) commands”

show secure-peering mobile-trusts

Displays trusted SteelCentral Controller for SteelHead Mobile entities that can sign certificates for SteelHead Mobile product family clients.

Syntax

show secure-peering mobile-trusts

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Secure peering (secure inner channel) commands”

show secure-peering scep

Displays SCEP information.

Syntax

show secure-peering scep

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Secure peering (secure inner channel) commands”

---

show secure-peering scep auto-reenroll csr

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Secure peering (secure inner channel) commands”

---

show secure-peering scep auto-reenroll last-result

Displays the result of the last completed automatic reenrollment.

Syntax

show secure-peering scep auto-reenroll last-result

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Secure peering (secure inner channel) commands”

---

show secure-peering scep ca certificate

Displays a specified SCEP peering CA certificate.

Syntax

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

Parameters

<cert-name>	Certificate name.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Secure peering (secure inner channel) commands"

show secure-peering scep enrollment status

Displays SCEP enrollment status.

Syntax

show secure-peering scep enrollment status

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Secure peering (secure inner channel) commands"

show secure-peering scep on-demand csr

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Secure peering (secure inner channel) commands"

show secure-peering scep on-demand last-result

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Secure peering (secure inner channel) commands”

show secure-peering white-lst-peer

Displays self-signed white list peers.

Syntax

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

Parameters

<ip-address>	IP address of the white list peer.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Secure peering (secure inner channel) commands”

show secure-peering white-lst-peers

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Secure peering (secure inner channel) commands”

show service

Displays whether services are running.

Syntax

show service

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“System administration and service commands”

show service connection pooling

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Connection pooling commands”

show service neural-framing

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“In-path and virtual in-path support commands”

show service ports

Displays service port settings.

Syntax

show service ports

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“System administration and service commands”

show single-ended rules

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“single-ended rule optimized scps-discover,” “single-ended rule optimized tcp-proxy”

---

show snmp

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“SNMP commands”

---

show snmp acl-info

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"SNMP commands"

---

show snmp ifindex

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"SNMP commands"

---

show snmp usernames

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

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller

Related Commands

“SNMP commands”

show ssh client

Displays the client settings.

Syntax

show ssh client [private | known-hosts]

Parameters

private	Displays SSH client public and private keys.
known-hosts	Displays the SSH client known hosts.

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“Secure shell access commands”

show ssh server

Displays the SSH server.

Syntax

show ssh server [allowed-ciphers| allowed-macs | publickey]

Parameters

allowed-ciphers	Displays SSH server allowed ciphers.
allowed-macs	Displays SSH server allowed MACs.
publickey	Displays 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
```

```
amnesiac > show ssh server allowed-macs
SSH server allowed MACs:
--------------------------
hmac-sha1
hmac-sha2-256
hmac-sha2-512
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“Secure shell access commands”

show stats bandwidth

Displays the bandwidth statistics.

Syntax

show stats bandwidth {<port> | all} {bi-directional | lan-to-wan | wan-to-lan} <time-period>

Parameters

<port> | all	Specifies all ports or a specified port.
bi-directional	Displays bandwidth statistics about bidirectional traffic.
lan-to-wan	Displays bandwidth statistics about lan-to-wan traffic.
wan-to-lan	Displays bandwidth statistics about wan-to-lan traffic.
<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“System administration and service commands”

show stats conn-pool

Displays the connection pooling statistics.

Syntax

show stats conn-pool <time-period>

Parameters

<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Connection pooling commands”

show stats connections

Displays connection statistics.

Syntax

show stats connections <time-period>

Parameters

<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

Example

```
amnesiac > show stats connections hour
Avg Total Optimized:   0
Peak Total Optimized:  0 (2014/10/17 17:26:23)
   Avg Established:    0
   Peak Established:   0 (2014/10/17 17:26:23)
   Avg Half Opened:    0
   Peak Half Opened:   0 (2014/10/17 17:26:23)
   Avg Half Closed:    0
   Peak Half Closed:   0 (2014/10/17 17:26:23)
Avg Active Optimized:  0
Peak Active Optimized: 0 (2014/10/17 17:26:23)
Avg Pass Through:      0
Peak Pass Through:     0 (2014/10/17 17:26:23)
Avg Forwarded:         0
Peak Forwarded:        0 (2014/10/17 17:26:23)
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Connection pooling commands”

show stats cpu

Displays connection pooling statistics.

Syntax

show stats cpu <time-period>

Parameters

<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

Example

```
amnesiac > show stats cpu
CPU 1
  Utilization:                3%
  Peak Utilization Last Hour: 10% at 2014/10/17 18:10:03
  Avg. Utilization Last Hour: 4%

CPU 2
  Utilization:                7%
  Peak Utilization Last Hour: 9% at 2014/10/17 17:43:13
  Avg. Utilization Last Hour: 4%
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show stats memory"

show stats datastore

Displays data store statistics.

Syntax

show stats datastore <time-period>

Parameters

<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Data store configuration commands"

show stats dns

Displays the DNS statistics.

Syntax

show stats dns <time-period>

Parameters

<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

Example

```
amnesiac > show stats dns hour
Total Requests:             0
```

```
Cache Hit Rate:             0%
Average Cache Entries:      0
Average Cache Usage:        0 Bytes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"DNS cache commands"

---

show stats ecc-ram

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show stats memory"

---

show stats fan

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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show hardware error-log"

---

show stats http

Displays HTTP statistics.

Syntax

show stats http <time-period>

Parameters

<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

Example

```
amnesiac > show stats http 5min
---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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“HTTP support commands”

show stats memory

Displays memory swapping statistics.

Syntax

show stats memory <time-period>

Parameters

<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

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:                     2016/02/17 17:37:41
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“show stats ecc-ram”

show stats neighbor-fwd all

Displays connection forwarding statistics. For detailed information about alarms, see the *SteelHead User Guide*.

Syntax

show stats neighbor-fwd all {packet | byte} <time-period>

Parameters

packet	Specifies the packet count statistics.
byte	Specifies the byte count statistics.
<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

Example

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

Total Sent:          0 packets
Data Sent Peak:      0 packets
Data Sent Peak Time: 2016/02/17 17:42:20
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Connection forwarding”

show stats nfs all

Displays NFS statistics.

Syntax

show stats nfs all <time-period>

Parameters

<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

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:        2015/03/09 14:34:23
Capacity Increase:               1X
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“NFS support commands”

show stats protocol srdf

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>	Specifies a Symmetrix ID. The Symmetrix ID is an alpha-numeric string (for example, a standard Symmetrix serial number : 000104900363).
rdf-group <rdf-group>	Specifies 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>	Specifies 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>	Specifies the start time to collect SRDF statistics. Use the format "yyyy/mm/dd hh:mm:ss" (enclosed in quotation marks).
end-time <yyyy/mm/dd hh:mm:ss>	Specifies the end time to stop collecting SRDF statistics. Use the format "yyyy/mm/dd hh:mm:ss" (enclosed in quotation marks).

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 6.1 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 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 2014/09/30
                     Peak WAN Tput: 3,073.7 Kbps at 11:00:00 on 2014/09/30
```

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 2014/09/30
                    Peak WAN transfer: 5,763 KB at 11:00:00 on 2014/09/30
```

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

```
amnesiac > show stats protocol srdf symm id 6000000060 start-time "2014/11/04 16:17:00" end-time
"2014/11/11 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 2014/11/10
                    Peak WAN Tput: 57,901.5 Kbps at 09:00:00 on 2014/11/10

6000000060          2          2,142.3            412.4              80.75%
                    Peak LAN Tput: 56,982.9 Kbps at 09:00:00 on 2014/11/10
                    Peak WAN Tput: 10,970.0 Kbps at 09:00:00 on 2014/11/10

6000000060          3          2,142.3            20.1               99.06%
                    Peak LAN Tput: 56,993.5 Kbps at 09:00:00 on 2014/11/10
                    Peak WAN Tput: 2,736.1 Kbps at 16:00:00 on 2014/11/07

6000000060          Total      21,423.0           2,751.8            87.16%
                    Peak LAN Tput: 569,949.3 Kbps at 09:00:00 on 2014/11/10
                    Peak WAN Tput: 72,609.9 Kbps at 09:00:00 on 2014/11/10
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“SRDF support commands”

---

show stats qos-inbound

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>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos inbound interface enable,” “qos inbound shaping enable”

show stats qos-outbound

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>	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>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos outbound interface enable,” “qos outbound shaping enable”

show stats settings app-vis

Displays whether or not the application visibility feature is enabled.

Syntax

show stats settings app-vis [disk-params]

Parameters

disk-params	Displays the disk parameter configuration.

Usage

Use the **stats settings app-vis enable** command to enable the application visibility feature. See the *SteelHead User Guide* for information about viewing Application Statistics reports.

Example

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

amnesiac > show stats settings app-vis disk-params
Disk Name:        /var
Threshold:        90 %
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“stats settings app-vis enable”

show stats settings bandwidth

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Top Talkers commands,” “Statistics manipulation commands”

show stats sharepoint

Displays Sharepoint optimization statistics.

Syntax

show stats sharepoint <time-period>

Parameters

<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

Example

```
amnesiac > show stats sharepoint 5min

---SharePoint FPSE Stats---
   Total FPSE Requests:  0
   Total FPSE Hits:      0

---SharePoint WebDAV Stats---
   Total WebDAV Requests:  0
   Total WebDAV Hits:      0
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Statistics manipulation commands"

show stats ssl

Displays SSL statistics.

Syntax

show stats ssl <time-period>

Parameters

<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SSL support commands," "Statistics manipulation commands"

show stats throughput

Displays throughput statistics.

Syntax

show stats throughput {<port> | all} {bidirectional | lan-to-wan | wan-to-lan} <time-period>

Parameters

<port>	Port number.
all	Specifies all ports
bidirectional	Displays throughput statistics about bidirectional traffic.
lan-to-wan	Displays throughput statistics about lan-to-wan traffic.
wan-to-lan	Displays throughput statistics about wan-to-lan traffic.
<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

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:       2014/10/18 10:56:30


WAN Link Throughput
Average Throughput:         0 bps
95th Percentile Throughput: 0 bps
Peak Throughput:            0 bps
Peak Throughput Time:       2014/10/18 10:56:30
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Statistics manipulation commands”

show stats top-talkers

Displays top talkers statistics.

Syntax

show stats top-talkers [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 2014/09/10 05:00:00
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Top Talkers commands”

show stats top-talkers protocol

Displays top talkers protocol statistics.

Syntax

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

Parameters

protocol {tcp | udp | both}	Displays top talkers for the specified protocol: TCP, UDP, or both.
[start-time <start-time>] [end-time <end-time>]	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 145.

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 CX, SteelHead EX

Related Commands

"Top Talkers commands"

show stats top-talkers report

Displays top talkers report statistics.

Syntax

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

Parameters

report conversation [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 [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.
src_host_only [start-time <start-time> end-time <end-time>]	Displays top sources generating traffic. Optionally, specify the start and end time. Use the following format: yyyy/mm/dd hh:mm:ss.
ignore_ports [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 [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 [start-time <start-time> end-time <end-time>]	Displays 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Top Talkers commands”

show stats top-talkers top-n

Displays the statistics for the specified number of top talkers.

Syntax

show stats top-talkers top-n <top-number> | [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]] | [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 147.
[traffic [optimized | pass-through | both] | [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 147.
[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 145.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Top Talkers commands"

show stats top-talkers traffic

Displays top talkers traffic statistics.

Syntax

show stats top-talkers traffic [optimized | pass-through | both] | [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 145.
[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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Top Talkers commands"

show stats traffic optimized

Displays the optimized traffic statistics.

Syntax

show stats traffic optimized {bidirectional | lan-to-wan | wan-to-lan} <time-period>

Parameters

bidirectional	Displays optimized traffic statistics about bidirectional traffic.
lan-to-wan	Displays optimized traffic statistics about lan-to-wan traffic.
wan-to-lan	Displays optimized statistics about wan-to-lan traffic.
<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

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%
```

If your SteelHead has been configured for SaaS, you can view statistics about the SaaS applications. However, the mapping between the port and the application could vary from customer to customer. For one customer, Office365 could map to port 56500 and for another customer, Office365 could map to port 55001.

```
amnesiac > show stats traffic optimized bi-directional month
Port                          Rdx%  LAN Data      WAN Data   Trf%
```

```
---------------------------  ----  --------      --------   ----
Total Traffic                           13.3 MB     8.4 MB
SVCNOW (55006)               55.80%      6.1 MB     2.7 MB   46.17%
O365 (56500)                 27.20%      5.1 MB     3.7 MB   38.27%
SSL (443)                     0.00%      1.2 MB     1.2 MB    9.01%
SFSF (55007)                 22.04%    422.4 KB   329.3 KB    3.09%
SFDC (56529)                 16.04%    314.6 KB   264.1 KB    2.30%
BOX (55004)                   0.00%    156.4 KB   161.5 KB    1.15
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Statistics manipulation commands”

show stats traffic passthrough

Displays the pass-through traffic statistics.

Syntax

show stats traffic passthrough <time-period>

Parameters

<time-period>	Time period for which to display statistics: **1min**, **5min**, **hour**, **day**, **week**, **month**.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Statistics manipulation commands”

show stp-client controller

Displays SteelHead controller information on the secure transport client.

Syntax

show stp-client controller

Parameters

None

Usage

This information is pushed to the secure transport client from the SCC.

Example

```
amnesiac > show stp-client controller

Controller Properties:

  Private address:        10.5.36.91
```

```
  Public address:         1.1.1.1:3333
  Status:                 Connected
  Last keep-alive:        2014/10/23 09:23:44
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“stp-controller address”

show stp-client group

Displays secure transport group configuration information.

Syntax

show stp-client group <group-name>

Parameters

<group-name>	Group name.

Usage

This command displays an extensive list of information about the secure transport client group such as group properties, aggregate statistics, current key, previous key, and peers. The SCC pushes all group information, including the group name, to the client.

Example

```
amnesiac > show stp-client group Default_Group

Group Properties:

  Name:                           Default_Group
  ID:                             1
  Encryption Algorithm:           AES-256 (CBC)
  Authentication Algorithm        SHA-256 (HMAC)

  Disconnected Mode Timeout:      120 seconds
  Rekey Interval:                 83 minutes (s)
  Rekey Data-size:                4194304 MB

  Last group key update:          2014/08/26 08:47:01

Aggregate Statistics:

  Bytes Decrypted:                17679240
  Bytes Encrypted:                17680800
  Packets Decrypted:              226598
  Packets Encrypted:              226618
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show stp-client peers”

show stp-client groups

Displays secure transport configuration information about all groups.

Syntax

show stp-client groups

Parameters

None

Usage

This command displays an extensive list of information about all the secure transport client groups such as group properties, aggregate statistics, current key, previous key, and peers. The SCC pushes all group information, including the group name, to the client.

Example

```
amnesiac > show stp-client groups

Group Properties:

  Name:                          Default_Group
  ID:                            1
  Encryption Algorithm:          AES-256 (CBC)
  Authentication Algorithm       SHA-256 (HMAC)

  Disconnected Mode Timeout:     120 seconds
  Rekey Interval:                83 minutes (s)
  Rekey Data-size:               4194304 MB

  Last group key update:         2014/08/26 08:47:01

Aggregate Statistics:

  Bytes Decrypted:               17679240
  Bytes Encrypted:               17680800
  Packets Decrypted:             226598
  Packets Encrypted:             226618
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show stp-client peers”

show stp-client peer

Displays secure transport peer configuration information.

Syntax

show stp-client peer <peer-name>

Parameters

<peer-name>	Peer name.

Usage

Use the **show stp-client peers** command to display information about all of the configured peers.

Example

```
amnesiac > show stp-client peer sh1
Peer Name    Peer ID        Group Name  Status    End-points                              Subnets
---------  -----------  -------------  --------  ----------------------------------  ---------
sh1       VC1WW00015ed8  Default_Group  Online    10.11.100.4 10.11.200.4 2.2.2.2:4500  10.11.0.0/16
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show stp-client group," "show stp-client peers"

show stp-client peers

Displays secure transport peer(s) configuration information.

Syntax

show stp-client peers

Parameters

None

Usage

Use the **show stp-client peers** command to display information about all of the configured peers.

Example

```
amnesiac > show stp-client peers
Peer Name    Peer ID        Group Name  Status    End-points                              Subnets
---------  -----------  -------------  --------  ----------------------------------  ---------
sh1       VC1WW00015ed8  Default_Group  Online    10.11.100.4 10.11.200.4 2.2.2.2:4500  10.11.0.0/16
sh3       VC1WW00015ed9  Default_Group  Online    10.31.100.4 10.13.200.4 2.2.3.3:4500  10.13.0.0/16
sh4       VC1WW00015ed4  Default_Group  Online    10.41.100.4 10.14.200.4               10.14.0.0/16
sh5       VC1WW00015ed3  Default_Group  Online    10.51.100.4 10.15.200.4               10.15.0.0/16
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show stp-client group," "show stp-client peer"

show stp-client settings

Displays secure transport client configuration settings.

Syntax

show stp-client settings

Parameters

None

Usage

This command displays the STP concentrator mode configuration, the STP controller in-path configuration to reach the controller's private and public IP address, and the last known successful connections to the controller's private and public IP address.

Example

```
amnesiac > show stp-client settings
Secure Transport Service settings:

Concentrator mode:     Disabled

Controller Connectivity over Inpath Config:

Status:                                  False
Interface to reach controller private IP: Not configured
Interface to reach controller public IP:  Not configured

Secure-Transport OCD Interface last used successfully:

Interface to controller private IP:        inpath0_0
Interface to controller public IP:         aux
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"stp-client stc enable," "stp-client controller in-path enable"

---

show stp-client status

Displays the status of the secure transport client.

Syntax

show stp-client status

Parameters

None

Usage

This secure transport service is enabled by default. When GRE and secure transport are both enabled, secure transport takes precedence.

Example

```
amnesiac > show stp-client status
Secure Transport service status: running
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show stp-client group"

---

show stp-controller address

Displays the SteelHead controller IP address.

Syntax

show stp-controller address

Parameters

None

Example

```
amnesiac > show stp-controller address
Controller Properties:

Private address: 10.5.12.198
Public address:  Not configured
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“stp-controller address”

---

show stp-controller status

Displays whether or not the SteelHead controller is enabled.

Syntax

show stp-controller status

Parameters

None

Example

```
amnesiac > show stp-controller status
SteelHead Controller status: enabled
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“stp-controller enable”

---

show subnet side rules

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Subnet-side rule commands”

---

show tcp cong-ctrl

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcp cong-ctrl mode”

---

show tcp highspeed

Displays HS-TCP settings.

Syntax

show tcp highspeed

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“High-speed TCP and satellite optimization commands”

---

show tcp max-time-out

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcp connection send keep-alive”

---

show tcp rate-pacing status

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcp rate-pacing enable”

---

show tcp reordering

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcp connection send reset”

show tcp sack

Displays the TCP selective acknowledgment setting.

Syntax

show tcp sack

Parameters

None

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcp connection send reset”

show tcp sat-opt scps legacy-comp

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

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

show tcp sat-opt scps rules

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“High-speed TCP and satellite optimization commands”

show tcp sat-opt settings

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“High-speed TCP and satellite optimization commands”

show tcpdump stop-trigger

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

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

---

show tcpdump-x

Displays the currently running TCP dumps.

Syntax

show tcpdump-x

Parameters

None

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"RiOS TCP dump commands"

---

show terminal

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“CLI terminal configuration commands”

show topology

Displays the network topology configuration.

Syntax

show topology {areas | networks}

Parameters

areas	Displays all the areas in the network topology.
networks	Displays all the configured networks.

Example

```
amnesiac > show topology areas

Site           Area Num  Peers    Subnets
-----------  ----------  -------  ---------
DefaultSite           1           0.0.0.0/0


amnesiac > show topology networks

Name      Security    Public
--------  ----------  --------
My WAN    None        No
MPLS      Secure      No
Internet  None        No
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“topology site area”

show topology site

Displays the network topology for a site

Syntax

show topology site {<name> | Local | DefaultSite} {areas | uplinks}

Parameters

<name> | Local | DefaultSite	Specify one of the following site names: ▪ **<name> -** Site name, for example, data center. ▪ **Local -** Specifies the local site name, which is where the SteelHead is located. ▪ DefaultSite - Specifies that the default site is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed.
areas	Displays all the site areas.
uplinks	Displays all the configured uplinks for a site.

Example

```
amnesiac > show topology site Local

Name     Network    Gateway  Interface   BW Up (kbps) BW Down (kbps) GRE  Probe DSCP   Probe Timeout  Probe Threshold
-----    --------   -------  ----------- ------------ -------------- ---- -----------  -------------  -----------
inpath0_0* My WAN     -      inpath0_0   1000000      1000000        No   0            2              3
inpath0_1* My WAN     -      inpath0_1   1000000      1000000        No   0            2              3
inpath1_0* My WAN     -      inpath1_0   1000000      1000000        No   0            2              3
primary*   My WAN     -      primary     1000000      1000000        No   0            2              3
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“topology site,” “topology site area,” “topology site uplink”

show topology sites

Displays the network topology for all the configured sites.

Syntax

show topology sites

Parameters

None

Example

```
amnesiac > show topology sites

Name         Type    Outbound QoS    Inbound QoS
-----------  ------  --------------  -------------
Local        Local   Default         Default
DefaultSite  Remote  Default         Default
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“topology site”

show topology uplink

Displays the details of the specified uplink.

Syntax

show topology uplink <uplink-name> {path-selection stats | site <name> path-selection {state | stats}}

Parameters

<uplink-name>	Uplink name.
path-selection stats	Displays path-selection statistics about the uplink.
site <name>	Specifies the site name.
path-selection state	Displays path-selection uplink-to-site state information.
path-selection stats	Displays path-selection site uplink statistics.

Example

```
amnesiac > show topology uplink MPLS_uplink site Default-site path-selection state
Uplink:                 MPLS_uplink
Network:                MPLS
Site:                   Default-Site
VLAN:                   None
Source Mac:             00:50:56:b8:1f:eb
Next Hop Mac:           00:01:e8:8b:d1:7a

Peer IP:                10.33.249.65(*)
Status:                 Reachable
Probe Sequence:         61960
Enacap port:            0
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"topology site uplink," "topology site uplink interface"

show topology uplinks

Displays information about all the configured uplinks.

Syntax

show topology uplinks [path-selection stats]

Parameters

path-selection stats	Displays path-selection statistics about all the configured uplinks.

Example

```
amnesiac > show topology uplinks path-selection stats

Uplink           Bytes  Probe Requests   Probe Response Relay Mismatch  Probe Requests Ricochet Dropped
----------    --------   --------------  ------------------------------  --------------------------------
VPN_uplink           0               0                               0                                 0
MPLS_uplink  364042549          637013                               0                                 0
PTP_uplink           0               0                               0                                 0
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"topology site uplink," "topology site uplink interface"

show uploads

Displays system dump files uploaded to Riverbed Technical Support.

Syntax

show uploads

Parameters

None

Usage

This 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/server-xxxx_aux_new.cap0
url: ftp://ftp.riverbed.com/incoming/case_194170_example
status: finished
percent complete: 100%
start time: 2013/03/25 12:16:40 -0700
finish time: 2013/03/25 12:16:41 –0700
```

Product

SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“file upload clear-stats”

show version

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:   9.6.0-mainline
Build ID:          #101
Build date:        2017-01-15 16:36:45
Build arch:        x86_64
Built by:          root@moscow.nbttech.com
Uptime:            15d 19h 40m 38s
Product model:     CX1555H
```

```
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 (config) # show version all
Product name:      rbt_sh
Product release:   9.6.0-mainline
Build ID:          #101
Build date:        2017-01-23 02:43:02
Build arch:        x86_64
Built by:          mockbuild@bannow-worker1

Uptime:            71d 2h 27m 5s

Product model:     CX1555 (CX1555H)
System memory:     7828 MB used / 103 MB free / 7932 MB total
Number of CPUs:    4
CPU load averages: 1.56 / 1.54 / 1.31
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“image fetch,” “image install”

---

show wccp

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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"WCCP support commands"

show wccp interface service-group

Displays WCCP settings for the specified interface and service group.

Syntax

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

Parameters

<interface>	Interface name (for example, **inpath0_0**).
<service-id>	WCCP group number.
detail	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:

- The redirection, return, and assignment methods that have been negotiated between the SteelHead and the WCCP routers.
- Whether or not the **wccp override-return route-no-gre command** is in use (displayed as WCCP Return via Gateway Override).
- Whether or not the SteelHead is receiving WCCP control messages from the router (*I-see-you* messages).
- Load distribution details 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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"WCCP support commands"

---

show web

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

SCC, SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"Web configuration commands"

---

show web ssl cert

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"web ssl cert generate"

---

show web prefs

Displays the current web preferences.

Syntax

show web prefs

Parameters

None

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"Web configuration commands"

---

show web-proxy audit-log settings

Displays information about the web proxy audit log settings.

Syntax

show web-proxy audit-log settings

Parameters

None

Usage

The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac > show web-proxy audit-log settings
Audit log settings:
Enabled:         yes
Remote Address:  192.168.1.233
Remote Port:     522
```

Product

SteelHead CX

Related Commands

"web-proxy audit-log enable"

show web-proxy cache

Displays web proxy cache settings.

Syntax

show web-proxy cache [all | ssl | maxfilesize]

Parameters

all	Displays all web proxy cache settings.
ssl	Displays whether or not SSL caching is enabled or disabled.
maxfilesize	Displays the global maximum size file that can be cached.

Usage

The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac > show web-proxy cache ssl
SSL enabled: yes
```

Product

SteelHead CX

Related Commands

"web-proxy cache enable"

show web-proxy cache size

Displays web proxy cache size.

Syntax

show web-proxy cache size

Parameters

None

Usage

The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac > show web-proxy cache size
Web-proxy min license allowed cache size (GB): 5.00
Web-proxy max license allowed cache size (GB): 200.00
Web-proxy configured cache size (GB): 12.00
Web-proxy actual cache size (GB): 200.00
```

Product

SteelHead-v

Related Commands

"web-proxy cache size"

---

show web-proxy parent status

Displays web proxy parent configuration settings.

Syntax

show web-proxy parent status

Parameters

None

Usage

The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac > show web-proxy parent status
Manual: Enabled
        HTTP: zscaler:80, cws:80
        HTTPS: zscaler:443, cws:443
        Excludes: testdomain.com
        Selection Mode: Failover
Automatic: Disabled
```

Product

SteelHead CX

Related Commands

"web-proxy parent manual enable," "web-proxy parent manual excludes domain," "web-proxy parent manual http," "web-proxy parent manual https"

---

show web-proxy ssl

Displays whether or not SSL decryption is enabled.

Syntax

show web-proxy ssl

Parameters

None

Usage

The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac > show web-proxy ssl
ssl enabled: yes
```

Product

SteelHead CX

Related Commands

"web-proxy ssl enable"

show web-proxy ssl-domain

Displays the specified SSL domain.

Syntax

show web-proxy ssl-domain

Parameters

<domain>	Domain name.

Usage

The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac > show web-proxy ssl-domain googlevideo.com
```

Product

SteelHead CX

Related Commands

"web-proxy ssl-domain"

show web-proxy ssl-domains

Displays all configured SSL domains.

Syntax

show web-proxy ssl-domains

Parameters

None

Usage

The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac > show web-proxy ssl-domains
*.googlevideo.com
*.youtube.com
www.mycompany.com
*.riverbed.com
```

Product

SteelHead CX

Related Commands

"web-proxy ssl-domain"

show web-proxy stats cache

Displays information about the current web proxy cache statistics.

Syntax

show web-proxy stats cache

Parameters

None

Usage

This command displays the number of entries in the cache. These statistics are specific to the SteelHead and are not reported on the SCC.

Example

```
amnesiac > show web-proxy stats cache
Webcache statistics:
Percentage Full:  99 (as a percentage)
Hit Rate:  12 (as a percentage)
Hits:      35102
Lookups:   280539
Misses:    245437
```

Product

SteelHead CX

Related Commands

“Web proxy commands”

show web-proxy status

Displays whether or not the web proxy service is enabled.

Syntax

show web-proxy status

Parameters

None

Usage

The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac > show web-proxy status
service status: stopped
```

Product

SteelHead CX

Related Commands

“web-proxy enable”

show web-proxy stats domain

Displays the traffic statistics of the specified domain.

Syntax

show web-proxy stats domain <domain-name> [start-time <start-time> end-time <end-time>]

(or)

show web-proxy stats domain <domain-name> [duration <time-interval>]

Parameters

<domain-name>	Domain name. The domain names can be hostnames (for example, hostname.com).
start-time <start-time>	Specifies the start time to return statistics for a specified time period. Use UNIX Epoch time (the number of seconds that have elapsed since 00:00:00 UTC on 1st May, 1970). For example, 12:00:00 AM PST on 4/15/2018 is represented as 1523775600. To derive the UNIX time, you can use the **date -j -f "%b %d %Y %T" "Mon DD YYYY HH:MM:SS" "+%s"** command. For example, date -j -f "%b %d %Y %T" "Jan 01 2000 12:10:00" "+%s" returns 946708800.
end-time <end-time>	Specifies the end time to return statistics for a specified time period. Use UNIX Epoch time (the number of seconds that have elapsed since 00:00:00 UTC on 1st May, 1970). For example, 12:00:00 AM PST on 5/15/2018 is represented as 1526367600. To derive the UNIX time, you can use the **date -j -f "%b %d %Y %T" "Mon DD YYYY HH:MM:SS" "+%s"** command. For example, date -j -f "%b %d %Y %T" "Jan 01 2000 12:10:00" "+%s" returns 946708800.
duration <time-interval>	Returns statistics for one of the following time intervals: ▪ **last-15-min** - Returns traffic statistics for the last 15 minutes. ▪ **last-hour** - Returns traffic statistics for the last hour. ▪ **last-day** - Returns traffic statistics for the last 24 hours. ▪ **last-week** - Returns traffic statistics for the last week. ▪ **last-year -** Returns traffic statistics for the last year.

Usage

Web proxy must be enabled on the appliance before you run this command.

This command displays the total number of requests, hits, misses, hit-rate, bytes served from cache, and total bytes served by the domain in the specified time interval.

See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amneasic (config) # show web-proxy stats domain riverbed.com duration last-year
Domain                          Hits     Misses    Requests    Hit Rate    Cache Bytes    Total Bytes
-------------------------------------------------------------------------------------------------
riverbed.com                       0        164         164      0.0000              0          54568
```

Product

SteelHead CX

Related Commands

"web-proxy enable," "show web-proxy stats order-by," "show web-proxy stats service"

show web-proxy stats order-by

Displays web proxy domain statistics ordered by the statistics type.

Syntax

show web-proxy stats order-by <stats-type> [start-time <start-time> end-time <end-time>] [count <count>]

(or)

show web-proxy stats order-by <stats-type> [duration <time-interval >] [count <count>]

Parameters

<stats-type>	Specify one of these statistics type to determine the order of domains in the statistics table: ▪ **hits** - Returns the list of domains ordered by the number of hits. ▪ **misses** - Returns the list of domains ordered by the number of misses. ▪ **requests** - Returns the list of domains ordered by the number of requests. ▪ **cache-bytes** - Returns the lists of domains ordered by the number of bytes served from the cache. ▪ **total-bytes** - Returns the list of domains ordered by the total number of bytes consumed by the domain. ▪ **hit-rate -** Returns the list of domains ordered by the hit-rate of the cache.
count <count>	Sets the number of top domains for which statistics are returned. If you did not specify the count, the command returns the statistics of all the domains.
start-time <start-time>	Specifies the start time to return statistics for a specified time period. Use UNIX Epoch time (the number of seconds that have elapsed since 00:00:00 UTC on 1st May, 1970). For example, 12:00:00 AM PST on 4/15/2018 is represented as 1523775600. To derive the UNIX time, you can use the **date -j -f "%b %d %Y %T" "Mon DD YYYY HH:MM:SS" "+%s"** command. For example, date -j -f "%b %d %Y %T" "Jan 01 2000 12:10:00" "+%s" returns 946708800.
end-time <end-time>	Specifies the end time to return statistics for a specified time period. Use UNIX Epoch time (the number of seconds that have elapsed since 00:00:00 UTC on 1st May, 1970). For example, 12:00:00 AM PST on 5/15/2018 is represented as 1526367600. To derive the UNIX time, you can use the **date -j -f "%b %d %Y %T" "Mon DD YYYY HH:MM:SS" "+%s"** command. For example, date -j -f "%b %d %Y %T" "Jan 01 2000 12:10:00" "+%s" returns 946708800.
duration <time-interval>	Returns statistics for one of the following time intervals: ▪ **last-15-min** - Returns traffic statistics for the last 15 minutes. ▪ **last-hour** - Returns traffic statistics for the last hour. ▪ **last-day** - Returns traffic statistics for the last 24 hours. ▪ **last-week** - Returns traffic statistics for the last week. ▪ **last-year -** Returns traffic statistics for the last year.

Usage

Web proxy must be enabled on the appliance before you run this command.

This command displays the statistics of the top domains, ordered by the statistics type you select in the specified time interval.

See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac (config) # show web-proxy stats order-by cache-bytes duration last-year count 5
Domain                        Hits     Misses    Requests    Hit Rate    Cache Bytes    Total Bytes
-------------------------------------------------------------------------------------------------
googlevideo.com                145       3574        3719      0.0390      169031120     2594400021
nbttech.com                    690      35061       35751      0.0193       52926851      112214558
youtube.com                    169        837        1006      0.1680        9392759       23683194
apple.com                      112        137         249      0.4498         900249      527822499
amazon.com                      30        199         229      0.1310         419197         207899
```

Product

SteelHead CX

Related Commands

“web-proxy enable,” “show web-proxy stats service,” “show web-proxy stats domain”

---

show web-proxy stats service

Displays the traffic statistics of the specified service.

Syntax

show web-proxy stats service <service-name> [start-time <start-time> end-time <end-time>]

(or)

show web-proxy stats service <service-name> [duration <time-interval>]

Parameters

<service-name>	Specifies the service name and returns traffic statistics of the service for all domains. RiOS 9.8.0 only returns traffic statistics of YouTube.
start-time <start-time>	Specifies the start time to return statistics for a specified time period. Use UNIX Epoch time (the number of seconds that have elapsed since 00:00:00 UTC on 1st May, 1970). For example, 12:00:00 AM PST on 4/15/2018 is represented as 1523775600. To derive the UNIX time, you can use the **date -j -f "%b %d %Y %T" "Mon DD YYYY HH:MM:SS" "+%s"** command. For example, date -j -f "%b %d %Y %T" "Jan 01 2000 12:10:00" "+%s" returns 946708800.
end-time <end-time>	Specifies the end time to return statistics for a specified time period. Use UNIX Epoch time (the number of seconds that have elapsed since 00:00:00 UTC on 1st May, 1970). For example, 12:00:00 AM PST on 5/15/2018 is represented as 1526367600. To derive the UNIX time, you can use the **date -j -f "%b %d %Y %T" "Mon DD YYYY HH:MM:SS" "+%s"** command. For example, date -j -f "%b %d %Y %T" "Jan 01 2000 12:10:00" "+%s" returns 946708800.
duration <time-interval>	Returns statistics for one of the following time intervals: ▪ **last-15-min** - Returns traffic statistics for the last 15 minutes. ▪ **last-hour** - Returns traffic statistics for the last hour. ▪ **last-day** - Returns traffic statistics for the last 24 hours. ▪ **last-week** - Returns traffic statistics for the last week. ▪ **last-year -** Returns traffic statistics for the last year.

Usage

Web proxy must be enabled on the appliance before you run this command. When web proxy is enabled, YouTube caching is enabled by default. Also ensure that YouTube domains (such as youtube.com and googlevideo.com) are configured in the web proxy SSL domain before you run this command.

This command displays the total number of requests, hits, misses, hit-rate, bytes served from cache, and total number of bytes served by YouTube in the specified time interval. This command also returns the requests, hits, bytes served from cache, and total number of bytes YouTube served by the type of the content (such as audio, video, and other).

See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac (config) # show web-proxy stats service youtube duration last-year
Service             Hits      Misses    Requests    Hit Rate    Cache Bytes    Total Bytes
-------------------------------------------------------------------------------------------
youtube              314        4411        4725      0.0665      178423879     2618083215
```

Product

SteelHead CX

Related Commands

"web-proxy enable," "web-proxy youtube enable," "show web-proxy stats order-by," "show web-proxy stats domain," "web-proxy ssl-domain"

show web-proxy youtube

Displays information about the cache key and whether or not YouTube caching is enabled for web proxy operations.

Syntax

show web-proxy youtube

Parameters

None

Usage

YouTube caching is enabled by default and requires no manual configuration. You can disable YouTube caching using the **no web-proxy youtube** command. The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac > show web-proxy youtube
YouTube configuration:
Enabled: yes
Cache Key: DEFAULT
```

Product

SteelHead CX

Related Commands

“web-proxy youtube enable”

---

show workgroup account

Displays the current workgroup account settings.

Syntax

show workgroup account

Parameters

None

Example

```
amnesiac > show workgroup account
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Job commands”

---

show workgroup configuration

Displays the current workgroup configuration settings.

Syntax

show workgroup configuration

Parameters

None

Example

```
amnesiac > show workgroup configuration
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Job commands”

---

show workgroup status

Displays the current workgroup status settings.

Syntax

show workgroup status

Parameters

None

Example

```
amnesiac > show workgroup status
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Job commands”

---

show saml

Displays the status of IdP configuration in SteelHeads and SCCs.

Syntax

show saml

Parameters

None

Usage

Before you enable SAML on an appliance, it is useful to know whether IdP has been validated or not. This command displays both the IdP validation status and SAML status.

For more details on how to configure IdP, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # show saml
SAML Enabled:       Yes
IDP Status:        Validated
```

Product

SCC, SteelHead CX, SteelHead EX, SteelHead-c, SteelHead-v

Related Commands

“aaa saml enable”

3

Enable Mode Commands

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

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

Chapter 4, "Configuration Mode Commands" describes additional enable mode 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 reminds you that you can also access these commands while in enable mode.

To enter enable mode

- Connect to the CLI and enter the following command:

```
login as: admin
Riverbed SteelHead
Last login: Wed Jan 20 13:02:09 2016 from 10.0.1.1
amnesiac > enable
amnesiac #
```

To exit enable mode, enter **exit**. For information about the **exit** command, see "exit" on page 14.

System administration commands

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

clear arp-cache

Clears dynamic entries from the ARP cache.

Syntax

clear arp-cache

Parameters

None

Usage

This command does not clear static entries.

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“show arp”

---

clear hardware edac-ue-alarm

Clears the Error Detection and Correction (EDAC) Uncorrectable Errors (UEs) alarm.

Syntax

clear hardware edac-ue-alarm

Parameters

None

Example

```
amnesiac # clear hardware edac-ue-alarm
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“clear hardware error-log”

---

clear hardware error-log

Clears Intelligent Platform Management Interface (IPMI) System Event Log (SEL).

Syntax

clear hardware error-log

Parameters

None

Usage

The amber LED light stops blinking on the system when you enter this command.

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“show hardware error-log”

---

clear in-path rule

Clears in-path rule statistics.

Syntax

clear in-path rule [<rule-number> | default | all]

Parameters

<rule-number>	Clears the statistics for the in-path rule number you specify. Valid values are from 1 to 65534.
default	Clears the statistics for the system-generated default in-path rule.
all	Clears the statistics for all in-path rules.

Usage

This command clears the in-path rule statistics for the rules displayed by the **show in-path rules** command.

You can choose to clear the statistics for a specific in-path rule, the system-generated default in-path rule, or all in-path rules.

To specify more than one in-path rule, enter the in-path rule numbers separated by commas (no spaces): for example, 5,7,9.

If you don't specify a rule number, by default the statistics for all in-path rules are cleared.

Example

```
amnesiac (config) # clear in-path rule 2,3
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path rules"

clear interface

Sets the interface counters for the specified interface to 0.

Syntax

clear interface <interface-name>

Parameters

<interface-name>	Interface name: **aux**, **primary**, **lo**, **wan1_1**, **lan1_1**, **wan1_0**, **lan1_0**, **inpath1_0**, **inpath1_1**, or **all.**

Example

```
amnesiac # clear interface aux
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show in-path mgmt-interface"

clock set

Sets the system date and time.

Syntax

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

Parameters

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

Example

```
amnesiac # clock set 2014/12/31 23:59:59
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show clock"

configure terminal

Enters configuration from the terminal by entering the configuration subsystem.

Syntax

[no] configure terminal

Parameters

None

Usage

You must execute the "enable" command first to enter configuration mode.

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

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

Example

```
amnesiac # configure terminal
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show terminal," "show connection"

debug generate dump

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	Generates a full system dump.
brief	Generates a brief system dump.
rsp	Generates a full system dump, including VMware Server data.
stats	Generates a full system dump including .dat files.
all-logs	Generates a full system dump with .dat files and all logs.
blockstore	Generates a full system dump with .dat files, all logs, and blockstore phash.
blockstore-fifo	Generates a full system dump with .dat files, all logs, blockstore phash, and fifo.
upload <case-number>	Generates a full system dump for the specified customer case number to upload to Riverbed Technical Support. The case number is a numeric string.
upload <url>	Generates a full system dump for the specified customer URL to upload to Riverbed Technical Support.

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 forward slash "/" : for example, ftp://ftp.riverbed.com/incoming/and not ftp://ftp.riverbed.com/incoming. The filename as it exists on the system is renamed to the filename specified in the URL.

After the dump generation, the upload is performed in the background so you can exit the command-line interface without interrupting the upload process.

Example

```
amnesiac # debug generate dump brief
amnesiac # debug generate dump upload 194170
amnesiac # debug generate dump upload ftp://ftp.riverbed.com/incoming/
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“RiOS TCP dump commands”

disable

Exits enable mode.

Syntax

disable

Parameters

None

Example

```
amnesiac # disable
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"exit"

file debug-dump delete

Deletes the specified debug dump file.

Syntax

file debug-dump delete <filename>

Parameters

<filename>	Filename of the debug dump file.

Example

```
amnesiac # file debug-dump delete mydumpfile.txt
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"RiOS TCP dump commands"

file debug-dump email

Sends a debug dump file in an email to preconfigured recipients.

Syntax

file debug-dump email <filename>

Parameters

<filename>	Filename of the debug dump file.

Example

```
amnesiac # file debug-dump email mydumpfile.txt
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"RiOS TCP dump commands"

file debug-dump upload

Uploads the specified debug dump file.

Syntax

file debug-dump upload <filename> [<url> | <case-number>]

Parameters

<filename>	Filename of the debug dump file to upload.
<url>	Protocol used (either https, http, ftp, or scp), the location, and authentication credentials to upload the file. For example, **scp://username:password@hostname/path/filename**
<case-number>	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 # file debug-dump upload mydebug.txt scp://me:test@example.com/mypath
amnesiac # file debug-dump upload mydebug.txt 194170
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“RiOS TCP dump commands”

file process-dump delete

Deletes the specified crash dump file.

Syntax

file process-dump delete <filename>

Parameters

<filename>	Filename of the crash dump file.

Example

```
amnesiac # file process-dump delete mycrash.txt
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“RiOS TCP dump commands”

file process-dump upload

Uploads the specified crash dump file.

Syntax

file process-dump upload <filename> [**<url>** | **<case-number>**]

Parameters

<filename>	Filename of the crash dump file.
<url>	Protocol used (either https, http, ftp, or scp), the location, and authentication credentials to upload the file. For example, **scp://username:password@hostname/path/filename**
<case-number>	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 # file process-dump upload mycrash.txt scp://mylogin:mypassword@myhostname/path/filename
amnesiac # file process-dump upload mycrash.txt 194170
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"RiOS TCP dump commands"

file sa delete

Deletes a system activity report (SAR) log file.

Syntax

file sa delete <filename>

Parameters

<filename>	Filename for the SAR file.

Example

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

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show files sa," "show files stats"

file sa generate

Generates a system activity report (SAR) log file.

Syntax

file sa generate

Parameters

None

Example

```
amnesiac # file sa generate
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show files sa,” “show files stats”

file sa upload

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

Syntax

file sa upload <filename> [<url> | <case-number>]

Parameters

<filename>	Name of the file to upload.
<url>	Protocol used (either https, http, ftp, or scp), the location, and authentication credentials to upload the file. For example, **scp://username:password@hostname/path/filename**
<case-number>	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 sa upload 2007.12.18.23.54.sar http://www.riverbed.com/support
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show files sa,” “show files stats”

file stats delete

Deletes the statistics file.

Syntax

file stats delete <filename>

Parameters

<filename>	Name of the file to delete.

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“show files stats”

file stats move

Renames the statistics file.

Syntax

file stats move <source-filename> <destination-filename>

Parameters

<source-filename>	Source file to rename.
<destination-filename>	New filename.

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show files stats"

file stats upload

Uploads the statistics report file to a remote host.

Syntax

file stats upload <filename> [<url>| <case-number>]

Parameters

<filename>	Source filename to upload.
<url>	Protocol used (either https, http, ftp, or scp), the location, and authentication credentials to upload the file. For example, **scp://username:password@hostname/path/filename**
<case-number>	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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show files stats"

file tcpdump delete

Deletes a tcpdump output file.

Syntax

file tcpdump delete <filename>

Parameters

<filename>	tcpdump file to delete.

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"debug generate dump," "file tcpdump upload"

file tcpdump upload

Uploads a tcpdump output file.

Syntax

file tcpdump upload <filename> [**<url>** | **<case-number>**]

Parameters

<filename>	Name of the tcpdump output file to upload
<url>	Protocol used (either https, http, ftp, or scp), the location, and authentication credentials to upload the file. For example, **scp://username:password@hostname/path/filename**
<case-number>	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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"debug generate dump," "file tcpdump delete"

file upload clear-stats

Clears the file upload statistics.

Syntax

file upload clear-stats

Parameters

None

Usage

This command clears the statistics displayed by the **show uploads** command.

Example

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

Product

SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show uploads"

file upload stop

Stops an upload.

Syntax

file upload stop <upload-number>

Parameters

<upload-number>	File upload number.

Usage

The **file upload stop** command stops an upload of a resource.

Example

```
amnesiac > file upload stop 5
```

Product

SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show uploads"

image delete

Deletes the specified software image.

Syntax

image delete <image-filename>

Parameters

<image-filename>	Name of the software image to delete.

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

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

image delete-all

Deletes all software image files on the disk.

Syntax

image delete-all

Parameters

None

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, Mobile Controller

Related Commands

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

image fetch

Downloads a software image from a remote host.

Syntax

image fetch <url> <image-filename>

Parameters

<url>	Protocol used (either https, http, ftp, or scp), the location, and authentication credentials to download the file. For example, **scp://username:password@hostname/path/filename** Press the Enter key to download the image. The image retains the same name it had on the server.
<image-filename>	Local filename for the image.

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

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

image install

Installs the software image onto a system partition.

Syntax

image install <image-filename> <partition>

Parameters

<image-filename>	Software image filename to install.
<partition>	Partition number: **1**, **2**.

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

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

image move

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

Syntax

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

Parameters

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

Example

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

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

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

image upgrade

Installs a system image on the backup boot partition.

Syntax

image upgrade <image-name>

Parameters

<image-name>	Software image filename to install.

Usage

This command only installs the image on the backup boot partition.

Example

```
amnesiac # image upgrade image187.img
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

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

ntpdate

Conducts a one-time synchronization with a specified NTP server.

Syntax

ntpdate <ip-address>

Parameters

<ip-address>	NTP server IP address with which to synchronize.

Example

```
amnesiac # ntpdate 10.10.10.1
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show ntp"

reload

Reboots the system.

Syntax

reload [clean [halt] | halt | force]

Parameters

clean	Reboots or shuts down the system, then clears the RiOS datastore.
clean halt	Shuts down the system, then clears the RiOS datastore.
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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show configuration running," "show hardware error-log," "show info," "show log"

restart

Restarts the optimization service.

Syntax

restart [clean]

Parameters

clean	Restarts the optimization service and clears the datastore.

Example

```
amnesiac # restart
Terminating the process....
Relaunching the process
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"service enable," "show configuration running"

service enable

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, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show configuration running"

service error reset

Resets the SteelHead service after a service error.

Syntax

service error reset

Parameters

None

Example

```
amnesiac # service error reset
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show connection," "show service"

service restart

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, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show service"

stats clear-all

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show alarm," "show alarms"

stats convert

Converts statistical data from one storage format to another.

Syntax

stats convert <format>

Parameters

<format>	Storage format: ▪ **1** - Storage 1 version ▪ **2** - Storage 2 version

Example

```
amnesiac # stats convert 2
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show alarm,” “show alarms”

tcpdump

Executes the tcpdump utility. You can quickly diagnose problems and take traces for Riverbed Support.

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 hexadecimal 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

The **tcpdump** command takes the standard Linux options. For detailed information, see the Linux man page. 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 - 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 SteelHeads 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 SteelHeads 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 capturing 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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“RiOS TCP dump commands”

---

tproxytrace

Describes the proxy path in real time.

Syntax

tproxytrace [options] <target-ip>:<target-port>

Parameters

<options>	**tproxytrace** options: ▪ **-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.
<target-ip>:<target-port>	Specify the target IP address and port.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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

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

Controller, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, Mobile Controller

Related Commands

"AAA, role-based management, Radius, and TACACS+ commands"

show arp

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"clear arp-cache"

show autolicense status

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"license autolicense enable"

show banner

Displays the banner settings.

Syntax

show banner

Parameters

None

Example

```
amnesiac # show banner
Banners:
    MOTD:
    Issue: Riverbed Interceptor
    Net Issue: Riverbed Interceptor
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“CLI terminal configuration commands”

show cmc

Displays Controller 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 (10.0.2.2)
Auto configuration status:           Inactive
Last message sent to cmc:            Auto-registration
Time that message was sent:          Thu Nov 13 12:02:25 2014
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-c, SteelHead-v

Related Commands

“SteelCentral Controller for SteelHead commands”

show configuration

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“Configuration file commands”

show configuration files

Displays the list of active and backup configuration files or the contents of a specified file.

Syntax

show configuration [**<filename>**]

Parameters

<filename>	Configuration file. The default filenames 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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“Configuration file commands”

show configuration flash

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“Configuration file commands”

show configuration running

Displays running configuration settings that are different from the defaults.

Syntax

show configuration running [full]

Parameters

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“Configuration file commands”

show files debug-dump

Displays a list of debug dump files.

Syntax

show files debug-dump [<filename>]

Parameters

<filename>	Filename.

Example

```
amnesiac # show files debug-dump
sysinfo-sysdump-amnesiac-20050725-183016.txt
sysdump-amnesiac-20050606-140826.tgz
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"file debug-dump delete," "file debug-dump email," "file debug-dump upload"

show debug health-report

Displays the health report settings.

Syntax

show debug health-report

Parameters

None

Example

```
amnesiac# show debug health-report
Enable Health Report: yes
```

Product

SCC, SteelHead CX, SteelHead EX, SteelHead-v

Related Commands

"debug health-report enable"

show debug uptime-report

Displays the uptime-report settings.

Syntax

show debug uptime-report

Parameters

None

Example

```
amnesiac # show debug uptime-report
Enable Uptime Report: yes
```

Product

SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"debug uptime-report enable"

show files process-dump

Displays a list of crash dump files.

Syntax

show files process-dump

Parameters

None

Example

```
amnesiac # show files process-dump
```

Product

Controller, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"file process-dump delete," "file process-dump upload"

show files sa

Displays SteelHead log files.

Syntax

show files sa [<filename>]

Parameters

<filename>	Filename to display.

Example

```
amnesiac # show files sa
2014.05.16.23.53.sar
2014.05.17.23.53.sar
2014.05.18.23.53.sar
2014.05.19.23.53.sar
2014.05.20.23.53.sar
2014.05.21.23.53.sar
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"file sa generate"

show files stats

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"show stats bandwidth," "stats export"

---

show files tcpdump

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"tcpdump"

---

show hardware all

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“hardware spec activate”

---

show hardware licensing info

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“hardware spec activate”

---

show in-path mgmt-interface

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Management in-path interface commands”

show ip default-gateway

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“ip in-path-gateway”

show ipv6 default-gateway

Displays the IPv6 default gateway.

Syntax

show ipv6 default gateway [static]

Parameters

static	Displays the static IPv6 default gateway.

Example

```
amnesiac # show ipv6 default-gateway static
Configured default gateway: 2001:38dc:52::e9a4:c5:6282/64
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“ipv6 default-gateway”

show ipv6 in-path-gateway

Displays the in-path IPv6 default gateway.

Syntax

show ipv6 in-path-gateway <interface> [static]

Parameters

<interface>	Interface to display.
static	Displays configured in-path IPv6 routes.

Example

```
amnesiac # show ipv6 in-path-gateway inpath0_0
Destination Network                         Gateway
default                                     2001:38dc:52::e9a4:c5:6282
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"ipv6 in-path-gateway"

show ipv6 in-path route

Displays active in-path IPv6 route settings, both dynamic and static.

Syntax

show ipv6 in-path route <interface> [static]

Parameters

<interface>	Name of the interface to display.
static	Displays configured in-path IPv6 routes.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"ipv6 in-path route"

show ipv6 route

Displays active IPv6 routes, both dynamic and static.

Syntax

show ipv6 route [static]

Parameters

static	Displays the configured static IPv6 routes.

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“ipv6 route”

show ip route

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“ip route”

show job

Displays the status of a scheduled job.

Syntax

show job <job-id>

Parameters

<job-id>	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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“Job commands”

---

show jobs

Displays a list of all jobs.

Syntax

show jobs

Parameters

None

Example

```
amnesiac # show jobs
% No jobs configured.
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“Job commands”

---

show license-client

Displays details of the licenses retrieved by the appliance.

Syntax

show license-client

Parameters

None

Example

```
amnesiac # 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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"license client init," "license client init"

---

show license-servers

Displays the name, port number, and priority of the server that the appliance uses for licensing.

Syntax

show license-servers

Parameters

None

Example

```
amnesiac # show license-servers
Server Name                          Port               Priority
---------------                      ---------------    ---------------
aws-cloud-df.riverbed.com            80                 5
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"System administration and service commands"

---

show licenses

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“License and hardware upgrade commands”

show log

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“Logging commands”

show papi rest access_codes

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“papi rest access_code generate,” “papi rest access_code import,” “web rest-server enable”

---

show port-label

Displays a list of port labels configurations or a list of ports that belong to the specified port label.

Syntax

show port-label [**<port-label>**]

Parameters

<port-label>	A list of ports that belong to the specified port-label name: ▪ **Secure -** Displays the list of ports that belong to the system label for secure ports. The SteelHead automatically passes through traffic on commonly secure ports (for example, ssh, https, and smtps). For a list of secure ports, see Appendix , “SteelHead 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 374. ▪ **SteelFusion -** Displays the list of ports that belong to the system label for Riverbed SteelFusion ports 7950-7954, and 7960. ▪ **Interactive -** Displays ports that belong to the system label for interactive ports. The SteelHead 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 (SteelHead Interceptor), 7870 (SteelCentral Controller for SteelHead Mobile).

Example

```
amnesiac # show port-label
Port Label:        Interactive
PortLabel:         RBT-Proto
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, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“Port label commands”

show protocol domain-auth auto-conf delegation

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol domain-auth auto-conf delegation adminuser,” “protocol domain-auth auto-conf delegation domain”

show protocol domain-auth auto-conf easy-auth

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol domain-auth auto-conf easy-auth”

show protocol domain-auth auto-conf replication

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol domain-auth auto-conf replication”

show protocol domain-auth configure load-balancing

Displays the results of the last run of the configure load-balancing action.

Syntax

show protocol domain-auth configure load-balancing [verbose]

Parameters

verbose	Displays load-balancing configuration settings with verbose logs.

Example

```
amnesiac # show protocol domain-auth configure load-balancing

Action                          Status           Last Run
-------------------------------------------------------------------------------
Configure Load-Balancing        SUCCESS          Tue Jan 21 12:16:27 2014
PST
-------------------------------------------------------------------------------

RESULT:
Configure load-balancing result:

You must restart the optimization service for your changes to take effect.
Enable load balancing support successfully completed
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol domain-auth configure load-balancing"

show protocol domain-auth load-balancing configuration

Displays whether or not load balancing is enabled.

Syntax

show protocol domain-auth load-balancing configuration

Parameters

None

Example

```
amnesiac # show protocol domain-auth load-balancing configuration
Load Balancing: Enabled
Number of DCs to load balance across: 6
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol domain-auth configure load-balancing"

show protocol domain-auth test authentication

Displays authentication test results.

Syntax

show protocol domain-auth test authentication [verbose]

Parameters

verbose	Displays the authentication test result with verbose logs.

Example

```
amnesiac # show protocol domain-auth test authentication
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol domain-auth test authentication"

show protocol domain-auth test delegation server-privs

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 CX, SteelHead EX, SteelHead-c

Related Commands

“protocol domain-auth test delegation server-privs”

show protocol domain-auth test delegation setup

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 CX, SteelHead EX, SteelHead-c

Related Commands

“protocol domain-auth test delegation setup”

show protocol domain-auth test dns

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                        SUCCESS                Tue Aug 9 00:14: 2012
-------------------------------------------------------------------------------
RESULT: Testing DNS Configuration
Joined Domain: VCS246.GEN-VCS78DOM.COM

DNS Test Passed
```

Product

SteelHead CX, SteelHead EX, SteelHead-c

Related Commands

“protocol domain-auth test dns”

show protocol domain-auth test join

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                       SUCCESS                 Tue Jan 7 12:32:11 2014
-------------------------------------------------------------------------------
RESULT: Test Join result:

Testing if SH is joined to a domain
Join to domain PERF.TEST is OK
Domain Join Test Succeeded
```

Product

SteelHead CX, SteelHead EX, SteelHead-c

Related Commands

“protocol domain-auth test join”

show protocol domain-auth test replication prp

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 CX, SteelHead EX, SteelHead-c

Related Commands

“protocol domain-auth test replication prp”

show protocol domain-auth test replication try-repl

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol domain-auth test replication try-repl”

show protocol notes encrypt

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol notes encrypt server-port,” “protocol notes encrypt import server-id”

show radius

Displays RADIUS configuration settings.

Syntax

show radius

Parameters

None

Example

```
amnesiac (config) # radius-server host 10.1.18.55 auth-type mschapv2 key testing123
amnesiac (config) # radius-server host 2600:809:200:412:7a2b:cbff:feld:c793 auth-type mschapv2 key
testing123
amnesiac (config) # show radius
RADIUS defaults:
    key:
    timeout: 3
    retransmit: 1
RADIUS servers:
   10.1.18.55:1812
      Enabled: yes
      Auth Type: mschapv2
      Key: pjoqykkDkJLkSAkQDrReIo2Ev1Y724Iq
      Timeout: 3
      Retransmit: 1
   2600:809:200:412:7a2b:cbff:feld:c793:1812
      Enabled: yes
      Auth Type: mschapv2
      Key: =xLso97KDrH0b1uAqJVUQx6G5Uxqtrrn
      Timeout: 3
      Retransmit: 1
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“AAA, role-based management, Radius, and TACACS+ commands”

show rbm user

Displays role-based management (RBM) user configuration.

Syntax

show rbm user <username>

Parameters

<username>	Name of the user.

Example

```
amnesiac (config) # show rbm user helpdesk
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SCC

Related Commands

"AAA, role-based management, Radius, and TACACS+ commands"

show rbm users

Displays role-based management (RBM) user configuration for all users.

Syntax

show rbm users

Parameters

None

Example

```
amnesiac (config) # show rbm users
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SCC

Related Commands

"AAA, role-based management, Radius, and TACACS+ commands"

show remote configured

Displays the configuration settings for the remote management port.

Syntax

show remote configured

Parameters

None

Example

```
amnesiac # show remote configured
Channel      :: 2
DHCP enabled :: no
IP           :: 192.168.0.1
Netmask      :: 255.255.255.0
Gateway      :: 0.0.0.0
```

Product

SteelHead CX, SteelHead EX, Mobile Controller

Related Commands

“Remote management port commands”

show remote ip

Displays the current IP network settings for the remote management port.

Syntax

show remote ip

Parameters

None

Example

```
amnesiac # show remote ip
Channel:     1
DHCP:        Disabled
IP Address:  0.0.0.0
Netmask:     0.0.0.0
Gateway:     0.0.0.0
MAC Address: 00:0e:b6:93:aa:65
```

Product

SteelHead CX, SteelHead EX, Mobile Controller

Related Commands

“Remote management port commands”

show running-config

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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“Configuration file commands”

show tacacs

Displays TACACS+ settings.

Syntax

show tacacs

Parameters

None

Example

```
amnesiac # show tacacs
No tacacs settings
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"AAA, role-based management, Radius, and TACACS+ commands"

show telnet-server

Displays Telnet server settings.

Syntax

show telnet-server

Parameters

None

Example

```
amnesiac # show telnet-server
TCP reordering enabled:   no
TCP reordering threshold: 3
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"telnet-server enable"

show userlog

Displays the current user log file in a scrollable page.

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 RiO
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

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"Logging commands"

show usernames

Displays a list of user accounts.

Syntax

show usernames [detailed]

Parameters

detailed	Displays detailed user account information.

Example

```
amnesiac # show usernames
User                          Status      Active    Capability
-------------------------------------------------------------
admin@                        enabled        y         admin
monitor                       enabled        n         monitor
-------------------------------------------------------------
@ = current user

amnesiac # show usernames detailed
User admin details
   Current User:            Yes
   Logged In:               Yes
   Disabled:                No
   Password Change:         Allowed anytime
   Password Expired:        Never
   Account Locked:          Never
   Login Failure Lock Out:  No
   Login Failure Count:     0
   Last Login Failure:      None
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"AAA, role-based management, Radius, and TACACS+ commands"

show web ssl cipher

Displays the current Apache SSL cipher string.

Syntax

show web ssl cipher

Parameters

None

Example

```
amnesiac (config) # show web ssl cipher
    Apache SSL cipher string:
```

Product

Controller, Mobile Controller, SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

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

- Connect to the CLI and enter the following commands:

```
login as: admin
Riverbed SteelHead
Last login: Wed Jan 20 13:02:09 2017 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 14.

Although most of the SteelHead configuration commands are also available in the SteelHead Interceptor, Controller, SteelCentral Controller for SteelHead Mobile, and SteelHead (in the cloud), We strongly recommend that you do not use the CLI to perform configuration tasks on these products. We recommend 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 document.

System administration commands

This section describes commands you use to perform system administration tasks. Many system administration commands are common to the Controller, the SteelHead Interceptor, and the SteelHead. This section includes the following types of system administration commands:

Alarm commands

This section describes the commands to configure alarm settings.

alarm clear

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“alarm enable,” “alarm clear-threshold,” “show alarm,” “show alarms”

alarm clear-threshold

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>	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

SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“alarm enable,” “alarm clear,” “show alarm,” “show alarms”

alarm enable

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 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 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 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 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 moves out of this condition. ▪ **appliance_unlicensed** - This alarm triggers if the SteelHead 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 SteelHead-v 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 SteelHead-v appliance. ▪ **bypass** - This alarm should not be disabled. It indicates that the system is in bypass mode. If the SteelHead 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_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(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.

<type> (cont)

- **cf_neighbor_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, or if path selection is enabled locally and the neighbor does not have path selection enabled. The SteelHead neighbors pass through IPv6 connections when this alarm triggers.

cf_read_info_timeout_aggr - This alarm indicates that the SteelHead has timed out while waiting for an initialization message from the connection-forwarding neighbor.

- **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
- **critical_temp** - This alarm indicates that the CPU temperature has exceeded the critical threshold. The default value for the rising threshold temperature is 80ºC; the default reset threshold temperature is 70ºC.
- **crl_error: SSL_CAs** - Indicates that an SSL peering certificate has failed to reenroll automatically within the Simple Certificate Enrollment Protocol (SCEP) polling interval.
- **crl_error: SSL_Peering_CAs** - Indicates that an SSL peering certificate has failed to reenroll automatically within the Simple Certificate Enrollment Protocol (SCEP) polling interval.
- **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:<x>:status** - These alarms indicate 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.
- **fan_error** - This alarm indicates that the system has detected a fan error.

<type> (cont)

- **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 continues to function normally. When this error triggers you cannot perform a software upgrade, as the SteelHead 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 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.
- **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.
- **hsm_privatekey_error** - This alarm indicates that the Hardware Security Module (HSM) SSL private key is not accessible.
- **inbound_qos_wan_bw_err** - Enables an alarm and sends an email notification if the inbound QoS WAN bandwidth for one or more of the interfaces is set incorrectly. You must configure the WAN bandwidth to be less than or equal to the interface bandwidth link rate.
- **ipmi** - This alarm indicates that the system has detected an Intelligent Platform Management (IPMI) event. This alarm is not supported on all appliance models.
- **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-F00xxx (expired) and LK1-F00-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: <x> -** These alarms indicate 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.
- **memory_error** - This alarm indicates that the system has detected a memory error.

<type> (cont)

- **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.
- **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 5.5 to 6.0), the system has detected a preexisting 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 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 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
  ```

- **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 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 does not have enough disk, memory, CPU cores, or NIC cards to support the current configuration.
  - The SteelHead 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.
- **outbound_qos_wan_bw_err** - Enables an alarm and sends an email notification if the outbound QoS WAN bandwidth for one or more of the interfaces is set incorrectly. You must configure the WAN bandwidth to be less than or equal to the interface bandwidth link rate.
- **paging** - This alarm indicates whether the system has reached the memory paging threshold. If 100 pages are swapped approximately every two hours the SteelHead 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 predefined uplinks for a connection is unavailable because it has exceeded either the timeout value for uplink latency or the threshold for observed packet loss.
- **path_selection_path_probe_err** - This alarm indicates that a path selection monitoring probe for a predefined uplink has received a probe response from an unexpected relay or interface.

<type> (cont)	▪ **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 SteelFusion 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+ SteelFusion SteelHead. 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. ▪ **secure_transport_controller_unreachable** - This alarm indicates a network connectivity failure to the Controller for the secure transport feature. Issues that might trigger this alarm are Controller services down because of an upgrade or a network connectivity failure to the Controller. ▪ **secure_transport_registration_failed** - This alarm indicates that the peer SteelHead is not registered with the Controller and the Controller does not recognize it as a member of the secure transport group. ▪ **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 connection forwarding neighbor is lost. ▪ **smb_alert** - This alarm indicates that the system has detected an SMB signing error. ▪ **ssd_wear -** This alarm is the parent alarm for ssd_wear_warning. This alarm triggers if one of the ssd_wear_warning:<x> alarms becomes active.

<type> (cont)	▪ **ssd_wear_warning** - This alarm indicates that the specified disk is approaching its write cycle limit. (Appears only on SteelHead 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_reenroll** - This alarm indicates that the system has detected an SCEP error. The SteelHead 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_mismatch_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. To resolve the problem, upgrade your system software.
	▪ **system_detail_report** - This alarm indicates that a system component has encountered a problem. This alarm is disabled by default (RiOS 7.0.3 and later).
	▪ **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.
	▪ **warning_temp** - This alarm indicates whether the CPU temperature has exceeded the warning threshold. The default value for the rising threshold temperature is 80°C; the default reset threshold temperature is 70°C.
	▪ **web_proxy_config_alarm** - This alarm triggers when the cache configuration size is less than the actual cache size. By default, this alarm is enabled.
	▪ **web_proxy_service_alarm** - This alarm triggers when the web proxy service is disabled. By default, this alarm is enabled.

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“alarm clear,” “alarm clear-threshold,” “alarm error-threshold,” “show alarm,” “show alarms”

alarm error-threshold

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>	Threshold level. The threshold level and possible values depend on the alarm type.

Usage

The **no** command option resets the threshold to the default level.

Example

```
amnesiac (config) # alarm cpu_util_indiv error-threshold 80
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"alarm clear," "alarm clear-threshold," "alarm enable," "show alarm," "show alarms"

alarm rate-limit

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	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 3500
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“alarm clear,” “alarm clear-threshold,” “alarm enable,” “alarm error-threshold,” “show alarm,” “show alarms”

---

alarms reset-all

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“alarm clear,” “alarm clear-threshold,” “alarm enable,” “show alarm,” “show alarms”

Host setup commands

---

arp

Creates static ARP entries in the ARP table.

Syntax

[no] arp <ip-address> <mac-address>

Parameters

<ip-address>	IP address of the appliance.
<mac-address>	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

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

"show arp"

clock timezone

Sets the current time zone.

Syntax

clock timezone <zone>

Parameters

<zone>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show clock"

hostname

Sets the hostname for this system.

Syntax

[no] hostname <hostname>

Parameters

<hostname>	Hostname for the system. Do not include the domain name.

Usage

The **no** command option removes the hostname for this appliance.

Example

```
amnesiac (config) # hostname park
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show hosts"

interface

Configures system interfaces.

Syntax

[**no**] **interface <interface-name> <options>**

Parameters

<interface-name>	Interface name: **lo**, **aux**, **lan0_0**, **wan0_0**, **primary**, **in-path0_0**. The interface name varies according to the Riverbed product you are configuring. For example, for the SteelCentral Controller for SteelHead Mobile 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** - Enables DHCP on the interface. ▪ **dhcpv6** - Enables DHCPv6 on the 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. ▪ **dhcpv6 renew** - Enables DHCPv6 on the interface or renews DHCPv6. Setting DHCPv6 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 SteelCentral Controller for SteelHead Mobile. ▪ **dhcpv6 dynamic-dns** - Enables DHCPv6 hostname registration with dynamic DNS. This option is not available on the SteelCentral Controller for SteelHead Mobile. ▪ **duplex <speed>** - Specifies the duplex speed: **auto**, **full**, **half**. The default value is **auto**. ▪ **ip address <ip-address> <netmask>** - Specifies the IP address and netmask for the interface. ▪ **ipv6 address <ipv6-address> <prefix-length>** - Specifies the IPv6 address and prefix length for the interface. Your SteelHead 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>** - Specifies 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. ▪ **public-ip <address> [port <port>]** - Specifies the public IP address and optionally the port number. You can use this option to configure multiple public IP addresses and ports on a single in-path interface. Secure transport uses this configuration to reach public uplinks through SteelHead in-path interfaces. The default port for the public IP address is 4500. ▪ **shutdown** - Shuts down the interface. ▪ **speed <speed>** - Specifies the speed for the interface: **auto**, **10**, **100**, **1000**. The default value is 100.

<options> (cont)

- **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 SteelCentral Controller for SteelHead Mobile.

  In fail-to-block mode, if the SteelHead has an internal software failure or power loss, the SteelHead 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 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 WAN and LAN ports to serve as an Ethernet crossover cable. In fail-to-wire mode, SteelHeads cannot view or optimize traffic. Instead, all traffic is passed through the SteelHead unoptimized. All SteelHead in-path interfaces support fail-to-wire mode. Fail-to-wire mode is the default setting for SteelHeads.

  For details about enabling and disabling fail-to-block, see the *SteelHead Deployment Guide*.

Usage

The **no** command option disables the interface settings.

The **no interface <inpath-interface> public-ip** command option clears all public IP addresses on the specified in-path interface.

Example

```
amnesiac (config) # no interface inpath0_0 fail-to-bypass enable

amnesiac (config) # interface inpath0_0 public-ip 10.5.5.5
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path mgmt-interface,” “ipv6 in-path-gateway,” “show ipv6 default-gateway,” “show public-ip”

interface mtu-override enable

Enables an MTU override of the physical interface.

Syntax

[no] interface mtu-override enable

Parameters

None

Usage

In RiOS 8.0 and later, the SteelHead does not pass through packets larger than the MTU value of its interfaces, nor does it send ICMP notifications to the sending host of the dropped packets. Use this command so larger packets can pass through in environments in which the in-path MTU is lowered to account for a smaller MTU in the WAN network.

Example

```
amnesiac (config) # interface mtu-override enable
amnesiac (config) # interface inpath0_0 mtu 1300
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show interfaces mtu-override"

ip default-gateway

Sets the default gateway for the appliance.

Syntax

[no] ip default-gateway <ip-address>

Parameters

<ip-address>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show ip," "ipv6 default-gateway"

ip domain-list

Adds a domain name to the domain list for resolving hostnames.

Syntax

[no] ip domain-list <domain>

Parameters

<domain>	Domain name.

Usage

The **no** command option removes a domain from the domain list.

Example

```
amnesiac (config) # ip domain-list example.com
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show hosts”

ip host

Adds an entry to the static host table.

Syntax

[no] ip host <hostname> <ipv4-address>

Parameters

<hostname>	Hostname.
<ipv4-address>	IPv4 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show hosts”

in-path peering-ipv6 enable

Enables enhanced IPv6 autodiscovery.

Syntax

[no] in-path peering-ipv6 enable

Parameters

None

Usage

Enhanced IPv6 autodiscovery is disabled by default.

Enabling enhanced IPv6 discovery allows the SteelHeads to automatically discover other SteelHeads deployed in the network to handle IPv6 traffic intended to be optimized.

Enhanced autodiscovery is supported in SteelHeads in networks that run IPv6 (IPv6 single-stack), in addition to IPv4. SteelHeads running RiOS versions 8.5 to 9.2 require either IPv4 for the TCP inner connections between the peer SteelHeads or fixed-target rules.

You must configure an IPv6 address on the in-path interface before enabling this command.

Example

```
amnesiac (config) # in-path peering-ipv6 enable
```

Product

SteelHead CX , SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path peering-ipv6”

ipv6 default-gateway

Configures a default IPv6 route.

Syntax

[no] **ipv6 default-gateway <ipv6-address>**

Parameters

<ipv6-address>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show domain,” “ipv6 route”

ipv6 in-path-gateway

Configures an in-path IPv6 default gateway.

Syntax

[no] **ipv6 in-path-gateway <interface> <destination>**

Parameters

<interface>	Interface on which to configure the IPv6 address of the in-path gateway.
<destination>	IPv6 address of the in-path gateway. Use the format Use the format x:x:x::x/xxx..

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“ipv6 in-path route,” “show ipv6 default-gateway”

ipv6 in-path route

Adds IPv6 in-path routes to the IPv6 network prefix.

Syntax

[no] ipv6 in-path route <interface> <ipv6-network-prefix> <ipv6-address>

Parameters

<interface>	Interface name, for example, **inpath0_0** or **inpath0_1.**
<ipv6-network-prefix>	IPv6 network prefix. Use the format x:x:x::x/xxx.
<ipv6-address>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“ipv6 in-path-gateway,” “show ipv6 in-path route”

ipv6 route

Adds static IPv6 routes to the IPv6 destination address.

Syntax

[no] ipv6 route <ipv6-destination> <prefix-length> <ipv6-address>

Parameters

<ipv6-destination>	IPv6 destination address.
<prefix-length>	IPv6 prefix length. A valid entry is a number from 0 to 128.
<ipv6-address>	Next-hop IPv6 address in this route.

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show domain,” “ipv6 default-gateway”

ip name-server

Adds a DNS name server.

Syntax

[no] ip name-server <ip-address>

Parameters

<ip-address>	IP address of the name server.

Usage

The **no** command option removes a DNS name server.

Example

```
amnesiac (config) # ip name-server 10.10.10.1
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show hosts"

ip route

Adds a static route.

Syntax

[no] ip route <network-prefix> <netmask> <netmask-length> <next-hop-ip-address>

Parameters

<network-prefix>	Network prefix.
<netmask>	Netmask, for example, **255.255.255.0**.
<netmask-length>	Netmask length, for example, **/24**.
<next-hop-ip-address>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-c, SteelHead-v, SteelHead-c

Related Commands

"show ip"

limit connection

Sets the connection limit for the source IP address.

Syntax

[no] limit connection <limit>

Parameters

<limit>	Connection limit.

Usage

The **no** command option disables the connection limit.

Example

```
amnesiac (config) # limit connection 200
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show limit connection"

ntp authentication

Configures the Network Time Protocol (NTP) authentication settings to authenticate NTP servers and peers.

Syntax

[**no**] **ntp authentication key <key-id> <type> secret <string>**

Parameters

key <key-id>	Specifies the key identifier. The key ID values must be in the range from 1 to 65534.
<type>	Authentication algorithm type for the key ID: ▪ **MD5** - Specifies the message digest algorithm. ▪ **SHA1** - Specifies the secure hash algorithm.
secret <string>	Specifies the shared secret parameter. Choose one of the following: ▪ **<plaintext>** - Shared secret in plain text. This option is the same as the **0 <plaintext>** option and is provided for backward compatibility. ▪ **0 <plaintext>** - Specifies the shared secret in plain text. ▪ **7 <encrypted-string>** - Specifies the shared secret with an encrypted string.

Usage

The **no** command option 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.

NTP using either SHA authentication keys or no authentication keys is FIPS compliant. NTP using MD5 keys is not FIPS compliant. See the *FIPS Administrator's Guide* for more information.

Example

```
amnesiac (config) # ntp authentication key 56732 sha1 secret zza419
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"ntp authentication trustedkeys," "ntp peer key," "ntp server key," "show ntp," "show ntp authentication"

ntp authentication trustedkeys

Adds a configured key ID to the trusted keys list.

Syntax

[no] ntp authentication trustedkeys <key-id> [<key-id>, ...]

Parameters

<key-id> [<key-id>, ...]	Specifies 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 option 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 authentication trustedkeys 56732
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"ntp authentication," "ntp peer key," "ntp server key," "show ntp authentication"

ntp disable

Disables Network Time Protocol (NTP) support.

Syntax

[no] ntp disable

Parameters

None

Usage

The **no** command option enables NTP support.

Example

```
amnesiac (config) # ntp disable
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show ntp"

ntp enable

Enables Network Time Protocol (NTP) support.

Syntax

[no] ntp enable

Parameters

None

Usage

The **no** command option disables NTP support.

Example

```
amnesiac (config) # ntp enable
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show ntp"

ntp peer

Enables an NTP peer.

Syntax

[no] ntp peer {<hostname> | < ip-address>} [version <number>]

Parameters

<hostname>	NTP peer hostname.
<ip-address>	IPv4 or IPv6 address of the NTP peer.
version <number>	Specifies the NTP version number.

Usage

The **no** command option disables an NTP peer.

Example

```
amnesiac (config) # ntp peer 10.10.10.1
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show ntp," "show ntp active-peers"

ntp peer enable

Enables an NTP peer.

Syntax

[no] ntp peer {<hostname> | <ip-address >} enable

Parameters

<hostname>	Hostname of the NTP peer.
<ip-address>	IP address of the NTP peer.

Usage

The **no** command option removes an NTP server.

Example

```
amnesiac (config) # ntp peer companypeer enable
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-c

Related Commands

"show ntp"

ntp peer key

Configures an NTP peer with an authentication key ID.

Syntax

[no] ntp peer {<hostname> | <ip-address>} key <key-id>

Parameters

<hostname>	NTP peer hostname or IP address.
<ip-address>	IP address.
<key-id> [key-id, ...]	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show ntp," "show ntp active-peers"

ntp server

Configures an NTP server with the default NTP version number or with a specified version number.

Syntax

[no] ntp server {<hostname | ip-address>} [version <number>]

Parameters

<hostname>	Hostname of the NTP server to synchronize with.
<ip-address>	IP address of the NTP server to synchronize with.
version <number>	Specifies the NTP version number of this server.

Usage

The **no** command option removes an NTP server.

Example

```
amnesiac (config) # ntp server 10.10.10.1
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ntp,” “show ntp active-peers”

ntp server enable

Enables an NTP server.

Syntax

[no] ntp server <hostname | ip-address > enable

Parameters

<hostname>	Hostname of the NTP server.
<ip-address>	IP address of the NTP server.

Usage

The **no** command option removes an NTP server.

Example

```
amnesiac (config) # ntp server companyserver enable
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ntp”

ntp server key

Configures an NTP server with an authentication key ID.

Syntax

[no] ntp server {<hostname | ip-address>} key <key-id>

Parameters

<hostname>	Hostname of the NTP server to authenticate.
<ip-address>	IP address of the NTP server to authenticate.
<key-id>	Key identifier. The key ID values must be in the range 1 to 65534.

Usage

The **no** command option 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“ntp authentication,” “ntp authentication trustedkeys,” “ntp peer key,” “show ntp authentication”

telnet-server enable

Enables you to access the CLI using Telnet. This command 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show telnet-server”

telnet-server permit-admin

Allows administrator login through an unsecured Telnet server.

Syntax

[no] telnet-server permit-admin

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 permit-admin
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"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 supports authentication and authorization.

aaa accounting per-command default

Configures per-command account settings.

Syntax

[no] aaa accounting per-command default <method>

Parameters

<method>	Authentication method: **tacacs+** or **local**. You can enter multiple methods separated by a space.

Usage

The SteelHead 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show aaa," "show radius," "show tacacs"

aaa authentication cond-fallback

Configures fallback only if the server is unavailable.

Syntax

[no] aaa authentication cond-fallback

Parameters

None

Usage

If enabled, the SteelHead tries the next authentication method only if the servers for the current authentication method are unavailable.

The **no** command option disables fallback mode.

Example

```
amnesiac (config) # aaa authentication cond-fallback
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show aaa," "show radius," "show tacacs"

aaa authentication console-login default

Configures local, RADIUS, or TACACS+ console settings for log in.

Syntax

aaa authentication console-login default <method>

Parameters

<method>	Authentication method: **radius**, **tacacs+,** or **local**. You can enter multiple methods separated by a space.

Usage

The SteelHead 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 username database.

Example

```
amnesiac (config) # aaa authentication console-login default radius tacacs+ local
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show aaa," "show radius," "show tacacs"

aaa authentication login default

Configures local, RADIUS, or TACACS+ login settings.

Syntax

[no] aaa authentication login default <method>

Parameters

<method>	Authentication method: **radius**, **tacacs+**, or **local**. You can enter multiple methods separated by a space.

Usage

The SteelHead 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 username database.

Example

```
amnesiac (config) # aaa authentication login default radius tacacs+
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show aaa," "show radius," "show tacacs"

aaa authorization map default-user

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 <username>

Parameters

<username>	Username 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show aaa," "show protocol domain-auth test delegation server-privs," "show tacacs"

aaa authorization map order

Sets the order for remote-to-local user mappings for RADIUS or TACACS+ server authentication.

Syntax

[no] aaa authorization map order {remote-only | remote-first | local-only}

Parameters

remote-only	Maps 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.
remote-first	If a local-user mapping attribute is returned and it is a valid local username, maps the authenticated user to the local user specified in the attribute. If the attribute is not present or not valid locally, uses the username specified by the default-user command. (This is the default behavior.)
local-only	Maps all remote users to the user specified by the **aaa authorization map default-user <username>** command. Any vendor attributes received by an authentication server are ignored.

Usage

The order determines how the remote user mapping behaves. If the authenticated username is valid locally, the appliance does not perform any mapping. 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 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show aaa,” “show radius,” “show tacacs”

aaa authorization per-command default

Configures authorization mapping settings.

Syntax

[no] aaa authorization per-command default <method>

Parameters

<method>	Authentication method: **tacacs+** or **local**. Use a space-separated list. You can enter multiple methods separated by a space.

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 username database.

Example

```
amnesiac (config) # aaa authorization per-command default tacacs+ local
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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-address> | <hostname>} [auth-port <port>] [auth-type <type>] [timeout <seconds>] [retransmit <retries>] [key <string>]

Parameters

<ip-address>	RADIUS server IPv4or IPv6 address.
<hostname>	RADIUS server hostname.
auth-port <port>	Specifies the authentication port number to use with this RADIUS server. The default value is 1812.
auth-type <type>	Specifies the authentication type to use with this RADIUS server. ▪ **chap** - Specifies Challenge Handshake Authentication Protocol (CHAP), which provides better security than PAP. ▪ **mschapv2** - Specifies Microsoft Challenge Handshake Authentication Protocol version 2 (MSCHAPv2). ▪ **pap** - Specifies Password Authentication Protocol (PAP).
timeout <seconds>	Specifies the time-out period to use with this RADIUS server.
retransmit <retries>	Specifies the number of times the client attempts to authenticate with any RADIUS server. The default value is 1. The range is from 0 to 5. To disable retransmissions, set it to 0.
key <string>	Specifies the shared secret text string used to communicate with this RADIUS server. ▪ **0** - Specifies the shared secret to use with this RADIUS server. ▪ **7** - Specifies the 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-address>** 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.

MSCHAPv2 addresses major security weaknesses found in CHAP and PAP. It provides asymmetric authentication between peers by piggybacking a peer challenge on the Response packet and an authentication response on the Success packet.

Some parameters override the RADIUS server global defaults. For details, see the *SteelHead Deployment Guide*.

The **no** command option stops sending RADIUS authentication requests to the host.

If **no radius-server host <ip-address>** is specified, all radius configurations for the host are deleted.

The **no radius-server host <ip-address> 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"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>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show aaa," "show radius"

radius-server retransmit

Specifies the number of times the client attempts to authenticate with a RADIUS server.

Syntax

[no] radius-server retransmit <retries>

Parameters

<retries>	Number of times the client attempts to authenticate with a RADIUS server. The range is from 0 to 5. The default value is 1.

Usage

This command can be overridden in a **radius-server host** command.

The **no** command option resets to the default value.

Example

```
amnesiac (config) # radius-server retransmit 5
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show aaa,” “show radius”

radius-server timeout

Sets the time-out period, in seconds, for retransmitting a request to a RADIUS server.

Syntax

[no] radius-server timeout <seconds>

Parameters

<seconds>	Time-out for retransmitting a request to a RADIUS server. The range is from 1 to 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show aaa,” “show radius”

rbm user

Assigns 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>	Username.
role <role>	Specifies a role-based management type: ▪ **acceleration_service** - Starts and stops the optimization service. ▪ **basic_diagnostics** - Customizes system diagnostic logs, but does not include TCP dumps. ▪ **cifs_acceleration** - Enables CIFS optimization settings and Overlapping Open Optimization. ▪ **citrix_acceleration** - Configures Citrix ICA optimization. ▪ **cloud_acceleration** - Configures Cloud optimization. ▪ **general_settings** - Configures a per-source IP connection limit and the maximum connection pooling size. ▪ **http_acceleration** - Configures 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** - Configures 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** - Optimizes Oracle E-business application content and forms applications. ▪ **mapi_acceleration** - Optimizes MAPI and set Exchange and NSPI ports. ▪ **network_settings** - Configures these features: – Topology definitions – Site and network definitions – Application definitions – Host interface settings – Network interface settings – DNS cache settings – Hardware assist rules – Host labels and port labels You must include this role for users configuring path selection or enforcing QoS policies in addition to the QoS and path selection roles. ▪ **nfs_acceleration** - Configures NFS optimization. ▪ **notes_acceleration** - Configures Lotus Notes optimization. ▪ **path_selection -** Configures path selection. You must also include the network settings role. ▪ **qos** - Enforces QoS policies. You must also include the network settings role. ▪ **replication_acceleration** - Configures the SDRF/A and FCIP storage optimization modules. ▪ **reports** - Sets system report parameters. ▪ **security_settings** - Configures security settings, including RADIUS and TACACS authentication settings and secure vault password. ▪ **sql_acceleration** - Configures MS-SQL optimization.

role <role>	▪ **ssl_acceleration** - Configures SSL support. ▪ **sys_admin** - Configures a system administrator role. Read-only permission is not allowed for this role. This role allows permission for all other role-based management (RBM) roles, including changing users without being logged in as an administrator. The system administrator role allows you to add or remove a system administrator role for any other user, but not for yourself. ▪ **tcpdump** - Configures TCP dump utility. ▪ **virtual_services_platform** - Adds various types of basic services (such as print, DNS, and DHCP services) in the branch to run in a virtual environment on a SteelHead EX. VSP uses ESXi 5.0 as the virtualization platform. VSP services are available only on the SteelHead EX. ▪ **windows_domain_auth** - Configures Windows domain authentication.
permissions <permissions>	You can also create users, assign passwords to the users, and assign varying configuration roles to the users. 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

SCC, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Host setup commands”

tacacs-server first_hit

Enables a first-hit option for TACACS+ servers.

Syntax

[**no**] **tacacs-server first_hit**

Parameters

None

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
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show aaa," "show tacacs"

tacacs-server host

Adds a TACACS+ server to the set of servers used for authentication.

Syntax

[no] tacacs-server host {<ip-address> | <hostname>} [auth-port <port>] [auth-type <type>] [timeout <seconds>] retransmit <retries> | [key {<string> | key 0 | key 7}]

Parameters

<ip-address>	TACACS+ server IP address.
<hostname>	TACACS+ server hostname.
auth-port <port>	Specifies the authorization port number. The default value is 49.
auth-type <type>	Specifies 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 from 1 to 60. The default value is 3.
retransmit <number>	Specifies the number of times the client attempts to authenticate with any TACACS+ server. The default value is 1. The range is from 0 to 5. To disable retransmissions set it to 0.
key {<string> | key 0 | key 7}	Specifies the shared secret text string used to communicate with this TACACS+ server. ▪ **0** - Shared secret to use with this RADIUS server. ▪ **7** - 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 Deployment Guide*.

If **no tacacs-server host <ip-address>** is specified, all TACACS+ configurations for this host are deleted. The **no tacacs-server host <ip-address> 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show aaa," "show tacacs"

tacacs-server key

Sets the shared secret text string used to communicate with any TACACS+ server.

Syntax

[no] tacacs-server key <string>

Parameters

<string>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show aaa," "show tacacs"

tacacs-server retransmit

Configures the number of times the client attempts to authenticate with any TACACS+ server.

Syntax

[no] tacacs-server retransmit <retries>

Parameters

<retries>	Number of times the client attempts to authenticate with any TACACS+ server. The range is from 0 to 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show aaa," "show tacacs"

tacacs-server timeout

Sets the time-out period for retransmitting a request to any TACACS+ server.

Syntax

[no] tacacs-server timeout <seconds>

Parameters

<seconds>	Time-out for retransmitting a request to any TACACS+ server. The range is from 1 to 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show aaa," "show tacacs"

username disable

Disables the account so that no one can log in.

Syntax

[no] username <user-id> disable

Parameters

<user-id>	User login: **admin** or **monitor**.

Usage

The **no** command option reenables the specified user account.

Example

```
amnesiac (config) # username monitor disable
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show usernames"

username nopassword

Disables password protection for a user.

Syntax

username <user-id> nopassword

Parameters

<user-id>	User login: **admin** or **monitor**.

Example

```
amnesiac (config) # username monitor nopassword
```

Product

SCC, SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show usernames”

username password

Sets the password for the specified user.

Syntax

username <user-id> password <cleartext> [old-password <cleartext>]

Parameters

<user-id>	User login: **admin** or **monitor**.
<cleartext>	Password in cleartext format. The password must be at least six characters.
old-password	Specifies 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show usernames,” “Account control management commands”

username password 0

Sets the password for the specified user in cleartext format.

Syntax

username <user-id> password 0 <cleartext-password>

Parameters

<user-id>	User login: **admin** or **monitor**.
<cleartext-password>	Password in cleartext format. 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show usernames”

username password 7

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 <user-id> password 7 <encrypted-password>

Parameters

<user-id>	User login: **admin** or **monitor**.
<encrypted-password>	Encrypted password. The password must be at least six 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show usernames”

Account control management commands

authentication policy enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show authentication policy," "username password 7"

authentication policy login max-failures

Sets the maximum number of unsuccessful login attempts before temporarily locking the user's access to the SteelHead.

Syntax

authentication policy login max-failures <count> [unlock-time <seconds>]

no authentication policy login max-failures

Parameters

<count>	Maximum number of unsuccessful login attempts before a temporary account lockout.
unlock-time <seconds>	Specifies 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show authentication policy"

authentication policy password

Configures the authentication policy password settings for account control.

Syntax

[no] authentication policy password {change-days <days> | dictionary enable | difference <count> | expire <days> [warn <days>] | length <length> | lock <days> | lower-case <count> | numeric <count> | repeat <count> | reuse-interval <count> | special <count> | upper-case <count>}

Parameters

change-days <days>	Specifies 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>	Specifies 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>	Specifies 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>	Specifies the number of days the user is warned before the password expires. The default for the strong security template is 7.
length <length>	Specifies the minimum password length. The default setting for the strong security template is 14 alphanumeric characters.
lock <days>	Specifies the number of days before an account with an expired password locks.
lower-case <count>	Specifies the minimum number of lowercase letters required in the password. The default for the strong security template is 1.
numeric <count>	Specifies the minimum number of numeric characters required in the password. The default for the strong security template is 1.
repeat <count>	Specifies the maximum number of times a character can occur consecutively.
reuse-interval <count>	Specifies the number of password changes allowed before a password can be reused. The default for the strong security template is 5.
special <count>	Specifies the minimum number of special characters required in the password. The default for the strong security template is 1.
upper-case <count>	Specifies 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“authentication policy template,” “username password,” “username password 7,” “show authentication policy”

authentication policy template

Specifies 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
Maximum characters can occur consecutively in password: 1
Prevent dictionary words in password:                   yes
Minimum days before password change allowed:            1 day
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:      no limit
      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
Maximum characters can occur consecutively in password:  no limit
Prevent dictionary words in password:                    yes
User passwords expire:                                   never
Warn user of an expiring password:                       N/A
User accounts with expired passwords lock:               never
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show authentication policy”

authentication policy user lock never

Configures the user account lock settings for account control management.

Syntax

[**no**] **authentication policy user <username> lock never**

Parameters

<username>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show authentication policy”

authentication policy user login-failures reset

Resets a user account so the user can log in again.

Syntax

[**no**] **authentication policy user <username> login-failures reset**

Parameters

<username>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show authentication policy"

ACL management commands

This section describes the ACL management commands. For details, see the Management Console online help or the *SteelHead User Guide*.

access enable

Enables secure access to a SteelHead using an internal management access control list (ACL).

Syntax

[no] access enable

Parameters

None

Usage

SteelHeads 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.
- restrict inbound IP access to a SteelHead, 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 by IP address, simplifying the integration of SteelHeads into your network. You can also restrict access to certain interfaces or protocols.

This command provides the following safeguards to prevent accidental disconnection from the SteelHead (or the SCC):

- 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 ports 7800, 7801, 7810, 7820, and 7850.
- It always allows a previously connected SCC to connect and tracks any changes to the IP address of the SCC 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.

When you change the default port of services (SSH, HTTP, HTTPS, and so on) on either the client or server-side SteelHead and then create a management ACL rule denying that service, the rule will not work as expected. The SteelHead 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 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 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 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 User Guide*.

The **no** command option disables management ACL.

Example

```
amnesiac (config) # access enable
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show access inbound rules," "show access status"

access inbound rule add

Adds a secure access inbound rule.

Syntax

[no] access inbound rule add [allow | deny] protocol {<protocol-number> [dstport <port-number>} | service <service>} [srcaddr <ip-address>] [interface <interface>] [description <description>] [rulenum <rule-number>] [log {on | off}] [override]

Parameters

allow	Allows a matching packet access to the SteelHead. This is the default action.
deny	Denies access to any matching packets.
protocol <protocol-number>	Specifies the protocol name (**all**, **icmp**, **tcp**, **udp**) or protocol number (**1**, **6**, **17**) in the IP packet header. The default setting is **all**.
dstport <port-number>	Specifies the destination port of the inbound packet. You can also specify port ranges: 1000-30000.
service <service>	Optionally, specify the service name: **http**, **https**, **snmp**, **ssh, soap**, **telnet**.
srcaddr <ip-address>	Specifies the source subnet of the inbound packet; for example, 1.2.3.0/24.
interface <interface>	Specifies an interface name: **primary**, **aux**, **inpath0_0**.
rulenum <rule-number>	Specifies a rule number from **1** to <**N**>, **start**, or **end**. The SteelHeads 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>	Provides a description to facilitate communication about network administration.

log {on | off}	Tracks denied packets in the log. By default, packet logging is enabled.
override	Ignores the warning and forces 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, the destination specifies the SteelHead 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 such as DNS caching. These default rules allow access to certain ports required by these features. The list also includes a default rule that allows access to the SCC. As an example, enter the commands below for your feature if you delete the default ACL rule and need to restore it.

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 that prevents access to the server-side SteelHead, 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 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
dstport 1234 srcaddr 10.0.0.1/16 interface primary rulenum 2
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show access inbound rules,” “show access status”

access inbound rule edit rulenum

Modifies a secure access inbound rule.

Syntax

[no] access inbound rule edit rulenum <rule-number> {protocol <protocol> [dstport <port-number>] | service <service>} [srcaddr <ip-address>] [interface <interface>] [description <description>] [log {on | off}] [action {allow | deny}]

Parameters

<rule-number>	Rule number from **1** to <***n***>, **start**, or **end**. 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.
protocol <protocol>	Specifies the protocol name **(all**, **icmp**, **tcp**, **udp)**, or protocol number (**1**, **6**, **17**) in the IP packet header. The default setting is **all**.
service <service>	Specifies the service name: **http**, **https**, **snmp**, **ssh**, **soap**, or **telnet**.
action allow	Allows a matching packet access to the appliance. This is the default action.
action deny	Denies access to and logs any matching packets.
description <description>	Provides a description to facilitate communication about network administration.
dstport <port-number>	Specifies the destination port. You can also specify port ranges: for example, 1000 to 30000
interface <interface>	Specifies the interface: **primary**, **aux**, or **inpath0_0**.
log on	Enables logging for this command.
log off	Disables logging for this command.
srcaddr <subnet>	Specifies the source subnet. For the subnet address, use the format XXX.XXX.XXX.XXX/XX.

Example

```
amnesiac (config) # access inbound rule edit action allow dstport 1234 srcaddr 10.0.0.1/16 service
http interface primary rulenum 2
```

Example

```
amnesiac (config) # access inbound rule edit rulenum action allow dstport 1234 srcaddr 10.0.0.1/16
service http interface primary rulenum 2
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show access inbound rules,” “show access status”

access inbound rule move

Moves a secure access inbound rule.

Syntax

[no] access inbound rule move <rule-number> to <rule-number> [override]

Parameters

<rule-number> to <rule-number>	Rule number from **1** to *n*, **start**, or **end**. 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	Ignores the warning and forces the rule modification. If you add, delete, edit, or move a rule that could disconnect you from the 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show access inbound rules,” “show access status”

Secure shell access commands

ssh client generate identity user

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>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ssh client”

ssh client user authorized-key key sshv2

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>	Username. Must be an existing local user.
<public-key>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ssh client”

ssh server allowed-ciphers

Sets the list of allowed ciphers for ssh server.

Syntax

[no] ssh server allowed-ciphers <ciphers>

Parameters

<ciphers>	Specifies a 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ssh server”

ssh server allowed-macs

Sets the list of message authentication codes (MACs) allowed for use on the SSH server.

Syntax

[no] ssh server allowed-macs <macs>

Parameters

<macs>	Name of one or more MACs (separated by commas) allowed for use on the SSH server.

Usage

The **no** command option removes the MAC from the list of allowed MACs.

Example

```
amnesiac (config) # ssh server allowed-macs hmac-md5
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ssh server”

ssh server enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ssh server”

ssh server listen enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ssh server”

ssh server listen interface

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>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ssh server”

ssh server port

Sets a port for SSH access.

Syntax

[no] ssh server port <port>

Parameters

<port>	Port for SSH access.

Usage

The **no** command option resets the SSH port to its default.

Example

```
amnesiac (config) # ssh server port 8080
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ssh server”

ssh server v2-only enable

Enables the 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ssh server”

CLI terminal configuration commands

banner login

Creates the system log in banner.

Syntax

[no] banner login <message-string>

Parameters

<message-string>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show bootvar”

banner motd

Creates the system Message of the Day banner.

Syntax

[no] banner motd <message-string>

Parameters

<message-string>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show bootvar”

cli clear-history

Clears the command history for the current user.

Syntax

cli clear-history

Parameters

None

Example

```
amnesiac (config) # cli clear-history
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show cli”

cli default auto-logout

Sets the keyboard inactivity time for automatic log out.

Syntax

[no] cli default auto-logout <minutes>

Parameters

<minutes>	Number of minutes before log out occurs.

Usage

By default, the Steelhead appliance closes the SSH session to the command line after 15 minutes. This timeout interval (in minutes) can be increased or decreased.

This command only affects new sessions.

The **no** command option disables the automatic logout feature.

Example

```
amnesiac (config) # cli default auto-logout 25
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show cli”

cli default paging enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show cli”

cli session

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show cli”

Web configuration commands

This section describes the Management Console configuration commands.

network proxy host

Sets the HTTP, HTTPS, and FTP proxy.

Syntax

[no] network proxy host <ip-address> [port <port>] [user-cred username <username> password <password> [authtype <authentication-type>]]

Parameters

<ip-address>	IP address for the host.
port <port>	Specifies the port for the host.
user-cred	Specifies the user credentials for the autolicensing feature: ▪ **username <username>** - Specifies the username. ▪ **password <password>** - Specifies the password in cleartext format.
authtype <authentication-type>	Specifies the authentication type: ▪ **basic** - Authenticates user credentials by requesting a valid username 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 to use a network proxy to contact the Riverbed licensing portal and fetch licenses in a secure environment. You can optionally require user credentials to communicate with the network 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 network proxy settings to the default behavior. Network 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) # network proxy host 10.1.2.1 port 1220
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web auto-logout

Sets the number of minutes before the Management Console automatically logs out the user.

Syntax

[no] web auto-logout <minutes>

Parameters

<minutes>	Number of minutes before the system automatically logs out the user. The default value is 15.

Usage

The **no** command option disables the automatic log out feature.

Example

```
amnesiac (config) # web auto-logout 20
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

---

web auto-refresh timeout

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

---

web enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web http enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web http port

Sets the web port for HTTP access.

Syntax

[no] web http port <port>

Parameters

<port>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web http redirect

Redirects all HTTP access to HTTPS.

Syntax

[no] web http redirect

Parameters

None

Usage

This command redirects HTTP access from port 80 to port 443 for HTTPS access. The **no** version of the command disables redirection of all HTTP access to HTTPS.

Example

```
amnesiac (config) # web http redirect
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show web"

---

web httpd listen enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show web"

---

web httpd listen interface

Adds an interface to the web server access restriction list.

Syntax

[no] web httpd listen interface <interface>

Parameters

<interface>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web httpd log-format

Changes the web server log format (Apache httpd LogFormat).

Syntax

[no] web httpd log-format <apache-httpd-log-format>

Parameters

<apache-httpd-log-format>	Log format arguments for Apache LogFormat. For detailed information about the Apache LogFormat arguments, see http://httpd.apache.org/docs.

Usage

The **no** command returns to the default web server log format.

Example

```
amnesiac (config) # web httpd log-format "%h %l %u %t \"%r\" %>s %b"
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web httpd server-header

Changes the Apache Server header line.

Syntax

[no] web httpd server-header "<server: header line>"

Parameters

"<server: header line>"	Apache Server header line. For detailed information about the Apache Server header line, see http://httpd.apache.org/docs.

Usage

The **no** command option returns to the default "Server:" header line.

Example

```
amnesiac (config) # web httpd server-header "Server:Example HTTPD Server"
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web https enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web https port

Sets the HTTPS secure web port.

Syntax

[no] web https port <port>

Parameters

<port>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web prefs graphs anti-aliasing

Enables anti-aliasing for graphics in the Management Console.

Syntax

[no] web prefs graphs anti-aliasing

Parameters

None

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # web prefs graphs anti-aliasing
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web prefs”

web prefs log lines

Sets the number of lines for the system log page.

Syntax

[no] web prefs log lines <number>

Parameters

<number>	Number of lines per log page.

Usage

The **no** command option disables the number of log lines.

Example

```
amnesiac (config) # web prefs log lines 10
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web rest-server enable

Enables the Representational State Transfer (REST) 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“papi rest access_code generate,” “papi rest access_code import,” “show papi rest access_codes,” “show web”

web session renewal

Sets the session renewal time.

Syntax

[no] web session renewal <minutes>

Parameters

<minutes>	Number of minutes. The default value is 10 minutes.

Usage

The session renewal time is the time before the web session time-out. If a web request comes in, it automatically renews the session. The **no** command option resets the session renewal time to the default value.

Example

```
amnesiac (config) # web session renewal 5
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web session timeout

Sets the session time-out value.

Syntax

[no] web session timeout <minutes>

Parameters

<minutes>	Number of minutes. The default value is **60** minutes.

Usage

The time-out value is the amount of time the cookie is active. The **no** command option resets the session time-out to the default value.

Example

```
amnesiac (config) # web session timeout 120
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web snmp-trap conf-mode enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web soap-server enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

web soap-server port

Enables the Simple Object Access Protocol (SOAP) server port.

Syntax

[no] web soap-server port <port>

Parameters

<port>	Port number.

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # web soap-server port 1234
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web”

Configuration file commands

cmc enable

Enables auto-registration for the SCC.

Syntax

[no] cmc enable

Parameters

None

Usage

The **no** command option disables SCC auto-registration.

Example

```
amnesiac (config) # cmc enable
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show running-config”

cmc hostname

Sets the CMC hostname used for auto-registration.

Syntax

[no] cmc hostname <hostname>

Parameters

<hostname>	Hostname.

Usage

The **no** command option disables SCC auto-registration.

Example

```
amnesiac (config) # cmc hostname test
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show running-config”

configuration copy

Copies a configuration file.

Syntax

configuration copy <source-name> <new-filename>

Parameters

<source-name>	Name of the source file.
<new-filename>	Name of the destination file.

Example

```
amnesiac (config) # configuration copy westcoast eastcoast
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show info”

configuration delete

Deletes a configuration file.

Syntax

configuration delete <filename>

Parameters

<filename>	Name of the configuration file to delete.

Example

```
amnesiac (config) # configuration delete westcoast
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show info”

configuration factory

Creates a new configuration file.

Syntax

configuration factory <filename>

Parameters

<filename>	Name of the destination file.

Example

```
amnesiac (config) # configuration factory eastcoast
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show info"

configuration fetch

Downloads a configuration file over the network.

Syntax

configuration fetch <location> [**<filename>**]

Parameters

<location>	Location of the configuration file to download in HTTP, SCP, or FTP URL format. For example **scp://<username>:<password>@<hostname>/<path>.**
<filename>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show info"

configuration jump-start

Restarts the configuration wizard.

Syntax

configuration jump-start

Parameters

None

Usage

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.

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show info”

configuration merge

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.

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show info”

configuration move

Moves and renames a configuration file.

Syntax

configuration move <source-name> <dest-name>

Parameters

<source-name>	Name of the source configuration file.
<dest-name>	Name of the new configuration file.

Example

```
amnesiac (config) # configuration move westcoast eastcoast
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show info"

configuration new

Creates a new, blank configuration file.

Syntax

configuration new <new-filename>

Parameters

<new-filename>	Name of the new configuration file.

Example

```
amnesiac (config) # configuration new westcoast
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show info"

configuration revert keep-local

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show info"

configuration revert saved

Reverts the active configuration to the last saved configuration.

Syntax

configuration revert saved

Parameters

None

Example

```
amnesiac (config) # configuration revert saved
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show info”

configuration switch-to

Loads a new configuration file and makes it the active configuration.

Syntax

configuration switch-to <filename>

Parameters

<filename>	Filename. The default filenames are: ▪ **initial -** Specifies the initial configuration. ▪ **initial.bak -** Specifies the initial backup configuration. ▪ **cold -** Specifies the configuration file before SDR has occurred. ▪ **working -** Specifies the current configuration.

Example

```
amnesiac (config) # configuration switch-to cold
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show info”

configuration upload

Uploads the configuration file.

Syntax

configuration upload <filename> <location> [active]

Parameters

<filename>	Configuration filename.
<location>	Location of the configuration file to download in HTTP, SCP, or FTP URL format. For example **scp://<username>:<password>@<hostname>/<path>.**
active	Sets the uploaded file to the active configuration file.

Example

```
amnesiac (config) # configuration upload initial scp://test:MyPassword@example/tmp/
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show info”

configuration write

Writes the current, active configuration file to memory.

Syntax

configuration write [to <filename>]

Parameters

to <filename>	Saves the running configuration to a file.

Example

```
amnesiac (config) # configuration write
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show info”

tcp connection send keep-alive

Configures TCP connection tools for debugging the system.

Syntax

tcp connection send keep-alive local-addr <local-ip-address> local-port <port> remote-addr <remote ip-address> remote-port <port>

Parameters

local-addr <local ip-address> local-port <port> remote-addr <remote ip-address> remote-port <port>	Specifies a local and remote SteelHead for which you want to terminate a connection.

Usage

Enables a keep-alive timer between a local and remote SteelHead 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show tcpdump-x”

tcp connection send pass-reset

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-address> source-port <source-port> dest-addr <destination- ip-address> dest-port <destination-port>

Parameters

source-addr <source ip-address>	Specifies the source IP address.
source-port <source-port>	Specifies the source port.
dest-addr <destination-ip-address>	Specifies the destination IP address.
dest-port <destination-port>	Specifies the destination port.

Usage

Enables you to individually reset passed-through connections on the SteelHead so that upon reestablishment 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show stats traffic passthrough”

tcp connection send reset

Configures TCP connection tools for debugging the system.

Syntax

tcp connection send reset
{both local-addr <local-ip-address> local-port <port> remote-addr <remote-ip-address> remote-port <port> | local-only local-addr <local-ip-address> local-port <port> remote-addr <remote-ip-address> remote-port <port> | remote-only remote-addr <remote-ip-address> remote-port <port> local-addr <local-ip-address> local-port <port>}

Parameters

both local-addr <local ip-address> local-port <port> remote-addr <remote-ip-address> remote-port <port>	Terminates the connection for the local and remote SteelHeads.
local-only local-addr <local-ip-address> local-port <port> remote-addr <remote-ip-address> remote-port <port>	Terminates the connection for the local SteelHead.
remote-only remote-addr <remote-ip-address> remote-port <port> local-addr <local-ip-address> local-port <port>	Terminates the connection for the remote SteelHead.

Usage

Terminates connections between SteelHeads 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 CX, SteelHead EX, SteelHead-v, SteelHead-v, SteelHead-c

Related Commands

“show tcpdump-x”

write memory

Saves the current configuration settings to memory.

Syntax

write memory

Parameters

None

Example

```
amnesiac (config) # write memory
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show info”

write terminal

Displays commands to re-create the current running configuration.

Syntax

write terminal

Parameters

None

Example

```
amnesiac (config) # write terminal
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show info”

Statistics manipulation commands

stats settings

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>	Specifies a port to be monitored for statistics.
desc <string>	Specifies a description for the port.
top-talkers enable	Enables top-talkers.
top-talkers interval <hours>	Specifies the top talkers collection interval: **24** or **48** hours.

Example

```
amnesiac (config) # stats settings top-talkers enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show stats bandwidth”

stats settings app-vis enable

Enables the generation of statistics about application-based traffic flowing through the SteelHead.

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 a while to view the most meaningful data display.

The **no** command option disables 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 User Guide* for details about viewing and interpreting Application Statistics reports.

Example

```
amnesiac (config) # stats settings app-vis enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show stats settings app-vis"

stats settings totalwantxbps enable

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 User Guide* for details about viewing and interpreting the WAN throughput report.

Example

```
amnesiac (config) # stats settings totalwantxbps enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show stats bandwidth"

Notification commands

email autosupport enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show email”

email domain

Sets the domain or IP address for email notifications.

Syntax

[no] email domain {<hostname> | <ip-address>}

Parameters

<hostname>	Domain for email notifications (only if the email address does not contain it).
<ip-address>	IP address for email notifications.

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show domain”

email from-address

Sets the address from which email messages appear to come.

Syntax

[no] email from-address <email-address>

Parameters

<email-address>	Full username and domain to appear in the email "From:" address.

Usage

Use this 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show domain,” “show email”

email mailhub

Sets the SMTP server for email notifications.

Syntax

[no] email mailhub {<hostname> | <ip-address>}

Parameters

<hostname>	Specifies the SMTP hostname for email notifications.
<ip-address>	Specifies the SMTP IP address for email notifications.

Usage

The **no** command option disables the SMTP server.

Example

```
amnesiac (config) # email mailhub mail-server.example.com
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show email”

email mailhub-port

Sets the email port for email notifications.

Syntax

[no] email mailhub-port <port>

Parameters

<port>	Email port for email notifications.

Usage

The **no** command option disables the email port.

Example

```
amnesiac (config) # email mailhub-port 135
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-c

Related Commands

“show email”

email notify events enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show email”

email notify events recipient

Sets the email address for notification of events.

Syntax

[no] email notify events recipient <email-address>

Parameters

<email-address>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show email”

email notify failures enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show email”

email notify failures recipient

Enables email notification of system failures, such as core dumps.

Syntax

[no] email notify failures recipient <email-address>

Parameters

recipient <email-address>	Specifies 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show email”

email notify passthrough rule enable

Enables or disables sending email reminders about pass-through rules and, optionally, sets the frequency of the email reminders.

Syntax

[no] email notify passthrough rule [notify-timer <frequency>] enable

Parameters

notify-timer <frequency>	Number of days to wait before receiving the next email reminder. By default, email reminders are sent every 15 days.

Usage

Pass-through rules are often created as a solution for a temporary network issue. When the issue is resolved, it's easy to forget that the rule is in use, which results in traffic not being optimized. With this command enabled, you'll receive an email message reminding you that you have pass-through rules in use on your network, and asking you to check periodically whether you still need to use them. The email reminders help to identify any obsolete rules that you might want to delete to improve traffic optimization.

This command is enabled by default. To turn off the email reminders for all pass-through rules (in-path and load-balancing), use the **no** command option without using the **notify-timer** keyword and specifying a frequency.

To renable email reminders, use this command along with the **in-path rule pass-through email-notify** command for in-path pass-through rules and the **load balance rule pass email-notify** command for load-balancing pass-through rules.

The email reminders are sent to the addresses shown in the event email recipients field of the **show email** command.

Example

```
amnesiac (config) # no email notify passthrough rule enable
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"in-path rule pass-through," "load balance rule pass," "show email"

email send-test

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show email"

SNMP commands

RiOS provides support for the following:

- SNMP Version 1
- SNMP Version 2c
- 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).
- Access Control Lists (ACLs) for users (v1 and v2c only).

For detailed information about SNMP traps sent to configured servers, see the *SteelHead User 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

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>	Specifies the name of the SNMP server community.
security-level <level>	Specifies 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. This setting determines whether a single atomic message exchange is authenticated. A security level applies to a group, not to an individual user.
read-view <name>	Specifies that read requests will be restricted to this view.

Usage

For details about SNMP traps sent to configured servers, see the Management Console online help or the *SteelHead User 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp”

snmp-server community

Sets an SNMP read-only server community.

Syntax

[no] snmp-server community <name>

Parameters

<name>	Name of the SNMP server community. The pound sign (#) and hyphen (-) characters are not allowed at the beginning of the name. If you use either of these characters at the beginning of the name, 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 User 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 312.

This community string overrides any VACM settings.

The **no** command option disables an SNMP server community.

Example

```
amnesiac (config) # snmp-server community ReaDonLy
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show snmp"

snmp-server contact

Sets the SNMP server contact.

Syntax

[no] snmp-server contact <name>

Parameters

<name>	Username of the SNMP server community contact.

Usage

The **no** command option disables the SNMP server contact.

Example

```
amnesiac (config) # snmp-server contact johndoe
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp”

snmp-server enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp”

snmp-server group

Configures the View Access Control Model (VACM) group configuration.

Syntax

[no] snmp-server group <group> security name <name> security-model <model>

Parameters

group <group>	Specifies a group name.
security-name <name>	Specifies 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.
security-model <model>	Specifies a security model: ▪ **v1** - Enables SNMPv1 security model. ▪ **v2c** - Enables SNMPv2c security model. ▪ **usm** - Enables User-based Security Model (USM).

Usage

The **no** command option disables the SNMP server group.

Example

```
amnesiac (config) # snmp-server group rvbdgrp security-name riverbed security-model v1
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show snmp"

snmp-server host

Configures hosts to which to send SNMP traps.

Syntax

[no] snmp-server host {<hostname> | <ipv4-address> | <ipv6-address>} traps <community-string>

Parameters

<hostname>	Hostname for SNMP server.
<ipv4-address>	IPv4 address for the SNMP server.
<ipv6-address>	IPv6 address for the SNMP server.
traps <community-string>	Sends 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. The pound sign (#) and hyphen (-) characters are not allowed at the beginning of the community string. **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. If you do not specify a community string value using this command, the system defaults to the value specified in the **snmp-server trap-community** command.

Example

```
amnesiac (config) # snmp-server host 10.0.0.1 traps public
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"snmp-server trap-community," "show snmp"

snmp-server host enable

Enables the SNMP trap receiver.

Syntax

[no] snmp-server host {<hostname> | <ipv4-address>} enable

Parameters

<hostname>	Hostname.
<ipv4-address>	IPv4 address.

Usage

An SNMP trap receiver captures, displays, and logs SNMP traps. The **no** command option disables the SNMP trap receiver.

Example

```
amnesiac (config) # snmp-server host 10.0.0.1 enable
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show snmp"

snmp-server host traps version

Configures the SNMP version of traps to send to the host.

Syntax

[no] snmp-server host {<hostname> | <ip-address>} traps version {1 | 2 c} <community-string> [port <port>]

Parameters

<hostname>	Hostname for the SNMP server.
<ip-address>	IPv4 address or IPv6 address for the SNMP server.
<version>	SNMP version of traps to send to this host: ▪ **1** - SNMPv1 ▪ **2c** - SNMPv2c
<community-string>	Specifies 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. The pound sign (#) and hyphen (-) characters are not allowed at the beginning of the community string.
port <port>	Specifies 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 port 41148
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show snmp," "snmp-server community," "snmp-server security-name"

snmp-server host traps version 3

Configures the SNMP version 3 of traps to send to the host.

Syntax

[no] snmp-server host {<hostname> | <ip-address>} traps version 3 remote-user <name> password {encrypted <key> | plain-text <text>} auth-protocol {md5 | sha} security-level {noauth | auth | authpriv} [priv-protocol <protocol> priv-key {encrypted <key> | plain-text <text>}] [port <port>]

Parameters

<hostname>	Hostname for the SNMP server.
<ip-address>	IPv4 address or IPv6 address for the SNMP server.
remote-user <name>	Specifies the username for SNMPv3.
password encrypted <key>	Specifies the authentication key in the form of an MD5 or SHA digest.
password plaintext <text>	Enables the plain-text password to generate the authentication key.
auth-protocol <protocol>	Specifies the authentication protocol: ▪ **md5** - Enables MD5 security protocol. ▪ **sha** - Enables SHA security protocol.
security-level <level>	Specifies the security level: ▪ **noauth** - No authorization required. ▪ **auth** - Authorization required. ▪ **authpriv** - Authorization and privacy required.
priv-protocol <protocol>	Specifies the privacy protocol: ▪ **aes** - CFB128-AES-128 as the privacy protocol. ▪ **des** - CBC-DES as the privacy protocol.
priv-key <key>	Specifies the privacy key: ▪ **encrypted <key>** - Encrypted privacy key. ▪ **plain-text <text>** - Plain-text privacy key. The plain-text privacy key must be at least 8 characters.
port <port>	Specifies the destination port.

Usage

The **no** command option disables the SNMP server host.

Example

```
amnesiac (config) # snmp-server host 10.12.8.4 traps version 3 remote-user johndoe password plain-
text mypassword auth-protocol md5 security-level auth
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp,” “snmp-server community,” “snmp-server security-name”

snmp-server ifindex

Adds a custom index value for an interface.

Syntax

snmp-server ifindex <interface> <index>

Parameters

<interface>	Interface name: **wan0_0**, **lan0_0**, **wan0_1**, **lan0_1**, **primary**, **aux**, **inpath0_0**, **inpath0_1.**
<index>	Index number.

Example

```
amnesiac (config) # snmp-server ifindex aux 1234
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp”

snmp-server ifindex-persist

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp”

snmp-server ifindex-reset

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp”

snmp-server listen enable

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp”

snmp-server listen interface

Adds an interface to the SNMP server access restriction list.

Syntax

[no] snmp-server listen interface <interface>

Parameters

<interface>	Interface name: **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

```
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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp”

snmp-server location

Sets the value for the system location variable in the MIB.

Syntax

[no] snmp-server location <ip-address>

Parameters

<ip-address>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp”

snmp-server security-name

Configures the SNMP security name.

Syntax

[no] snmp-server security-name <name> community <community-string> source <ip-address> <netmask>

Parameters

<name>	Security name.
community <community-string>	Specifies 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. Community strings allow printable 7-bit ASCII characters except for white spaces. Community strings cannot begin with the pound (#) or hyphen (-) characters. 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 <ip-address> <netmask>	Specifies 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp”

snmp-server trap-community

Configures the default community string for sending traps.

Syntax

[**no**] **snmp-server trap-community <trap-community-name>**

Parameters

<trap-community-name>	Password-like trap-community string to control access. Use a combination of uppercase, lowercase, and numerical characters to reduce the chance of unauthorized access to the SteelHead. Community strings allow printable 7-bit ASCII characters except for white spaces. Community strings cannot begin with the pound (#) or hyphen (-) characters. This trap-community name is the default community string for the **snmp-server host** command.

Usage

The **no** option of this command disables the trap.

Example

```
amnesiac (config) # snmp-server trap-community public
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"snmp-server host," "show snmp"

snmp-server trap-interface

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>	Interface name.

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show snmp"

snmp-server trap-test

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.

Example

```
amnesiac (config) # snmp-server trap-test
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show snmp"

snmp-server user

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>	Username.
password	Specifies the password type: ▪ **encrypted <key>** - Enables encrypted password authentication. ▪ **plain-text <text>** - Enables plain-text password authentication. The plain-text password must be at least eight characters.
auth-protocol	Specifies the authorization protocol: ▪ **MD5** - Enables MD5 security protocol. ▪ **SHA** - Enables SHA security protocol.
priv-protocol	Specifies the privacy protocol: ▪ **AES** - CFB128-AES-128 as the privacy protocol. ▪ **DES** - CBC-DES as the privacy protocol.
priv-key	Specifies the privacy key: ▪ **encrypted <key>** - Encrypted privacy key. ▪ **plain-text <text>** - Plain-text privacy key. The plain-text privacy key must be at least 8 characters.

Usage

The **no** version of this command disables this option.

Example

```
amnesiac (config) # snmp-server user testuser password plain-text testpass auth-protocol SHA
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp”

snmp-server view

Configures changes to the View-based Access Control Model (VACM) configuration.

Syntax

[no] snmp-server view <name> [excluded | included] <oid>

Parameters

<name>	Name of the user.
excluded	Excludes an OID subtree from this view.
included	Includes an OID subtree into this view.
<oid>	Object ID. For example: **.1.3.6.1.2.1.1** or **.iso.org.dod.internet.mgmt.mib-2.system**

Usage

The **no** version of this command disables this option.

Example

```
amnesiac (config) # snmp-server view joedoe included .1.3.6.1.2.1.1
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show snmp”

Logging commands

logging

Adds a remote system log (syslog) server to the system.

Syntax

[no] logging <ip-address> [trap <log-level>]

Parameters

<ip-address>	IPv4 or IPv6 address for the syslog server.
trap <log -level>	Specifies 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show logging”

logging facility

Configures the syslog facilities for logging.

Syntax

[**no**] **logging facility user <local-facility> system <local-facility> perprocess <local-facility>**

Parameters

user <local-facility>	Specifies the local facility for tagging user messages: **local0...local7**
system <local-facility>	Specifies the local facility for tagging system messages: **local0...local7**
perprocess <local-facility>	Specifies the local facility for tagging per-process priority filtering: **local0...local7**

Usage

The local facility is the ID of a syslog packet. The local facility allows a syslog daemon to send the syslog message to the correct log file. The configured logging facility is appended to the log messages.

The **no** command option stops sending the event logs to the server.

Example

```
amnesiac (config) # logging facility user local2 system local3 perprocess local4
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

“show logging”

logging files delete

Deletes the oldest log file or a specified number of the oldest log files.

Syntax

logging files delete oldest <number>

Parameters

oldest <number>	Specifies the number of old log files to delete. The range is from 1 to 10.

Usage

You can also access this command from enable mode.

Example

```
amnesiac (config) # logging files delete oldest 10
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

"show logging"

logging files rotation criteria frequency

Sets the frequency of log rotation.

Syntax

logging files rotation criteria frequency <rotation-frequency>

Parameters

<rotation-frequency>	Frequency of log rotation: **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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show logging"

logging files rotation criteria size

Sets the size, in megabytes, of the log file before rotation occurs.

Syntax

logging files rotation criteria size <size>

Parameters

<size>	Size of the log file to save in megabytes. 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show logging"

logging files rotation force

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show logging”

logging files rotation max-num

Sets the maximum number of log files to keep locally.

Syntax

logging files rotation max-num <number>

Parameters

<number>	Number of log files to keep locally. The range is from 1 to 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-c

Related Commands

“show logging”

logging filter

Sets the minimal level of messages arriving from the specified process to the local subsystem.

Syntax

logging filter <process> <level>

Parameters

<process>	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. ▪ **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>	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 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 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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show logging”

logging local

Sets the minimum severity of log messages saved on the local syslog servers.

Syntax

[no] logging local <log-level>

Parameters

<log-level>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show logging”

logging trap

Sets the minimum severity for messages sent to the remote syslog servers.

Syntax

[no] logging trap <log-level>

Parameters

<log-level>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show logging”

License and hardware upgrade commands

boot bootloader password

Sets the password for the bootloader.

Syntax

boot bootloader password {<password> | 0 <password> | 7 <password>}

Parameters

<password>	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>	Bootloader password in clear text.
7 <password>	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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show images”

boot system

Boots the specified partition the next time the system is rebooted.

Syntax

boot system <partition>

Parameters

<partition>	Partition to boot: **1** or **2**

Example

```
amnesiac (config) # boot system 1
```

Product

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show images”

hardware nic slot

Configures network interface settings.

Syntax

hardware nic slot <slot> mode <mode> [force]

Parameters

slot <slot>	Specifies the network interface card slot. You cannot modify slot 0.
mode <mode>	Specifies the network interface slot mode: ▪ **data** - Selects data mode. ▪ **inpath** - Selects in-path mode, which is the default mode.
force	Skips validation checks. Use caution with this option because certain storage configuration settings may be lost.

Usage

You can use the **hardware nic slot mode data** command option to support products such as SteelFusion. 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 CX, SteelHead EX

Related Commands

“show hardware nic slots,” “show interfaces”

hardware spec activate

Activates hardware specification settings.

Syntax

hardware spec activate <spec>

Parameters

<spec>	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 CX, SteelHead EX

Related Commands

“show hardware spec”

hardware upgrade model

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 CX, SteelHead EX

Related Commands

“show hardware spec”

image boot

Boots the specified system image by default.

Syntax

image boot <partition>

Parameters

<partition>	Partition to boot: **1** or **2**.

Example

```
amnesiac (config) # image boot 1
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

"show version"

image check upgrades

Checks for available software upgrades for the release running on the appliance.

Syntax

image check upgrades [version <version>]

Parameters

version <version>	Specifies 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
9.1.0
amnesiac (config) # image check upgrades version 9.1.0
Upgrade path:
8.5.5 > 9.0.0 > 9.1.0
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

"image fetch version," "show version"

image fetch version

Downloads a version of a software image directly from the Riverbed Support Site.

Syntax

image fetch version <version> [<image-filename>]

Parameters

<version>	Version of the image to download from the Riverbed Support Site.
<image-filename>	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

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

"image check upgrades," "image fetch," "image install," "image upgrade," "show images," "show bootvar," "show info," "show version"

license autolicense enable

Enables automatic license retrieval.

Syntax

[no] license autolicense enable

Parameters

None

Usage

This command enables the SteelHead, 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** command option disables automatic license retrievals.

Example

```
amnesiac (config) # license autolicense enable
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

"show autolicense status"

license autolicense fetch

Immediately initiates the retrieval of an automatic license.

Syntax

license autolicense fetch

Parameters

None

Usage

This 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

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

“show autolicense status”

license autolicense server

Configures autolicense server settings.

Syntax

license autolicense server {<hostname> | <ip-address>}

Parameters

<hostname>	Hostname of the autolicensing server.
<ip-address>	IP address of the autolicensing server.

Usage

This command configures the SteelHead to contact the specified server for license retrieval requests.

Example

```
amnesiac (config) # license autolicense server licensing.company1.com
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

“show autolicense status”

license client init

Initializes the license client.

Syntax

license client init <license-number>

Parameters

<license-number>	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

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

"show licenses"

license clmf challenge

Generates a license challenge string for authentication.

Syntax

license clmf challenge

Parameters

None

Usage

After you install the customer key and feature key, use this command on the appliance to request a challenge for authentication purposes.

You enter the generated challenge onto the Riverbed Licensing Portal at https://support.riverbed.com/content/support/licensing.html to generate a *response*. You then enter the generated response on the appliance using the **license clmf response** command to activate the license.

Example

```
amnesiac (config) # license clmf challenge
DAEBA-ABB6Q-AABY-QAAEC-CACEH-6SMS4-TTAAA-Z7QUY-536GF
```

Product

SteelHead (virtual edition)

Related Commands

"license clmf response," "show licenses"

license clmf customer-key

Sets the customer key.

Syntax

license clmf customer-key <customer-key>

Parameters

<customer-key>	Customer key.

Usage

The customer key is issued and sent to the customer by Riverbed and is used across purchases. Licenses are tied to the customer key and are provided for model performance tier, WAN optimization, and optional add-on features.

For more information, see the *SteelHead (Virtual Edition) Installation Guide*.

Example

```
amnesiac (config) # license clmf customer-key BH7MT-5ACWA-A13FM
```

Product

SteelHead (virtual edition)

Related Commands

"license clmf install," "show licenses"

license clmf delete

Deletes the common license management framework (CLMF) feature key using the index ID.

Syntax

license clmf delete <index-id>

Parameters

<index-id>	Index ID.

Usage

Use the **show licenses** command to determine the index ID of the feature key.

Example

```
amnesiac (config) # license clmf delete 2
```

Product

SteelHead (virtual edition)

Related Commands

"license clmf install," "show licenses"

license clmf install

Installs the common license management framework (CLMF) license using the specified feature key.

Syntax

license clmf install <key>

Parameters

<key>	CLMF feature key.

Usage

This CLMF license is a perpetual license that is not attached to any physical appliance. It can "float" between SteelHead virtual appliances. After you install the feature key sent by Riverbed, this command prompts you to request a challenge and enter a response to complete the validation process.

Follow this workflow of commands to install and validate your license:

- “license clmf customer-key” - Install the customer key that is issued and sent by Riverbed.
- “license clmf install” - Install the feature keys sent by Riverbed.
- “license clmf challenge” - Generate the challenge and then enter it on the Riverbed Licensing Portal.
- “license clmf response” - Enter the response from the licensing portal to complete the challenge and response operation.
- “license clmf delete” - Delete a license if needed.

Use the **show licenses** command any time during this work flow to verify which licenses are installed or need to be validated.

For more information, see the *SteelHead (Virtual Edition) Installation Guide*.

Example

```
amnesiac (config) # license clmf install DAEBA-ABB6Q-AABY-QAAEC-CAGEH-GSMS4-TIAAA-Z7Q07-636GE
License key needs validation, use “license clmf challenge” and “license clmf response” to complete
validation
```

Use the **show licenses** command to verify the status of the licenses. Because the challenge and response operation has not been performed yet, the status shows as “Unlicensed”.

```
amnesiac (config) # show licenses
License Key Id: 1
   License Key:       DAEBA-ABB6Q-AABY-QAAEC-CAGEH-GSMS4-TIAAA-Z7Q07-636GE
   Status:            Unlicensed
   Start time:        Tue Aug 15 2017
   Last Renewal time: Wed Dec 31 2016
   Features:          FIPS
                      SH10BASE
                      SH10CIFS
                      SH10EXCH
                      SH40SSL
                      SH40SCPS
                      VCX-10
```

Product

SteelHead (virtual edition)

Related Commands

“license clmf challenge,” “license clmf response,” “show licenses”

---

license clmf refresh

Initiates a license refresh and validation immediately.

Syntax

license clmf refresh

Parameters

None

Example

```
amnesiac (config) # license clmf refresh
```

Product

SteelHead (virtual edition)

Related Commands

"show licenses"

license clmf response

Enter the license response string that was generated from the Riverbed Licensing Portal.

Syntax

license clmf response <response-string>

Parameters

<response>	License response string.

Usage

Enter the response string on the appliance to complete the challenge and response operation and activate the license. Recall that the response string was generated from the Riverbed Licensing Portal at https://support.riverbed.com/content/support/licensing.html by entering the challenge string.

After a successful challenge and response operation, the license keys are validated and the licensed features will be available for use on the appliance.

Example

```
amnesiac (config) # license clmf response BKCMB-WSNGM-4K627-PPN3G-OHCY6
```

Product

SteelHead (virtual edition)

Related Commands

"license clmf challenge," "show licenses"

license delete

Deletes the specified license key.

Syntax

license delete <license-number>

Parameters

<license-number>	License number.

Example

```
amnesiac (config) # license delete 4
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

"show licenses"

license install

Installs a new software license key.

Syntax

[no] license install <license-key>

Parameters

<license-key>	License key.

Usage

The **no** command option disables this command.

Example

```
amnesiac (config) # license install SH10_B-0000-1-7F14-FC1F
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

"show licenses"

license request gen-key

Displays a new license request string.

Syntax

license request gen-key

Parameters

None

Example

```
amnesiac (config) # license request gen-key
```

Product

SteelHead (virtual edition)

Related Commands

"show licenses"

license request set-token

Specifies the Riverbed-generated token for SteelHead (virtual edition).

Syntax

license request set-token <token>

Parameters

<token>	Token for license request and registration.

Example

```
amnesiac (config) # license request set-token VLAB-XXX123ADDD90DBF9E2254597
```

Product

SteelHead (virtual edition)

Related Commands

"show licenses"

System administration and service commands

This section describes the system administration and service commands.

---

hardware watchdog enable

Enables the hardware watchdog, which monitors the system for hardware errors.

Syntax

hardware watchdog enable

Parameters

None

Example

```
amnesiac (config) # hardware watchdog enable
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller

Related Commands

"show hardware error-log"

---

hardware watchdog shutdown

Shuts down the hardware watchdog.

Syntax

hardware watchdog shutdown

Parameters

None

Example

```
amnesiac (config) # hardware watchdog shutdown
```

Product

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller

Related Commands

"show hardware error-log"

---

service default-port

Sets the default service port.

Syntax

service default-port <port>

Parameters

<port>	New target port. The default service ports are 7800 and 7810.

Usage

Service ports are the ports used for inner connections between SteelHeads.

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

SCC, Interceptor, SteelHead CX, SteelHead EX, Mobile Controller, SteelHead-v, SteelHead-c

Related Commands

“show service ports”

service map-port

Sets a target port for service port mapping.

Syntax

[**no**] **service map-port <dest-port> <service-port>**

Parameters

<dest-port>	Destination port to which you want to map.
<service-port>	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, and you define an in-path, fixed-target rule on the client SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service ports”

service neural-framing

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 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 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service neural-framing”

service port

Sets a new service port to add for multiple service ports. Service ports are the ports used for inner connections between SteelHeads.

Syntax

[no] service port <port>

Parameters

<port>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show service ports"

Product health and usage reporting commands

debug health-report enable

Enables the reporting of product health information.

Syntax

[no] debug health-report enable

Parameters

None

Usage

Riverbed has enhanced its product health reporting. A single encrypted HTTPS connection is now opened from each managed device and periodically delivers anonymized information to secure servers located at comms.usage.riverbed.com:443.

This reporting is enabled by default. To disable reporting of product health information, use the **no** command option.

Example

```
amnesiac (config) # no debug health-report enable
```

Product

SCC, SteelHead CX, SteelHead EX, Interceptor, SteelHead-v, SteelHead-c

Related Commands

"debug uptime-report enable," "show debug health-report"

debug uptime-report enable

Enables the reporting of product usage information.

Syntax

[no] debug uptime-report enable

Parameters

None

Usage

Riverbed has enhanced its product usage reporting by directing a periodic DNS request to a dynamically generated host ending in updates.riverbed.com.

This reporting is enabled by default. To disable reporting of product usage information, use the **no** command option.

Example

```
amnesiac (config) # no debug uptime-report enable
```

Product

SCC, SteelHead CX, SteelHead EX, Interceptor, SteelHead-v, SteelHead-c

Related Commands

"debug health-report enable," "show debug uptime-report"

Performance test commands for SteelHead-v

perf-test run

Runs a performance test for the SteelHead (virtual edition) to validate CPU performance and disk throughput for a target model.

Syntax

perf-test run test {<test-name> | disk_io_rate confirm | optimize_simulate}

Parameters

test <test-name>	Adds a custom test.
test disk_io_rate	Tests the disk throughput rate. The random read and sequential write throughput of each of the data store disks is tested at random locations. This test clears the data store so you need to run it before placing the appliance in a production environment.
confirm	Confirms that you want to complete the disk performance test. This step is required.
test optimize_simulate	Tests simulated optimization performance. This test emulates the optimization service under maximum load, bypassing the network stack. The configuration of the emulated service is based on the real configuration on the appliance.

Usage

After deploying a SteelHead-v, use this command if you want to verify its optimization and disk-usage performance before using it in a production environment. Use the **show perf-test tests** command to view the overall results of the test. Test results indicate the set of SteelHead-v models that can run on the tested appliance.

Example

```
amnesiac (config) # perf-test run test optimize_simulate
```

Product

SteelHead-v

Related Commands

“show perf-test”

SteelHead configuration commands

This section describes commands you use to configure SteelHead features. It includes the following sections:

In-path and virtual in-path support commands

in-path broadcast support enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path”

in-path bundle

Adds a bundle of interfaces for link aggregation protocol support.

Syntax

[no] in-path bundle <bundle-name> interfaces <interface>

Parameters

<bundle-name>	Bundle name.
interfaces <interface>	Specifies a comma-separated list of interfaces (for example, inpath0_0,inpath0_1).

Usage

This command is used to provide support to interoperate with other networking devices that communicate using link aggregation protocols, such as Etherchannel. Link aggregation compatibility allows easier integration into networks with preexisting link aggregation in place. The SteelHead does not terminate the link aggregation protocol and it is transparent to the link aggregation devices.

All interfaces in a bundle must have the same settings including the WAN and LAN interfaces:

- Speed/duplex
- MTU
- VLAN ID
- IP subnet (each interface must have a unique IP address on the same subnet)
- Default gateway

- User defined routing table entries

Once a bundle is configured, the corresponding settings cannot be changed until the bundle is removed. Each bundle can have as many interfaces as you want and you can configure multiple bundles per SteelHead.

Link state propagation must be turned on to propagate the link state. Use the **in-path lsp enable** command to turn on link state propagation.

In a failover scenario, a link state alarm is triggered that shows which in-path interface went down and which in-path interface from the bundle is the backup. The failover logic chooses the next available link from the bundle and moves all the flows from the failed link to the backup link.

You must restart the optimization service for your changes to take effect. The **no** command option removes the bundle of interfaces.

Example

```
amnesiac (config) # in-path bundle bundle1 interfaces inpath0_0,inpath0_1
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“in-path lsp enable,” “show in-path bundles”

in-path enable

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 User Guide*.

The **no** command option disables in-path support.

Example

```
amnesiac (config) # in-path enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path”

in-path interface enable

Enables the in-path interface for optimization.

Syntax

[no] in-path interface <interface> enable

Parameters

<interface>	IP address of the in-path interface. For example, inpath0_0**.**

Usage

This 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 points to the remote SteelHeads 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 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 (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 in the master/backup pair. For details about master and backup commands, see “failover enable” and “failover master”.

The **no** command option disables the in-path interface.

Example

```
amnesiac (config) # in-path interface inpath0_0 enable
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ip”

in-path interface vlan

Enables VLAN support for an in-path interface on a trunked link.

Syntax

[no] in-path interface <interface> vlan <id>

Parameters

<interface>	In-path interface for which the VLAN applies. For example, inpath0_0.
<id>	VLAN identification number. The VLAN identification number is a value with a range from 0 to 4094 (0 specifies no tagging).

Usage

This 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, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path mgmt-interface”

in-path kickoff

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 SteelHeads that use autodiscovery or if you do not have a SteelHead 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 started are reset.

The **no** command option disables the in-path kickoff feature.

Example

```
amnesiac (config) # in-path kickoff
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path peering rules”

in-path lsp enable

Enables link state propagation.

Syntax

[no] in-path lsp enable

Parameters

None

Usage

If you require a SteelHead to fail-to-wire (bypass) when the LAN or WAN ports become disconnected, enable this command. For example, if the LAN interface drops the link then the WAN also drops the link. Link state propagation (LSP) is on by default. 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 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 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, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path lsp”

---

in-path multi-path maintain

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path peering oobtransparency”

---

in-path oop enable

Enables in-path support for networks that utilize Layer-4 switches, PBR, WCCP, and SteelHead Interceptors.

Syntax

[no] in-path oop enable

Parameters

None

Usage

For details, see the Management Console online help or the *SteelHead User Guide*.

The **no** command option disables OOP support.

Example

```
amnesiac (config) # in-path oop enable
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show out-of-path”

in-path rule auto-discover

Adds an autodiscovery rule.

Syntax

[no] in-path rule auto-discover [srcaddr {<ip-address> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<ip-address> | all-ip | all-ipv4 | all-ipv6}] [dstport <port>] [dst-app <application>] [dst-domain <domain-label>] [dst-host <host-label>] [optimization <policy>] [preoptimization <policy>] [latency-opt <policy>] [vlan <vlan-tag-id>] [neural-mode <policy>] [cloud-accel <mode>] [web-proxy <mode>] [wan-visibility {correct | port | full {wan-vis-opt fwd-reset | none] [description <description>] [auto-kickoff {enable | disable}] [rule-enable {true | false}] [rulenum <rule-number>]

Parameters

srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies a single port (number), a port label, or **all** to specify all ports. If you are using domain labels, specifying **all** defaults to ports 80 and 443 for optimization.
dst-app <application>	Specify a destination SaaS application for this rule, such as shrpoint or exchange. You can only specify applications set up for SaaS acceleration on the SteelConnect Manager that manages SaaS acceleration for the appliance.

dst-domain <domain-label>	Specifies a destination domain label for this rule. You configure the domain label settings using the **domain-label** command. When you add a domain label to an existing in-path rule that is using **all-ip** you must change the destination address to **all-ipv4**. Domain labels are only compatible with IPv4. Domain labels and cloud acceleration are mutually exclusive except when the **_cloud-accel-saas** host label is used. To use cloud acceleration with domain labels, we recommend placing the domain labels rules lower than cloud acceleration rules in your rule list so the cloud rules match before the domain label rules. Best practice is to position domain label rules as the last in the list, so RiOS matches all previous rules before matching the domain label rule. We recommend using host labels as the destination IP address for a rule configured with domain labels. The host label limits the connections for the extra processing needed for the domain label check. If you rely on the default rule in the in-path rule set for optimization and would like to incorporate domain-label optimization, see the *SteelHead Deployment Guide* for best practices. Enter an empty string, represented by two quotation marks (""), to remove a domain label.
dst-host <host-label>	Specifies a destination host label for this rule. You configure the host label settings using the **host-label** command. A destination IP address and host label cannot be specified in the same rule. A host label can be used instead of a destination IP address. RiOS versions 9.2.1 and later include a predefined host label, **_cloud-accel-saas_,** that detects any IP addresses that carry Cloud Accelerator-enabled SaaS traffic automatically. As SaaS applications are added or deleted, the host label is automatically updated with the list of associated IP addresses. This host label mitigates the requirement that domain rules and Cloud Acceleration be mutually exclusive. Enter an empty string, represented by two quotation marks (""), to remove a host label.
optimization <policy>	Specifies an optimization policy: ▪ **normal** - Performs LZ compression and SDR. This is the default optimization policy. ▪ **sdr-only** - Turns off LZ compression. ▪ **sdr-m** - Performs data reduction entirely in memory, which prevents the SteelHead 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** - Turns off SDR but perform LZ compression. ▪ **none** - Turns 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 affects passive FTP, while setting the QoS for port 20 on the server-side SteelHead 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 <policy>	Specifies a preoptimization policy: ▪ **ssl** - Enables SSL preoptimization processing for traffic via SSL secure ports. ▪ **oracle-forms** - Enables preoptimization processing for the Oracle Forms browser plug-in. This policy is not compatible with IPv6. ▪ **oracle-forms+ssl** - Enables preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side SteelHead. 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**. Traffic to port 443 always uses a preoptimization policy of SSL, even if an in-path rule on the client-side SteelHead 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. or – modify the peering rule on the server-side SteelHead by setting the SSL capability control to No Check. **Note:** Make sure you set **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 <policy>	Specifies a latency-optimization policy: ▪ **citrix** - Always uses 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 **pre-optimization ssl** option. This policy is not compatible with IPv6. ▪ **http** - Performs HTTP optimization on connections matching this rule. ▪ **normal** - Performs HTTP optimization on ports 80, 8080, and (with SSL pre-optimization) 443. This is the default setting. ▪ **outlook-anywhr** - Always uses Outlook-Anywhere optimization on the connection. ▪ **exchange-auto** - Automatically detects MAPI transport protocols (Autodiscover, Outlook Anywhere, and MAPI over HTTP) and HTTP traffic. ▪ **none** - Does not perform latency optimization on connections matching this rule.
vlan <vlan-tag-id>	Specifies the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0 to 4094. Specify 0 to mark the link untagged.

neural-mode <policy>	Enables neural framing in the SteelHead. 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 uses 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 adjusts the Nagle parameters. The SteelHead 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 uses 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** - Bases the 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>	Specifies a cloud-acceleration 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 SteelHead SaaS. 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 SteelHead SaaS, but it follows the rule's other parameters so that the connection might be optimized by this SteelHead with other SteelHeads in the network, or it might be passed through. Domain labels and cloud acceleration are mutually exclusive except when the **_cloud-accel-saas** host label is used. To use cloud acceleration with domain labels, we recommend placing the domain labels rules lower than cloud acceleration rules in your rule list so the cloud rules match before the domain label rules.

web-proxy <mode>	Specifies the web proxy optimization mode for this rule: ▪ **auto** - Automatically directs all Internet-bound traffic destined to a public IP address on ports 80 and 443 through the web proxy. This is the default setting. An in-path cloud acceleration rule (**cloud_accel <mode>** option) for SaaS takes priority over a web proxy auto mode rule when they are configured together. Only IPv4 addressing is supported. When **auto is** enabled on an Auto Discover rule, and the SteelHead is prioritizing the traffic through the web proxy, the full or port transparency WAN visibility modes have no impact. When the traffic cannot be prioritized through the web proxy, autodiscovery will occur and the full or port transparency modes will be used. ▪ **force** - Forwards any IP address and port matching this rule to the web proxy service. This is a pass-through rule. No address in an SCA server list is web proxied unless the **web-proxy force** mode is configured. ▪ **none** - Does not direct traffic matching this rule through the web proxy service. Web proxy enables a client-side appliance with an autodiscovery or pass-through rule to use a single-ended web proxy to transparently intercept all traffic bound to the Internet. Enabling the web proxy improves performance by providing optimization services such as web object caching and SSL decryption to enable content caching and logging services. You can use host labels and domain labels to define more granular traffic with the web proxy service.
wan-visibility <mode>	Enables WAN visibility, which pertains to how packets traversing the WAN are addressed. RiOS offers three types of WAN visibility modes: correct addressing, port transparency, and full address transparency. You configure WAN visibility on the client-side SteelHead (where the connection is initiated). The server-side SteelHead must also support WAN visibility.(RiOS 5.0 or later). ▪ **correct** - Turns off WAN visibility. Correct addressing uses SteelHead 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** - Enables port address transparency, which 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 SteelHeads 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 SteelHeads) 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 SteelHeads. **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.

wan-visibility <mode> (cont)	▪ **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 SteelHeads 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 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 set 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** - Sets the WAN visibility option to none. **Note:** 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 User Guide* and the *SteelHead Deployment Guide.*
description <description>	Specifies a description to facilitate communication about network administration.

auto-kickoff enable	Enables kickoff, which resets established connections to force them to go through the connection creation process again. 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 6.5 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. **Note:** 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.
auto-kickoff disable	Disables kickoff. By default, auto kickoff per in-path rule is disabled.
rule-enable true	Enables an in-path rule.
rule-enable false	Disables an in-path rule.
rulenum <rule-number>	Specifies 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

Use the autodiscovery process to determine if a remote SteelHead is able to optimize the connection attempting to be created by this SYN packet. By default, autodiscovery 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.

With regular autodiscovery, the SteelHead finds the first remote SteelHead along the connection path of the TCP connection and optimization occurs there. For example, if you had a deployment with four SteelHeads (A, B, C, D) where D represents the appliance that is furthest from A, the SteelHead automatically finds B, then C, and finally D, and optimization takes place in each.

With enhanced autodiscovery (automatic peering), the SteelHead automatically finds the furthest SteelHead along the connection path of the TCP connection and optimization occurs there. For example, in a deployment with four SteelHeads (A, B, C, D), where D represents the appliance that is furthest from A, the SteelHead automatically finds D. This simplifies configuration and makes your deployment more scalable. For details, see the “in-path peering auto”.

Autodiscovery of SteelHeads is supported for IPv6 TCP traffic. However, TCP inner connections between the peer SteelHeads are strictly IPv4.

By default, enhanced autodiscovery is enabled. If you do not enable enhanced autodiscovery the SteelHead uses regular auto-discovery. For details, see the Management Console online help or the *SteelHead Deployment Guide*.

Automatic peering (enhanced autodiscovery) greatly reduces the complexities and time it takes to deploy SteelHeads. 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 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 receives an autodiscovery probe from the unknown SteelHead. To prevent an unknown SteelHead from peering, you must add a pass-through peering rule that passes through traffic from the unknown SteelHead in the remote location. For details, see the "in-path peering rule", or the Management Console online help.

Web proxy is a client-side feature and is controlled and managed from a SteelCentral Controller for SteelHead (SCC). You can configure the in-path rule on the client-side SteelHead running the web proxy or on the SCC. You must also enable the web proxy globally on the SCC, add domains to the global HTTPs whitelist, and create any exceptions to the whitelist. For details, see the *SteelCentral Controller for SteelHead User Guide*.

The **no** command option disables the rule. The **no** command option has the following syntax: **no in-path rule <rule-number>**

Example

The following in-path rule example configures transparency (WAN visibility) for IPv6 traffic only:

```
amnesiac (config) # in-path rule auto-discover srcaddr all-ipv6 dstaddr all-ipv6 wan-visibility full
wan-vis-opt fwd-reset rule-enable true rulenum 4
```

The following in-path rule example configures transparency (WAN visibility) for all traffic:

```
amnesiac (config) # in-path rule auto-discover srcaddr all-ip dstaddr all-ip wan-visibility full
wan-vis-opt fwd-reset rule-enable true rulenum 4
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"domain-label," "in-path rule edit auto-discover," "show in-path," "show in-path rules"

in-path rule edit auto-discover

Edits an autodiscovery rule.

Syntax

in-path rule edit rulenum <rule-number> auto-discover [srcaddr {<ip-address>| all-ip |all-ipv4 | all-ipv6>}] [dstaddr {<ip-address> | all-ip |all-ipv4 | all-ipv6>}] [dstport <port>] [dst-domain <domain-label>] [dst-host <host-label>] [optimization <policy>] [preoptimization <policy>] [latency-opt <policy>] [vlan <vlan-tag-id>] [neural-mode <policy>] [web-proxy <mode>] [wan-visibility correct | port | full {wan-vis-opt fwd-reset | none}] [description <description>] [auto-kickoff {enable | disable}] [rule-enable {true | false}]

Parameters

rulenum <rule-number>	Specifies the rule number to edit: **1-N** or **start** or **end**.
srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.

srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies a single port (number), a port label, or **all** to specify all ports. If you are using domain labels, specifying **all** defaults to ports 80 and 443 for optimization.
dst-domain <domain-label>	Specifies a destination domain label for this rule. You configure the domain label settings using the **domain-label** command. When you add a domain label to an existing in-path rule that is using **all-ip**, you must change the destination address to **all-ipv4**. Domain labels are only compatible with IPv4. Domain labels and cloud acceleration are mutually exclusive. To use cloud acceleration with domain labels, place the domain label rules lower than cloud acceleration rules in your rule list so the cloud rules match before the domain label rules. We recommend positioning domain label rules as the last in the list, so RiOS matches all previous rules before matching the domain label rule. We recommend using host labels as the destination IP address for a rule configured with domain labels. The host label limits the connections for the extra processing needed for the domain label check. If you rely on the default rule in the in-path rule set for optimization and would like to incorporate domain-label optimization, see the *SteelHead Deployment Guide* for best practices. Enter an empty string, represented by two quotation marks (""), to remove a domain label.
dst-host <host-label>	Specifies a destination host label for this rule. You configure the host label settings using the **host-label** command. A destination IP address and host label cannot be specified in the same rule. A host label can be used instead of a destination IP address. Enter an empty string, represented by two quotation marks (""), to remove a host label.

optimization <policy>	Specifies an optimization policy: ▪ **normal** - Performs LZ compression and SDR. This is the default optimization policy. ▪ **sdr-only** - Turns off LZ compression. ▪ **sdr-m** - Performs data reduction entirely in memory, which prevents the SteelHead 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** - Turns off SDR but perform LZ compression. ▪ **none** - Turns 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 affects passive FTP, while setting the QoS for port 20 on the server-side SteelHead 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 <policy>	Specifies a preoptimization policy: ▪ **ssl** - Enables SSL preoptimization processing for traffic via SSL secure ports. ▪ **oracle-forms** - Enables preoptimization processing for the Oracle Forms browser plug-in. This policy is not compatible with IPv6. ▪ **oracle-forms+ssl** - Enables preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side SteelHead. 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**. Traffic to port 443 always uses a preoptimization policy of SSL even if an in-path rule on the client-side SteelHead 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. or – modify the peering rule on the server-side SteelHead by setting the SSL capability control to No Check. **Note:** Make sure you set **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 <policy>	Specifies a latency-optimization policy: ▪ **citrix** - Always uses 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** - Performs HTTP optimization on connections matching this rule. ▪ **normal** - Performs HTTP optimization on ports 80, 8080, and (with SSL preoptimization) 443. This is the default setting. ▪ **outlook-anywhr** - Always uses Outlook-Anywhere optimization on the connection. ▪ **exchange-auto** - Automatically detects MAPI transport protocols (Autodiscover, Outlook Anywhere, and MAPI over HTTP) and HTTP traffic. ▪ **none** - Does not perform latency optimization on connections matching this rule.
vlan <vlan-tag-id>	Specifies the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0 to 4094. Specify 0 to mark the link untagged.
neural-mode <policy>	Enables neural framing in the SteelHead. 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 uses 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 adjusts the Nagle parameters. The SteelHead 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 uses 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** - Bases the 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.

web-proxy <mode>	Specifies the web proxy optimization mode for this rule: ▪ **auto** - Automatically directs all Internet-bound traffic destined to a public IP address on ports 80 and 443 through the web proxy. This is the default setting. An in-path cloud acceleration rule (**cloud_accel <mode>** option) for SaaS takes priority over a web proxy auto mode rule when they are configured together. Only IPv4 addressing is supported. When **auto is** enabled on an Auto Discover rule, and the SteelHead is prioritizing the traffic through the web proxy, the full or port transparency WAN visibility modes have no impact. When the traffic cannot be prioritized through the web proxy, autodiscovery will occur and the full or port transparency modes will be used. ▪ **force** - Forwards any IP address and port matching this rule to the web proxy service. This is a pass-through rule. No address in an SCA server list is web proxied unless the **web-proxy force** mode is configured. ▪ **none** - Does not direct traffic matching this rule through the web proxy service. Web proxy enables a client-side appliance with an autodiscovery or pass-through rule to use a single-ended web proxy to transparently intercept all traffic bound to the Internet. Enabling the web proxy improves performance by providing optimization services such as web object caching and SSL decryption to enable content caching and logging services. You can use host labels and domain labels to define more granular traffic with the web proxy service.
wan-visibility <mode>	Enables WAN visibility, which pertains to how packets traversing the WAN are addressed. RiOS 5.0 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 (where the connection is initiated). The server-side SteelHead must also support WAN visibility (RiOS 5.0 or later). ▪ **correct** - Turns off WAN visibility off. Correct addressing uses SteelHead 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.

wan-visibility <mode> (cont)	▪ **port** - Enables port address transparency, which 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 SteelHeads 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 SteelHeads) 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 SteelHeads 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 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** - Sets the WAN visibility option to none. **Note:** 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 User Guide* and the *SteelHead Deployment Guide.*
description <description>	Specifies a description to facilitate communication about network administration.

auto-kickoff enable	Enables kickoff, which resets established connections to force them to go through the connection creation process again. 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 6.5 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. **Note:** 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.
auto-kickoff disable	Disables kickoff. By default, auto kickoff per in-path rule is disabled.
rule-enable true	Enables an in-path rule.
rule-enable false	Disables an in-path rule.

Usage

Use the autodiscovery process to determine if a remote SteelHead 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.

The **in-path rule auto-discover** command adds an autodiscovery 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“domain-label,” “in-path rule auto-discover,” “show in-path,” “show in-path rules”

in-path rule deny

Adds an in-path rule that rejects connection requests.

Syntax

[no] in-path rule deny [srcaddr {<ip-address>| all-ip | all-ipv4 | all-ipv6}] [dstaddr {<ip-address> | all-ip | all-ipv4 | all-ipv6>}] [dstport <port>] [vlan <vlan-tag-id>] [rule-enable {true | false}] [rulenum <rule-number>] [description <description>]

Parameters

srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
vlan <vlan-tag-id>	Specifies the VLAN tag ID (if any). The VLAN tag ID is a number with a range from 0 to 4094. Specify 0 to mark the link untagged.
rule-enable true	Enables an in-path rule.
rule-enable false	Disables an in-path rule.
rulenum <rule-number>	Specifies 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>	Specifies a description to facilitate network administration.

Usage

The SteelHead 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 <rule-number>

Example

```
amnesiac (config) # in-path rule deny srcaddr 10.0.0.1/24 dstaddr 10.0.0.2/24 rulenum 5 description
test
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"in-path rule edit deny," "show in-path," "show in-path rules"

in-path rule edit deny

Edits an in-path rule that rejects connection requests.

Syntax

in-path rule edit rulenum <rule-number> deny [srcaddr {<ip-address>| 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 <rule-number>	Specifies the rule number to edit: **1-N** or **start** or **end**.
srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
vlan <vlan-tag-id>	Specifies the VLAN tag ID (if any). The VLAN tag ID is a number with a range from 0 to 4094. Specify 0 to mark the link untagged.
rule-enable true	Enables an in-path rule.
rule-enable false	Disables an in-path rule.
description <description>	Specifies a description to facilitate network administration.

Usage

Use this 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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"in-path rule deny," "show in-path," "show in-path rules"

in-path rule discard

Adds an in-path rule that drops connections.

Syntax

[no] in-path rule discard [srcaddr {<ip-address> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<ip-address> | all-ip | all-ipv4 | all-ipv6}] [dstport <port>] [vlan <vlan-tag-id>] [rule-enable {true | false}] [rulenum <rule-number>] [description <description>]

Parameters

srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
vlan <vlan-tag-id>	Specifies the VLAN tag ID (if any). The VLAN tag ID is a number with a range from 0 to 4094. Specify 0 to mark the link untagged.
rule-enable true	Enables an in-path rule.
rule-enable false	Disables an in-path rule.
rulenum <rule-number>	Specifies 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>	Specifies a description to facilitate communication about network administration.

Usage

The SteelHead 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 dstport 1234 rulenum 2
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"in-path rule edit discard," "show in-path," "show in-path rules"

in-path rule edit discard

Edits an in-path rule that drops connections.

Syntax

[no] in-path rule edit rulenum <rule-number> discard [srcaddr {<ip-address> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<ip-address> | all-ip | all-ipv4 | all-ipv6}] [dstport <port>] [vlan <vlan-tag-id>] [rule-enable {true | false}] [description <description>]

Parameters

rulenum <rule-number>	Specifies the rule number to edit: **1-N** or **start** or **end**.
srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
vlan <vlan-tag-id>	Specifies the VLAN tag ID (if any). The VLAN tag ID is a number with a range from 0 to 4094. Specify 0 to mark the link untagged.
rule-enable true	Enables an in-path rule.
rule-enable false	Disables an in-path rule.
description <description>	Specifies 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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"in-path rule discard," "show in-path," "show in-path rules"

in-path rule edit disable

Disables a single in-path rule.

Syntax

in-path rule edit rulenum <rule-number> disable

Parameters

rulenum <rule-number>	Specifies 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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path," "show in-path rules"

in-path rule edit enable

Enables a single in-path rule.

Syntax

in-path rule edit rulenum <rule-number> enable

Parameters

rulenum <rule-number>	Specifies 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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path," "show in-path rules"

in-path rule edit fixed-target

Edits a fixed-target in-path rule.

Syntax

in-path rule edit rulenum <rule-number> fixed-target target-addr <ip-address> [target-port <port>] [dstaddr {<ip-address>| all-ip | all-ipv4 | all-ipv6>}] [dstport <port>] [dst-domain <domain-label>] [dst-host <host-label>] [srcaddr {<ip-address> | all-ip | all-ipv4 | all-ipv6>}] [backup-addr <ip-address>] [backup-port <port>] [optimization <policy>] [preoptimization <policy>] [latency-opt <policy>] [neural-mode <mode>] [vlan <vlan-tag-id>] [description <description>] [auto-kickoff {enable | disable}] [rule-enable {true | false}]

Parameters

rulenum <rule-number>	Specifies the rule number to edit: **1-N** or **start** or **end**.
target-address <ip-address>	Specifies 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.
target-address target-port <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies a single port (number), a port label, or **all** to specify all ports. If you are using domain labels, specifying **all** defaults to ports 80 and 443 for optimization.
dst-domain <domain-label>	Specifies a destination domain label for this rule. You configure the domain label settings using the **domain-label** command. When you add a domain label to an existing in-path rule that is using **all-ip**, you must change the destination address to **all-ipv4**. Domain labels are only compatible with IPv4. We recommend positioning domain label rules as the last in the list, so RiOS matches all previous rules before matching the domain label rule. We recommend using host labels as the destination IP address for a rule configured with domain labels. The host label limits the connections for the extra processing needed for the domain label check. If you rely on the default rule in the in-path rule set for optimization and would like to incorporate domain-label optimization, see the *SteelHead Deployment Guide* for best practices. Enter an empty string, represented by two quotation marks (""), to remove a domain label.
dst-host <host-label>	Specifies a destination host label for this rule. You configure the host label settings using the **host-label** command. A destination IP address and host label cannot be specified in the same rule. A host label can be used instead of a destination IP address. Enter an empty string, represented by two quotation marks (""), to remove a host label.
backup-address <ip-address>	Specifies 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.

backup-port <port>	Specifies a backup port: single port (number), a port label, or **all** to specify all ports.
optimization <policy>	Specifies an optimization policy: ▪ **normal** - Performs LZ compression and SDR. This is the default optimization policy. ▪ **sdr-only** - Turns off LZ compression. ▪ **sdr-m** - Performs data reduction entirely in memory, which prevents the SteelHead 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** - Turns off SDR but perform LZ compression. ▪ **none** - Turns 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 affects passive FTP, while setting the QoS for port 20 on the server-side SteelHead 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 <policy>	Specifies a preoptimization policy: ▪ **ssl** - Specifies **ssl** to enable SSL preoptimization processing for traffic via SSL secure ports. ▪ **oracle-forms** - Enables preoptimization processing for the Oracle Forms browser plug-in. This policy is not compatible with IPv6. ▪ **oracle-forms+ssl** - Enables preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side SteelHead. 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**. Traffic to port 443 always uses a preoptimization policy of SSL even if an in-path rule on the client-side SteelHead 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. or – modify the peering rule on the server-side SteelHead by setting the SSL capability control to No Check. **Note:** 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 <policy>	Specifies a latency-optimization policy: ▪ **citrix** - Always uses 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** - Performs HTTP optimization on connections matching this rule. ▪ **normal** - Performs 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. ▪ **exchange-auto** - Automatically detects MAPI transport protocols (Autodiscover, Outlook Anywhere, and MAPI over HTTP) and HTTP traffic. ▪ **none** - Does not perform latency optimization on connections matching this rule.
neural-mode <mode>	Enables neural framing in the SteelHead. 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 uses 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 adjusts the Nagle parameters. The SteelHead 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 uses 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** - Bases the 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>	Specifies the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0 to 4094. Specify 0 to mark the link untagged.
description <description>	Specifies a description to facilitate network administration.

auto-kickoff enable	Enables kickoff, which resets established connections to force them to go through the connection creation process again. 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 6.5 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. **Note:** 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.
auto-kickoff disable	Disables kickoff. By default, auto kickoff per in-path rule is disabled.
rule-enable true	Enables an in-path rule.
rule-enable false	Disables an in-path rule.

Usage

This 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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“domain-label,” “in-path rule fixed-target,” “show in-path,” “show in-path rules”

in-path rule fixed-target

Adds a fixed-target in-path rule.

Syntax

[no] in-path rule fixed-target target-addr <ip-address> [target-port <port>] [dstaddr {<ip-address> | all-ip |all-ipv4 | all-ipv6>}] [dstport <port>] [dst-domain <domain-label>] [dst-host <host-label>] [srcaddr {<ipv4-addr> | <ipv6-addr>| all-ip |all-ipv4 | all-ipv6>}] [backup-addr {<ip-address>}] [backup-port <port>] [optimization <policy> | [preoptimization <policy>] [latency-opt <policy>] [neural-mode <policy>] [vlan <vlan-tag-id>] [description <description>] [auto-kickoff {enable | disable}] [rulenum <rule-number>] [rule-enable {true | false}]

Parameters

target-addr <ip-address>	Specifies 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.
target-port <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies a single port (number), a port label, or **all** to specify all ports. If you are using domain labels, specifying **all** defaults to ports 80 and 443 for optimization.
dst-domain <domain-label>	Specifies a destination domain label for this rule. You configure the domain label settings using the **domain-label** command. When you add a domain label to an existing in-path rule that is using **all-ip**, you must change the destination address to **all-ipv4**. Domain labels are only compatible with IPv4. Domain labels and cloud acceleration are mutually exclusive. To use cloud acceleration with domain labels, place the domain label rules lower than cloud acceleration rules in your rule list so the cloud rules match before the domain label rules. We recommend positioning domain label rules as the last in the list, so RiOS matches all previous rules before matching the domain label rule. We recommend using host labels as the destination IP address for a rule configured with domain labels. The host label limits the connections for the extra processing needed for the domain label check. If you rely on the default rule in the in-path rule set for optimization and would like to incorporate domain-label optimization, see the *SteelHead Deployment Guide* for best practices. Enter an empty string, represented by two quotation marks (""), to remove a domain label.
dst-host <host-label>	Specifies a destination host label for this rule. You configure the host label settings using the **host-label** command. A destination IP address and host label cannot be specified in the same rule. A host label can be used instead of a destination IP address. Enter an empty string, represented by two quotation marks (""), to remove a host label.

srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
backup-addr <ip-address>	Specifies 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.
backup-port <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
optimization <policy>	Specifies an optimization policy: ▪ **normal** - Performs LZ compression and SDR. This is the default optimization policy. ▪ **sdr-only** - Turns off LZ compression. ▪ **sdr-m** - Performs data reduction entirely in memory, which prevents the SteelHead 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** - Turns off SDR but perform LZ compression. ▪ **none** - Turns 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 affects passive FTP, while setting the QoS for port 20 on the server-side SteelHead 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 <policy>	Specifies a preoptimization policy: ▪ **ssl** - Enables SSL preoptimization processing for traffic via SSL secure ports. ▪ **oracle-forms** - Enables preoptimization processing for the Oracle Forms browser plug-in. This policy is not compatible with IPv6. ▪ **oracle-forms+ssl** - Enables preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side SteelHead. 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**. Traffic to port 443 always uses a preoptimization policy of SSL even if an in-path rule on the client-side SteelHead 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. or – modify the peering rule on the server-side SteelHead by setting the SSL capability control to No Check. **Note:** 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 <policy>	Specifies a latency-optimization policy: ▪ **citrix** - Always uses 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** - Performs HTTP optimization on connections matching this rule. ▪ **normal** - Performs HTTP optimization on ports 80, 8080, and (with SSL preoptimization) 443. This is the default setting. ▪ **outlook-anywhr** - Always uses Outlook-Anywhere optimization on the connection. ▪ **exchange-auto** - Automatically detects MAPI transport protocols (Autodiscover, Outlook Anywhere, and MAPI over HTTP) and HTTP traffic. ▪ **none** - Does not perform latency optimization on connections matching this rule.
neural-mode <policy>	Enables neural framing in the SteelHead. 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 uses 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 adjusts the Nagle parameters. The SteelHead 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 uses 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 -** Bases the 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>	Specifies the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0 to 4094. Specify 0 to mark the link untagged.
description <description>	Specifies a description to facilitate network administration.

auto-kickoff enable	Enables kickoff, which resets established connections to force them to go through the connection creation process again. 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 6.5 provides two ways to enable kickoff: globally and per in-path rule.
auto-kickoff enable (cont)	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. **Note:** 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.
auto-kickoff disable	Disables kickoff. By default, auto kickoff per in-path rule is disabled.
rulenum <rule-number>	Specifies 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	Enables an in-path rule.
rule-enable false	Disables an in-path rule.

Usage

Defining a fixed-target rule uses a specified remote SteelHead as an optimization peer.

You must specify at least one remote target SteelHead to optimize (and, optionally, which ports and backup SteelHeads), and add rules to specify the network of servers, ports, port labels, and out-of-path SteelHeads to use.

The SteelHead 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 SteelHeads 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 <rule-number>
```

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: the Microsoft end-point mapper port: 135; the SteelHead port for Exchange traffic: 7830; the SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"domain-label," "in-path rule edit fixed-target," "show in-path," "show in-path rules"

in-path rule edit fixed-target packet-mode-uni

Edits a fixed-target packet-mode optimization rule.

Syntax

in-path rule edit rulenum <rule-number> fixed-target packet-mode-uni target-addr{<ip-address> [target-port <port>] [protocol <protocol>] [backup-address <ip-address>] [backup-port <port>] [srcaddr {<ip-address> | all-ip |all-ipv4 | all-ipv6}] [srcport <port>] [dstaddr {<ip-address> | all-ip |all-ipv4 | all-ipv6}] [dstport <port>] [optimization <policy>] [vlan <vlan-tag-id>] [description <description>]

Parameters

rulenum <rule-number>	Specifies the rule number to edit: **1-N** or **start** or **end**.
target-address <ip-address>	Specifies 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.
target-port <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
protocol	Specifies a protocol to optimize: ▪ **tcp** - Specifies TCP protocol for TCPv4 and TCPv6 connections. ▪ **udp** - Specifies the UDP protocol for UDPv4 and UDPv6 connections. ▪ **any** - Optimizes all traffic.
backup-address <ip-address>	Specifies 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.
backup-port <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
srcport <port>	Specifies the source port. Packet-mode optimization is unidirectional, and this port is used on the SteelHead 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 <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
optimization <policy>	Specifies an optimization policy: ▪ **normal** - Performs LZ compression and SDR. This is the default optimization policy. ▪ **sdr-only** - Turns off LZ compression. ▪ **sdr-m** - Performs data reduction entirely in memory, which prevents the SteelHead 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** - Turns off SDR but perform LZ compression. ▪ **none** - Turns off LZ compression and SDR.
vlan <vlan-tag-id>	Specifies the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0 to 4094. Specify 0 to mark the link untagged.
description <description>	Specifies a description to facilitate network administration.

Usage

Use this 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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

Adds a fixed-target packet-mode optimization rule.

Syntax

[no] in-path rule fixed-target packet-mode-uni target-addr {<ip-address>} [target-port <port>] [protocol <protocol>] [backup-addr {<ip-address>} [backup-port <port>]] [srcaddr {<ip-address>| all-ip | all-ipv4 | all-ipv6>}] [scrport <port>] [dstaddr {<ip-address>| 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 <rule-number>]

Parameters

target-addr <ip-address>	Specifies 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.
target-port <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
protocol <protocol>	Specifies a protocol to optimize: ▪ **tcp** - TCP for TCPv4 and TCPv6 connections. ▪ **udp** - UDP for UDPv4 and UDPv6 connections. ▪ **any** - Optimizes all traffic.
backup-addr<ip-address>	Specifies 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.
backup-port <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
srcport <port>	Specifies the source port. Packet-mode optimization is unidirectional, and this port is used on the SteelHead 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 <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
optimization <policy>	Specifies an optimization policy: ▪ **normal** - Performs LZ compression and SDR. This is the default optimization policy. ▪ **sdr-only** - Turns off LZ compression. ▪ **sdr-m** - Performs data reduction entirely in memory, which prevents the SteelHead 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** - Turns off SDR but perform LZ compression. ▪ **none** - Turns off LZ compression and SDR.
vlan <vlan-tag-id>	Specifies the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0 to 4094. Specify 0 to mark the link untagged.

description <description>	Specifies a description to facilitate network administration.
rule-enable true	Enables a fixed-target packet-mode optimization rule.
rule-enable false	Disables a fixed-target packet-mode optimization rule.
rulenum <rule-number>	Specifies the rule number to edit: **1-N** or **start** or **end**.

Usage

Packet-mode optimization skips the autodiscovery process and uses a specified remote SteelHead 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, and, optionally, which ports and backup SteelHeads 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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

Edits a pass-through in-path rule.

Syntax

[no] in-path rule edit rulenum <rule-number> pass-through [srcaddr {<ip-address>| all-ip | all-ipv4 | all-ipv6}] [srcport <port>] [dstaddr {<ip-address>| all-ip |all-ipv4 | all-ipv6}] [dstport <port>] [dst-domain <domain-label>] [dst-host <host-label>] [protocol <protocol>] [vlan <vlan-tag-id>] [web-proxy <mode>] [description <description>] [rule-enable {true | false}] [email-notify {yes | no}]

Parameters

rulenum <rule-number>	Specifies the rule number to edit: **1-N** or **start** or **end**.
srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.

srcport <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
dst-domain <domain-label>	Specifies a destination domain label for this rule. You configure the domain label settings using the **domain-label** command. When you add a domain label to an existing in-path rule that is using **all-ip**, you must change the destination address to **all-ipv4**. Domain labels are only compatible with IPv4. Domain labels and cloud acceleration are mutually exclusive. To use cloud acceleration with domain labels, place the domain label rules lower than cloud acceleration rules in your rule list so the cloud rules match before the domain label rules. We recommend positioning domain label rules as the last in the list, so RiOS matches all previous rules before matching the domain label rule. We recommend using host labels as the destination IP address for a rule configured with domain labels. The host label limits the connections for the extra processing needed for the domain label check. If you rely on the default rule in the in-path rule set for optimization and would like to incorporate domain-label optimization, see the *SteelHead Deployment Guide* for best practices. Enter an empty string, represented by two quotation marks (""), to remove a domain label.
dst-host <host-label>	Specifies a destination host label for this rule. You configure the host label settings using the **host-label** command. A destination IP address and host label cannot be specified in the same rule. A host label can be used instead of a destination IP address. Enter an empty string, represented by two quotation marks (""), to remove a host label.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies a single port (number), a port label, or **all** to specify all ports. If you are using domain labels, specifying **all** defaults to ports 80 and 443 for optimization.
protocol <protocol>	Specifies the protocol traffic to pass through: ▪ **tcp** - Passes through TCPv4 and TCPv6 traffic. ▪ **udp** - Passes through UDPv4 and UDPv6 traffic. ▪ **any** - Passes through all TCP and UDP traffic.
vlan <vlan-tag-id>	Specifies the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0 to 4094. Specify **0** to mark the link untagged.

web-proxy <mode>	Specifies the web proxy optimization mode for this rule: ▪ **auto** - Automatically directs all Internet-bound traffic destined to a public IP address on ports 80 and 443 through the web proxy. This is the default setting. An in-path cloud acceleration rule (**cloud_accel <mode>** option) for SaaS takes priority over a web proxy auto mode rule when they are configured together. Only IPv4 traffic is supported. ▪ **force** - Forwards any IP address and port matching this rule to the web proxy service. This is a pass-through rule. No address in an SCA server list is web-proxied unless the **web-proxy force** mode is configured. ▪ **none** - Does not direct traffic matching this rule through the web proxy service. Web proxy enables a client-side appliance with an autodiscovery or pass-through rule to use a single-ended web proxy to transparently intercept all traffic bound to the Internet. Enabling the web proxy improves performance by providing optimization services such as web object caching and SSL decryption to enable content caching and logging services. You can use host labels and domain labels to define more granular traffic with the web proxy service.
description <description>	Specifies a description to facilitate communication about network administration.
rule-enable true	Enables a pass-through in-path rule.
rule-enable false	Disables a pass-through in-path rule.
email-notify {yes | no}	Specifies whether an email reminder is needed for a pass-through rule. Choose one of the following: ▪ **yes -** Sends email reminders every 15 days (the default) or at a frequency you specify (by using the **email notify passthrough rule notify-timer** command). ▪ **no** - Does not send email reminders. The email reminders are sent to the addresses shown in the event email recipients field of the **show email** command.

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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“domain-label,” “email notify passthrough rule enable,” “in-path rule pass-through,” “show email,” “show in-path,” “show in-path rules”

in-path rule move

Moves an in-path rule in the rule list to the specified position.

Syntax

in-path rule move rulenum <rule-number> to <rule-number>

Parameters

<rule-number>	Rule number or **start** or **end**.

Example

```
amnesiac (config) # in-path rule move rulenum 25 to 10
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path rules"

in-path rule pass-through

Adds a pass-through in-path rule.

Syntax

[no] in-path rule pass-through [srcaddr {<ip-address>| all-ip |all-ipv4 | all-ipv6>}] [srcport <port>] [dstaddr {<ip-address>| all-ip |all-ipv4 | all-ipv6>}] [dstport <port>] [dst-domain <domain-label>] [dst-host <host-label>] [protocol <protocol>] [vlan <vlan-tag-id>] [cloud-accel <mode>] [web-proxy <mode>] [description <description>] [rule-enable {true | false}] [rulenum <rule-number>] [email-notify {yes | no}]

Parameters

srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
srcport <port>	Specifies a single port (number), a port label, or **all** to specify all ports.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies a single port (number), a port label, or **all** to specify all ports.

dst-domain <domain-label>	Specifies a destination domain label for this rule. You configure the domain label settings using the **domain-label** command. When you add a domain label to an existing in-path rule that is using **all-ip**, you must change the destination address to **all-ipv4**. Domain labels are only compatible with IPv4. Domain labels and cloud acceleration are mutually exclusive. To use cloud acceleration with domain labels, place the domain label rules lower than cloud acceleration rules in your rule list so the cloud rules match before the domain label rules. We recommend positioning domain label rules as the last in the list, so RiOS matches all previous rules before matching the domain label rule. We recommend using host labels as the destination IP address for a rule configured with domain labels. The host label limits the connections for the extra processing needed for the domain label check. If you rely on the default rule in the in-path rule set for optimization and would like to incorporate domain-label optimization, see the *SteelHead Deployment Guide* for best practices. Enter an empty string, represented by two quotation marks (""), to remove a domain label.
dst-host <host-label>	Specifies a destination host label for this rule. You configure the host label settings using the **host-label** command. A destination IP address and host label cannot be specified in the same rule. A host label can be used instead of a destination IP address. Enter an empty string, represented by two quotation marks (""), to remove a host label.
protocol <protocol>	Specifies the protocol traffic to pass through: ▪ **tcp** - Passes through TCPv4 and TCPv6 traffic. ▪ **udp** -Passes through UDPv4 and UDPv6 traffic. ▪ **any** - Passes through all TCP and UDP traffic.
vlan <vlan-tag-id>	Specifies the VLAN tag ID (if any). The VLAN identification number is a value with a range from 0 to 4094. Specify **0** to mark the link untagged.
cloud-accel <mode>	Specifies a cloud-acceleration 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 SteelHead SaaS. 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 SteelHead SaaS, but it follows the rule's other parameters so that the connection might be optimized by this SteelHead with other SteelHeads in the network, or it might be passed through.

web-proxy <mode>	Specifies the web proxy optimization mode for this rule: ▪ **auto** - Automatically directs all Internet-bound traffic destined to a public IP address on ports 80 and 443 through the web proxy. This is the default setting. An in-path cloud acceleration rule (**cloud_accel <mode>** option) for SaaS takes priority over a web proxy auto mode rule when they are configured together. Only IPv4 addressing is supported. ▪ **force** - Forwards any IP address and port matching this rule to the web proxy service. This is a pass-through rule. No address in an SCA server list is web-proxied unless the **web-proxy force** mode is configured. ▪ **none** - Does not direct traffic matching this rule through the web proxy service. Web proxy enables a client-side appliance with an autodiscovery or pass-through rule to use a single-ended web proxy to transparently intercept all traffic bound to the Internet. Enabling the web proxy improves performance by providing optimization services such as web object caching and SSL decryption to enable content caching and logging services. You can use host labels and domain labels to define more granular traffic with the web proxy service.
description <description>	Specifies a description to facilitate communication about network administration.
rule-enable true	Enables the rule.
rule-enable false	Disables the rule.
rulenum <rule-number>	Specifies 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.
email-notify {yes | no}	Specifies whether an email reminder is needed for a pass-through rule. Choose one of the following: ▪ **yes -** Sends email reminders every 15 days (the default) or at a frequency you specify (by using the **email notify passthrough rule notify-timer** command). ▪ **no** - Does not send email reminders. The email reminders are sent to the addresses shown in the event email recipients field of the **show email** command.

Usage

The SteelHead 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 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 is in bypass mode. (Pass through of traffic might occur because of in-path rules or because the connection was established before the SteelHead was put in place or before the SteelHead service was enabled.)

Web proxy is a client-side feature and is controlled and managed from a SteelCentral Controller for SteelHead (SCC). You can configure the in-path rule on the client-side SteelHead running the web proxy or on the SCC. You must also enable the web proxy globally on the SCC, add domains to the global HTTPs whitelist, and create any exceptions to the whitelist. For details, see the *SteelCentral Controller for SteelHead User Guide*.

The **no** command option disables the rule. The **no** command option has the following syntax:

no in-path rule <rule-number>

Example

```
amnesiac (config) # in-path rule pass-through srcaddr 10.10.10.1 rulenum 25
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"domain-label," "email notify passthrough rule enable," "in-path rule edit pass-through," "show in-path," "show in-path rules"

ip in-path-gateway

Configures the default gateway for the in-path interface.

Syntax

[no] ip in-path-gateway <interface> <destination-address>

Parameters

<interface>	Interface name; for example, **in-path0_0** or **in-path1_1.**
<destination-address>	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, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path"

ip in-path route

Adds a static in-path route.

Syntax

[no] ip in-path route <interface> <network-prefix> <network-mask> <next-hop-ip-address>

Parameters

<interface>	Interface name: **aux**, **lan0_0**, **wan0_0**, **primary**, **in-path0_0**
<network-prefix>	Network prefix.
<network-mask>	Netmask.
<next-hop-IP-address>	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, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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 User Guide*.

in-path interface mgmt-interface enable

Enables a management in-path (MIP) interface.

Syntax

[no] in-path interface <interface> mgmt-interface enable

Parameters

<interface>	MIP interface. For example, inpath0_0.

Usage

In a typical in-path deployment, optimized and pass-through traffic flows through the SteelHead 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.

RiOS 6.1 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 SteelHeads 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 User 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 and is enabled by default in RiOS 6.0 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"in-path interface mgmt-interface ip," "in-path interface mgmt-interface vlan," "show in-path mgmt-interface"

in-path interface mgmt-interface ip

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-address>**

Parameters

<interface>	MIP interface; for example, inpath0_0.
<ip-address>	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.

For details, see the Management Console online help or the *SteelHead User 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"in-path interface vlan," "in-path interface mgmt-interface vlan," "show in-path mgmt-interface"

in-path interface mgmt-interface ipv6

Specifies the static IPv6 address and network mask for the management in-path (MIP) interface.

Syntax

[no] in-path interface <interface> mgmt-interface ip <ipv6-address> <ipv6-mask-length>

Parameters

<interface>	MIP interface; for example, inpath0_0.
<ipv6-address>	IPv6 address for the MIP interface. Use the format X:X:X::X/XXX.
<ipv6-mask-length>	IPv6 network mask length.

Usage

The MIP interface must reside in its own subnet and cannot share the same subnet with any other interfaces on the SteelHead.

For details, see the Management Console online help or the *SteelHead User Guide*.

The **no** command option disables in-path support.

Example

```
amnesiac (config) # in-path interface inpath0_0 mgmt-interface ipv6 2001:38dc:52::e9a4:c5:6282
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"in-path interface vlan," "in-path interface mgmt-interface vlan," "show in-path mgmt-interface"

in-path interface mgmt-interface vlan

Specifies the VLAN ID for the management in-path (MIP) interface.

Syntax

[no] in-path interface <interface> mgmt-interface vlan <vlan>

Parameters

<interface>	MIP interface; for example, inpath0_0.
<vlan>	VLAN tag ID. When you specify the VLAN tag ID for the MIP interface, all packets originating from the SteelHead are tagged with that identification number. Specify the VLAN tag that the appliance uses to communicate with other SteelHeads 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 User 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"in-path interface mgmt-interface ip,", "show in-path mgmt-interface," "in-path interface vlan"

WAN visibility (transparency) commands

For details about WAN visibility and configuring WAN transparency, see the *SteelHead Deployment Guide*.

---

in-path mac-match-vlan

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 SteelHeads)

For details, see the *SteelHead Deployment Guide*.

The **no** command option disables the use of VLAN IDs in simplified routing table look-ups.

Example

```
amnesiac (config) # in-path mac-match-vlan
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path probe-caching," "in-path rule auto-discover," "show in-path peering oobtransparency"

---

in-path multi-path maintain

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 use the in-path interface that on which it first saw an incoming probe. For details about VLAN transparency, see the *SteelHead Deployment Guide*.

Example

```
amnesiac (config) # in-path multi-path maintain
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path probe-caching," "in-path rule auto-discover," "show in-path peering oobtransparency"

in-path peering oobtransparency mode

Enables out-of-band (OOB) connection destination transparency. The OOB connection is a single, unique TCP connection that is established by a pair of SteelHeads that are optimizing traffic. The pair of SteelHeads 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 352 and the *SteelHead Deployment Guide*.

Syntax

[no] in-path peering oobtransparency mode {none | destination | full [port <port>]}

Parameters

none	Specifies correct addressing. The OOB connection is established between the two SteelHeads, without any TCP/IP header manipulation. This is the default setting.
destination	Specifies 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 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 SteelHeads.
full	Specifies 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, 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 SteelHeads.
port <port>	Changes the predetermined port in **full** mode (C-SHfixed). The default value is 708.

Usage

With RiOS 5.0.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 (where the connection is initiated). By default, the OOB connection uses correct addressing. Correct addressing uses the client-side SteelHead IP address, port number, and VLAN ID, and the server-side SteelHead IP address, port number, and VLAN ID.

If you are using OOB connection correct addressing and the client-side SteelHead cannot establish the OOB connection to the server-side SteelHead, 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 uses the server IP address and port number as the remote IP address and port number. SteelHeads 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.

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 SteelHeads reestablish the connection using the server IP address and port number from the next optimized connection.

OOB connection destination transparency uses the client-side SteelHead IP address and an ephemeral port number chosen by the client-side SteelHead, plus the server IP address and port number in the TCP/IP packet headers in both directions across the WAN

SteelHeads use the server IP address and port number from the first optimized connection.

Use OOB connection destination transparency if the client-side SteelHead cannot establish the OOB connection to the server-side SteelHead.

For details about configuring in-path IP addresses and OOB connections for WAN visibility, see the *SteelHead Deployment Guide*.

Example

```
amnesiac (config) # in-path peering oobtransparency mode none
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path probe-caching,” “in-path rule auto-discover,” “show in-path peering oobtransparency”

---

in-path probe-caching enable

Enable probe caching for WAN visibility. By default, probe caching is disabled in RiOS 5.5 and later.

Syntax

[no] in-path probe-caching enable

Parameters

None

Usage

With probe caching, the client-side SteelHead caches the autodiscovery probe response from the server-side SteelHead when trying to reach a specific server. On subsequent attempts to reach the same server, the SteelHead uses the already cached probe response. On those attempts, the client-side SteelHead sets up a session directly to the peer SteelHead within the 7800 inner channel, bypassing the autodiscovery process since it was successful with the previous attempt. By default, probes are cached for 10 seconds.

With probe caching enabled, SteelHeads still perform autodiscovery. 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 autodiscovery, instead of just some of the new TCP sessions.

Use the **show in-path probe-caching** command to determine if probe caching is enabled on the SteelHead**.**

When the server-side SteelHead is on a VLAN trunk and simplified routing is enabled, Riverbed recommends disabling probe caching on all the remote SteelHeads. 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 in-path VLAN. If the server is on a different VLAN than the SteelHead, the request will not have the correct VLAN ID and there is no easy way to determine it. With probe caching disabled, the SteelHead 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 SteelHeads.

If you have multiple SteelHeads 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. Disabling this mechanism ensures the routers have a chance to redirect every SYN packet to the correct SteelHead, preventing connection forwarding from occurring.

To avoid incorrect forwarded connections, disable probe caching on the client-side SteelHead which instructs the client-side SteelHead to not cache the probe response.

For details, see the *SteelHead Deployment Guide*.

The **no** command option disables probe caching.

Example

```
amnesiac (config) # in-path probe-caching enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path probe-caching,” “in-path rule auto-discover,” “show in-path peering oobtransparency”

---

in-path probe-ftp-data

Probes FTP data connections to learn VLAN information. Enables full address transparency for WAN visibility. For details, see the *SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path probe-ftp-data,” “in-path rule auto-discover,” “show in-path peering oobtransparency”

---

in-path probe-mapi-data

Probes MAPI connections.

Syntax

[no] in-path probe-mapi-data

Parameters

None

Usage

This command enables full address transparency for WAN visibility. It ensures that all MAPI connections are forced through the in-path rule table. For details, see the *SteelHead Deployment Guide*.

The **no** command option disables this command.

Example

The following example shows how to configure 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"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

Enables VLAN connection-based mapping for WAN visibility. For details, see the *SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"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

out-of-path enable

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 User Guide*.

The **no** command option disables out-of-path configuration.

Example

```
amnesiac (config) # out-of-path enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show out-of-path”

Connection pooling commands

service connection pooling

Enables a pool of connections to a peer SteelHead.

Syntax

[no] service connection pooling <max-pool-size>

Parameters

<max-pool-size>	Maximum size of the connection pool.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service connection pooling”

Failover support and out-of-band failure detection commands

failover connection

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 attempts to reconnect to the master SteelHead after a read time-out has expired. The default value is 5 attempts.
failed <timeout>	Sets the connection failed timeout setting.
timeout <timeout>	Sets the number of milliseconds the SteelHead waits before aborting the reconnection attempt to the master SteelHead. 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 periodically sends keep-alive messages to the master SteelHead on TCP port 7820. If the master SteelHead does not respond to the keep-alive message within five seconds, the backup SteelHead drops the connection and attempts to reconnect to the master SteelHead. The backup SteelHead 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 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 starts optimizing connections.

Use the **failover connection** command to adjust the number of times the backup SteelHead attempts to reconnect to the master SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“failover read timeout,” “show failover”

failover enable

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 SteelHeads: one as a master and the other as a backup. The master SteelHead in the pair (usually the SteelHead closest to the LAN) is active and the backup SteelHead is passive. The master SteelHead 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 does not intercept traffic while the master appliance is active. It pings the master SteelHead to make sure that it is alive and processing data. If the master SteelHead fails, the backup takes over and starts processing all of the connections. When the master SteelHead comes back up, it sends a message to the backup that it has recovered. The backup SteelHead 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 SteelHeads and add a fixed-target rule to the client-side SteelHead to define the master and backup target appliances. When both the master and backup SteelHeads are functioning properly, the connections traverse the master appliance. If the master SteelHead fails, subsequent connections traverse the backup SteelHead.

The master SteelHead uses an out-of-band (OOB) connection. The OOB connection is a single, unique TCP connection that communicates internal information. If the master SteelHead becomes unavailable, it loses this OOB connection and the OOB connection times out in approximately 40 to 45 seconds. Once the OOB connection times out, the client-side SteelHead declares the master SteelHead unavailable and connects to the backup SteelHead.

During the 40- to 45-second delay before the client-side SteelHead declares a peer unavailable, it passes through any incoming new connections; they are not black-holed.

While the client-side SteelHead is using the backup SteelHead for optimization, it attempts to connect to the master SteelHead every 30 seconds. If the connection succeeds, the client-side SteelHead reconnects to the master SteelHead for any new connections. Existing connections remain on the backup SteelHead 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 and the backup.

If both the master and backup SteelHeads become unreachable, the client-side SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show failover”

---

failover master

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show failover"

failover port

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>	Port number. The default value is 7820.

Usage

The **no** command option resets the port to the default value.

Example

```
amnesiac (config) # failover port 2515
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show failover"

failover read timeout

Specifies the failover read settings.

Syntax

[no] failover read timeout <timeout>

Parameters

<timeout>	Failover read time-out value, in milliseconds. The default value is 5000.

Usage

You can adjust the timers for faster master and backup failover for SteelHeads. In a steady, normal operating state, the backup SteelHead periodically sends keep-alive messages to the master SteelHead on TCP port 7820. If the master SteelHead does not respond to the keep-alive message within five seconds, the backup SteelHead drops the connection and attempts to reconnect to the master SteelHead. The backup SteelHead 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 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 starts optimizing connections.

Use this command to adjust the amount of time, in milliseconds, that the backup SteelHead waits for the master SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show failover”

failover steelhead addr

Sets the IP address for a failover SteelHead. A failover SteelHead is a backup appliance. If the master fails, the failover appliance takes over.

Syntax

[no] failover steelhead addr <ip-address>

Parameters

<ip-address>	IP address for the failover, backup machine. The default value is 0.0.0.0.
	For IPv4 addresses, use this format: XXX.XXX.XXX.XXX/XX
	For IPv6 addresses, use this format: X:X:X::X/XXX
	If you have installed multiple bypass cards, you must specify the IP address for the inpath0_0 slot.

Usage

The **no** command option resets the failover IP address to the default value.

Important: You can enter either IPv4 or IPv6 addresses. However, if you have enabled IPv6 connection forwarding, you must enter an IPv6 address. For more information about enabling IPv6 connection forwarding, see the *SteelHead User Guide* or the *SteelHead Interceptor User Guide*.

Example

```
amnesiac (config) # failover steelhead addr 10.10.10.1
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Interceptor

Related Commands

“show failover”

failover steelhead port

Sets the port for a failover SteelHead. A failover SteelHead is a backup appliance. If the master fails, the failover appliance takes over.

Syntax

[no] failover steelhead port <port>

Parameters

<port>	Port number for the failover SteelHead. The default value is 7820.

Usage

You cannot specify this command for the SteelHead Interceptor.

The **no** command option resets the port to the default value.

Example

```
amnesiac (config) # failover steelhead port 2515
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show failover"

protocol connection lan on-oob-timeout

Configures out-of-band (OOB) LAN timeout settings.

Syntax

[no] protocol connection lan on-oob-timeout {drop all | drop same-inpath enable}

Parameters

drop all	Configures OOB connection shutdown on loss of connection.
drop same-inpath enable	Configures an 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) and the inner channel (the WAN-side TCP connection between the SteelHeads). 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 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol connection”

protocol connection wan keep-alive oob def-count

Specifies the out-of-band (OOB) WAN keep-alive message count.

Syntax

[no] protocol connection wan keep-alive oob def-count <count>

Parameters

<count>	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 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. If you want faster peer failure detection, use this 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol connection wan keep-alive oob def-intvl,” “show protocol connection”

protocol connection wan keep-alive oob def-intvl

Specifies the out-of-band (OOB) WAN keep-alive message interval.

Syntax

[no] protocol connection wan keep-alive oob def-intvl <seconds>

Parameters

<seconds>	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 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 this 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol connection wan keep-alive oob def-count," "show protocol connection"

Packet-mode optimization commands

packet-mode enable

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 and the server-side SteelHead. 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 Deployment Guide* and the *SteelHead User Guide*.

Example

```
amnesiac (config) # packet-mode enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"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 Deployment Guide*.

in-path peering auto

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 automatically finds the furthest SteelHead in a network and optimization occurs there. For example, in a deployment with four SteelHeads (A, B, C, D), where D represents the appliance that is furthest from A, the SteelHead 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 uses regular auto-discovery. With regular auto-discovery, the SteelHead finds the first remote SteelHead along the connection path of the TCP connection and optimization occurs there. For example, if you had a deployment with four SteelHeads (A, B, C, D) where D represents the appliance that is furthest from A, the SteelHead 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 Deployment Guide*.

RiOS 5.5.x or later supports a large number of peers (up to 32,768) per SteelHead. This feature is available only on SteelHead 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 User Guide*.

Preventing an Unknown (or Unwanted) SteelHead from Peering

Automatic peering (enhanced auto-discovery) greatly reduces the complexities and time it takes to deploy SteelHeads. 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 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 receives an auto-discovery probe from the unknown SteelHead. To prevent an unknown SteelHead from peering you must add a pass-through peering rule that passes through traffic from the unknown SteelHead in the remote location. For details, see the Management Console online help and the *SteelHead Deployment Guide*.

The **no** command option disables enhanced auto-discovery.

Example

```
amnesiac (config) # in-path peering auto
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path peering rules”

in-path peering disc-outer-acpt

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path peering disc-outer-acpt”

in-path peering edit-rule

Modifies an in-path peering rule description.

Syntax

in-path peering edit-rule rulenum <rule-number> description "<description>"

Parameters

rulenum <rule-number>	Specifies the rule number.
description "<description>"	Specifies a description to help you identify the rule. Enclose the text in quotation marks (“).

Example

```
amnesiac (config) # in-path peering edit-rule rulenum 5 description “this is an example”
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path peering disc-outer-acpt”

in-path peering move-rule

Moves the rule to the specified position in the rule list.

Syntax

[no] in-path peering move-rule <rule-number> to <rule-number>

Parameters

<rule-number>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path peering auto"

---

in-path peering rule

Configures in-path peering rules.

Syntax

[no] in-path peering rule {auto | pass | accept} [peer <peer-ip-address>] [ssl-capability {cap | in-cap | no-check}] [src {<ip-address> | all-ip | all-ipv4 | all-ipv6>}] [dest {<ip-address> | all-ip | all-ipv4 | all-ipv6>} [dest-port <port>] [rulenum <rule-number>] [description <description>]

Parameters

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 {all-ipv4 | all-ipv6 | all-ip}	Specifies the in-path IP address of the probing SteelHead. If more than one in-path interface is present on the probing SteelHead, apply multiple peering rules, one for each in-path interface. The peer client-side SteelHead appliance IP address accepts IPv4 and IPv6 addresses.
ssl-capability	Specifies 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 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, and if there is no temporary or short-lived error condition, the SSL-capable check is a success. The SteelHead 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 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 performs both auto-discovery and SSL optimization. ▪ **in-cap (incapable)** - If the destination IP address and port are not an SSL server that is properly configured and enabled on the server-side SteelHead, or if there is a temporary or short-lived error condition, the SSL-capable check fails. The SteelHead 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. ▪ **no-check** - The peering rule does not determine whether the server SteelHead 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 performs auto-discovery and does not optimize SSL. This rule always appears last in the list and you cannot remove it.
src <ip-address>	Specifies 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.
src all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
src all-ipv4	Specifies all IPv4 addresses.
src all-ipv6	Specifies all IPv6 addresses.
dest <ip-address>	Specifies 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.
dest all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dest all-ipv4	Specifies all IPv4 addresses.

dest all-ipv6	Specifies all IPv6 addresses.
dest-port <port>	Specifies the destination port for this rule. You can specify a port label or **all** for all ports.
rulenum <rule-number>	Specifies 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 takes on the connection.
description <description>	Specifies a description to facilitate communication about network administration.

Usage

You can provide increased optimization by deploying two or more SteelHeads 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 is reached, that appliance stops intercepting new connections. This allows the next SteelHead 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 in a cluster not to intercept connections between themselves.

You configure peering rules that define what to do when a SteelHead receives an auto-discovery probe from another SteelHead.

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 that require all connections from a client to be optimized by one SteelHead, 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 SteelHead Interceptor to build multi-appliance clusters. For details, see the *SteelHead Interceptor Deployment Guide* and the *SteelHead Interceptor User Guide*.

Notes:

- When you combine two SteelHeads that have a bandwidth limit of 20 Mbps each, the serial cluster still has a limit of 20 Mbps.
- If the active SteelHead 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 from Peering

To prevent an unknown SteelHead from peering you must add a pass-through peering rule that passes through traffic from the unknown SteelHead in the remote location. For details, see the Management Console online help and the *SteelHead Deployment Guide*.

Example

This example shows how to configure a cluster with these 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 with in-path peering rules to prevent peering with another SteelHead in the cluster, and with in-path rules to not optimize connections originating from other SteelHeads 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) # write memory
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) # write memory
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) # write memory
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 *                  *                 *     --             --
```

IPv6 Peering Rule

```
amnesiac (config) # in-path peering rule auto dest-port 443 peer all-ipv6 ssl cap description
“default rule to auto-discover and attempt to optimize connections destined to port 443”
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path peering rules”

in-path peering-gre enable

Enables generic routing encapsulation (GRE) auto discovery for IPv4 tunneled traffic.

Syntax

[no] in-path peering-gre enable

Parameters

None

Usage

Enter this command on all SteelHeads to enable GRE tunnel optimization support. This feature optimizes GRE traffic by extracting and optimizing the data behind the GRE header between the two WAN links. The default route for the client-side and server-side SteelHead should be directed to the WAN side of the network. Before the introduction of this feature, GRE traffic was relayed and not optimized.

GRE optimization supports hub-and-spoke and spoke-to-spoke topologies. A maximum of 100 tunnels are supported on a hub-and-spoke topology or with a spoke-to-spoke topology.

See the *SteelHead User Guide* for more information.

Example

```
amnesiac (config) # in-path peering-gre enable
```

Related Commands

“show in-path peering-gre”

in-path probe direct

Sets probing with the SteelHead 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. 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 Deployment Guide*.

The **no** command option disables the probe.

Example

```
amnesiac (config) # in-path probe direct
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path peering rules"

in-path probe version

Sets probing with the in-path probe version settings.

Syntax

[no] in-path probe version <version>

Parameters

<version>	Specifies the in-path probe version setting: **1** or **2**

Usage

The **no** command option disables the version.

Example

```
amnesiac (config) # in-path probe version 1
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path probe-caching"

peer

Configures the connection protocol version.

Syntax

[no] peer <ip-address> version [min <version> | max <version>]

Parameters

<ip-address>	In-path or out-of-path IP address (or both) of the SteelHead.
min <version>	Specifies the minimum protocol version number: **5** or **8**.
max <version>	Specifies the maximum protocol version number: **5** or **8**.

Usage

Use this command only to harmonize connection protocol versions in deployments with a mix of v1.2 and v2.x appliances.

For each v1.2 SteelHead peer, enter the following commands:

```
sh> peer <ip-address> version min 5
sh> peer <ip-address> version max 5
```

After all the v1.2 SteelHeads in the network have been upgraded to v2.x SteelHeads, remove the version settings:

```
sh> no peer <ip-address> version min
sh> no peer <ip-address> version max
```

If you are unable to discover all v1.2 SteelHeads in the network, configure all v2.1 SteelHeads 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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

Sets the LAN receive buffer size for high-speed TCP (HS-TCP).

Syntax

[no] protocol connection lan receive buf-size <bytes>

Parameters

<bytes>	LAN receive buffer size in bytes. 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol connection”

protocol connection lan send buf-size

Sets the LAN send buffer size for HS-TCP.

Syntax

[no] protocol connection lan send buf-size <bytes>

Parameters

<bytes>	LAN send buffer size in bytes. 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol connection”

protocol connection wan receive def-buf-size

Sets the WAN receive buffer size for HS-TCP.

Syntax

[**no**] **protocol connection wan receive def-buf-size <bytes>**

Parameters

<bytes>	WAN receive buffer size in bytes. 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 receive def-buf-size 3875000
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol connection”

protocol connection wan send def-buf-size

Sets the WAN send buffer size for HS-TCP.

Syntax

[no] protocol connection wan send def-buf-size <bytes>

Parameters

<bytes>	WAN send buffer size in bytes. 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol connection”

single-ended rule optimized scps-discover

Adds a single-ended optimization rule for SCPS discovery.

Syntax

single-ended rule optimized scps-discover [srcaddr {ip-address> | all-ip | all-ipv4 | all-ipv6}] [dstaddr {<ip-address> | all-ip | all-ipv4 | all-ipv6}] [dstport <port>] [allow-tcp-proxy {enable | disable}] [vlan <vlan>] [web-proxy <mode>] [cong-ctrl-algo <method>] [rate-pacing {enable | disable}] [rulenum <rule-number>]

Parameters

srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.

dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies 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: – SteelFusion – Interactive – RBT-Proto – Secure For details on port labels, see "port-label" on page 534.
allow-tcp-proxy enable	Allows only SCPS peering. This is the default.
allow-tcp-proxy disable	Allows SCPS and non-SCPS peering.
vlan <vlan>	Specifies a VLAN identification number from **1** to **4094**, **-1,** or **0**. **-1** specifies that the rule applies to all VLANs; **0** specifies that the rule applies to untagged connections.
web-proxy <mode>	Specifies the web proxy optimization mode for this rule: ▪ **disable** - Use this rule if the connection is not web proxied. ▪ **enable** - Use this rule if the connection is web proxied. ▪ **ignore** - Use this rule if it is unimportant whether or not the connection is web proxied. Web proxy enables a client-side appliance with an autodiscovery or pass-through rule to use a single-ended web proxy to transparently intercept all traffic bound to the Internet. Enabling the web proxy improves performance by providing optimization services such as web object caching and SSL decryption to enable content caching and logging services.
cong-ctrl-algo <method>	Specifies 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 method is not available without an SCPS license. ▪ **err-tol-tcp** - SkipWare error-tolerant TCP optimization. This method is not available without an SCPS license.
rate-pacing enable	Enables 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. Enabling rate pacing evenly spreads the transmission of a window of packets across the entire duration of the round-trip time.

rate-pacing disable	Disables 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 <rule-number>	Specifies a rule number from **1** to **N**, **start**, or **end**. The SteelHeads 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 and a third-party device running TCP-PEP (Performance Enhancing Proxy). Both the SteelHead 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 an SCPS license to use this command or to configure rate pacing on a per-rule basis. The SteelHead 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 SteelHeads 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 User Guide* and the *SteelHead Deployment Guide*.

Example

```
amnesiac (config) # single-ended rule optimized scps-discover srcaddr all-ipv4 dstaddr all-ipv4
dstport secure rulenum 2
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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

Edits a single-ended optimization rule for SCPS discovery.

Syntax

single-ended rule edit rulenum <rule-number> optimized scps-discover [srcaddr {<ip-address> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<ip-address> | all-ip |all-ipv4 | all-ipv6}] [dstport <port>] [allow-tcp-proxy {enable | disable}] [vlan <vlan>] [web-proxy <mode>] [cong-ctrl-algo <method>] [rate-pacing {enable | disable}]

Parameters

rulenum <rule-number>	Specifies a rule number to edit.
srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies 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: – SteelFusion – Interactive – RBT-Proto – Secure For more information on port labels, see “port-label” on page 534.
allow-tcp-proxy enable	Allows only SCPS peering. This is the default.
allow-tcp-proxy disable	Allows SCPS and non-SCPS peering.
vlan <vlan>	Specifies a VLAN identification number from **1** to **4094**, **-1,** or **0**. **-1** specifies that the rule applies to all VLANs; **0** specifies that the rule applies to untagged connections.
web-proxy <mode>	Specifies the web proxy optimization mode for this rule: ▪ **disable** - Use this rule if the connection is not web-proxied. ▪ **enable** - Use this rule if the connection is web-proxied. ▪ **ignore** - Use this rule if it is unimportant whether or not the connection is web proxied. Web proxy enables a client-side appliance with an autodiscovery or pass-through in-path rule to use a single-ended web proxy to transparently intercept all traffic bound to the Internet. Enabling the web proxy improves performance by providing optimization services such as web object caching and SSL decryption to enable content caching and logging services.

cong-ctrl-algo <method>	Specifies 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 method is not available without a SCPS license. ▪ **err-tol-tcp** - SkipWare error-tolerant TCP optimization. This method is not available without an SCPS license.
rate-pacing enable	Enables 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. Enabling rate pacing evenly spreads the transmission of a window of packets across the entire duration of the round-trip time.
rate-pacing disable	Disables 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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

Changes the order of the existing SEI SCPS rules.

Syntax

[no] single-ended rule move <rule-number> to <rule-number>

Parameters

rulenum <rule-number>	Specifies a rule number from **1** to N, **start**, or **end**. SteelHeads 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"single-ended rule optimized scps-discover," "single-ended rule optimized tcp-proxy," "show connection," "show single-ended rules"

single-ended rule optimized tcp-proxy

Adds a single-ended optimization rule for TCP proxy.

Syntax

single-ended rule optimized tcp-proxy [srcaddr {<ip-address> | all-ip | all-ipv4 | all-ipv6}] [dstaddr {<ip-address> | all-ip | all-ipv4 | all-ipv6}] [dstport <port(s)>] [vlan <vlan>] [web-proxy <mode>] [cong-ctrl-algo <method>] [rate-pacing {enable | disable}] [rulenum <rule-number>]

Parameters

srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port(s)>	Specifies 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: – SteelFusion – Interactive – RBT-Proto – Secure For more information on port labels, see "port-label" on page 534.
vlan <vlan>	Specifies a VLAN identification number from **1** to **4094**, **-1**, or **0**. **-1** specifies that the rule applies to all VLANs; **0** specifies that the rule applies to untagged connections.

web-proxy <mode>	Specifies the web proxy optimization mode for this rule: ▪ **disable** - Use this rule if the connection is not web proxied. ▪ **enable** - Use this rule if the connection is web proxied. ▪ **ignore** - Use this rule if it is unimportant whether or not the connection is web proxied. Web proxy enables a client-side appliance with an auto-discovery or pass-through in-path rule to use a single-ended web proxy to transparently intercept all traffic bound to the Internet. Enabling the web proxy improves performance by providing optimization services such as web object caching and SSL decryption to enable content caching and logging services.
cong-ctrl-algo <method>	Specifies 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 method is not available without a SCPS license. ▪ **err-tol-tcp** - SkipWare error-tolerant TCP optimization. This method is not available without a SCPS license.
rate-pacing enable	Enables 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. Enabling rate pacing evenly spreads the transmission of a window of packets across the entire duration of the round-trip time.
rate-pacing disable	Disables rate pacing on a per-rule basis. Rate pacing is disabled by default.
rulenum <rule-number>	Specifies a rule number from **1** to **N**, **start**, or **end**. The SteelHeads 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 SteelHeads 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 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"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

Edits a single-ended optimization rule for TCP proxy.

Syntax

single-ended rule edit rulenum <rule-number> optimized tcp-proxy [srcaddr {<ip-address> | all-ip |all-ipv4 | all-ipv6}] [dstaddr {<ip-address> | all-ip |all-ipv4 | all-ipv6}] [dstport <port>] [vlan <vlan>] [web-proxy <mode>] [cong-ctrl-algo <method>] [rate-pacing {enable | disable}]

Parameters

rulenum <rule-number>	Specifies a rule number to edit.
srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port(s)>	Specifies 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: – SteelFusion – Interactive – RBT-Proto – Secure For more information on port labels, see "port-label" on page 534.
vlan <vlan>	Specifies a VLAN identification number from **1** to **4094**, **-1,** or **0**. **-1** specifies that the rule applies to all VLANs; **0** specifies that the rule applies to untagged connections.

web-proxy <mode>	Specifies the web proxy optimization mode for this rule: ▪ **disable** - Use this rule if the connection is not web proxied. ▪ **enable** - Use this rule if the connection is web proxied. ▪ **ignore** - Use this rule if it is unimportant whether or not the connection is web proxied. Web proxy enables a client-side appliance with an auto-discovery or pass-through in-path rule to use a single-ended web proxy to transparently intercept all traffic bound to the Internet. Enabling the web proxy improves performance by providing optimization services such as web object caching and SSL decryption to enable content caching and logging services.
cong-ctrl-algo <method>	Specifies 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 method is not available without a SCPS license. ▪ **err-tol-tcp** - SkipWare error-tolerant TCP optimization. This method is not available without a SCPS license.
rate-pacing enable	Enables 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. Enabling rate pacing evenly spreads the transmission of a window of packets across the entire duration of the round-trip time.
rate-pacing disable	Disables rate pacing on a per-rule basis. Rate pacing is disabled by default.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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

Adds a single-ended pass-through rule.

Syntax

single-ended rule pass-through [**srcaddr** {**<ip-address>** | **all-ip** | **all-ipv4** | **all-ipv6**}] [**dstaddr** {**<ip-address>** | **all-ip** | **all-ipv4** | **all-ipv6**}] [**dstport <port>**] [**vlan <vlan>**] [**rulenum <rule-number>**]

Parameters

srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port(s)>	Specifies 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: – SteelFusion – Interactive – RBT-Proto – Secure For more information on port labels, see “port-label” on page 534.
vlan <vlan>	Specifies a VLAN identification number from **1** to **4094**, **-1,** or **0**. **-1** specifies that the rule applies to all VLANs; **0** specifies that the rule applies to untagged connections.
rulenum <rule-number>	Specifies a rule number from **1** to **N**, **start**, or **end**. The SteelHeads 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 unoptimized.

Use the **no single-ended rule <rule>** to remove a rule.

For details about satellite optimization, see the *SteelHead User Guide* and the *SteelHead Deployment Guide*.

Example

```
amnesiac (config) # single-ended rule pass-through vlan 555
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“single-ended rule edit pass-through,” “show connection,” “show connections,” “show single-ended rules”

single-ended rule edit pass-through

Edits a single-ended pass-through rule.

Syntax

single-ended rule edit rulenum <rule-number> pass-through [srcaddr {<ip-address> | all-ip | all-ipv4 | all-ipv6}] [dstaddr {<ip-address> | all-ip | all-ipv4 | all-ipv6}] [dstport <port(s)>] [vlan <vlan>]

Parameters

rulenum <rule-number>	Specifies the rule number to edit.
srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
dstaddr <ip-address>	Specifies 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.
dstaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dstaddr all-ipv4	Specifies all IPv4 addresses.
dstaddr all-ipv6	Specifies all IPv6 addresses.
dstport <port>	Specifies 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: – SteelFusion – Interactive – RBT-Proto – Secure
vlan <vlan>	Specifies a VLAN identification number from **1** to **4094**, **-1,** or **0**. **-1** specifies that the rule applies to all VLANs; **0** specifies 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. For details on port labels, see “port-label” on page 534.

Example

```
amnesiac (config) # single-ended rule edit rulenum 2 pass-through srcaddr all-ipv6 dstaddr all-ipv6
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“single-ended rule pass-through,” “show connection,” “show connections,” “show single-ended rules”

tcp cong-ctrl mode

Enables TCP congestion control settings.

Syntax

tcp cong-ctrl mode {auto | default | hstcp | bw-est | per-conn-tcp | err-tol-tcp}

Parameters

auto	Specifies 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 7.0. For single-ended interception connections, this mode uses SkipWare when possible, or standard TCP otherwise.
default	Specifies 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 Deployment Guide*. This option clears any advanced bandwidth congestion control that was previously set.
hstcp	Specifies 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. We recommend that you enable high-speed TCP optimization only after you have carefully evaluated whether it benefits your network environment.
bw-est	Specifies 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	Specifies 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	Specifies SkipWare error-tolerant TCP optimization. Enables SkipWare optimization with the error rate detection and recovery mechanism on the SteelHead. 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 CX, SteelHead EX, SteelHead-c, SteelHead-v, SteelHead-c

Related Commands

“show tcp cong-ctrl”

---

tcp highspeed enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show tcp highspeed”

tcp max-time-out

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>	Maximum time-out value for TCP connections in seconds.

Example

```
amnesiac (config) # tcp max-time-out 60
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show tcp max-time-out”

tcp max-time-out mode enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show tcp max-time-out”

tcp rate-pacing enable

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 SteelHeads or on the link rate for a SteelHead 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 User Guide* and the *SteelHead Deployment Guide*.

Example

```
amnesiac (config) # tcp rate-pacing enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcp sat-opt scps rule,” “show tcp rate-pacing status”

tcp reordering threshold

Enables the TCP reordering threshold. Riverbed recommends you contact Riverbed Support before you configure this setting.

Syntax

[no] tcp reordering threshold <value>

Parameters

<value>	TCP reordering threshold.

Example

```
amnesiac (config) # tcp reordering threshold
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show tcp reordering"

tcp sat-opt bw-est mode

Specifies the TCP bandwidth estimation mode.

Syntax

[no] tcp sat-opt bw-est mode <mode>

Parameters

<mode>	Choose 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 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 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 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. 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 SteelHeads 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 7.0 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show tcp sat-opt settings”

tcp sat-opt scps legacy-comp enable

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** command option disables SkipWare legacy compression settings.

Example

```
amnesiac (config) # tcp sat-opt scps legacy-comp enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show tcp sat-opt settings”

tcp sat-opt scps legacy-comp process-batch

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>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show tcp sat-opt scps legacy-comp”

tcp sat-opt scps legacy-comp queuing-delay

Sets an upper boundary on packets queued for module processing.

Syntax

[no] tcp sat-opt scps legacy-comp queuing-delay <ms>

Parameters

<ms>	Queuing delay value, in milliseconds.

Usage

The **no** command option resets the maximum queuing delay to the default value.

Example

```
amnesiac (config) # tcp sat-opt scps legacy-comp queuing-delay 1000
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show tcp sat-opt scps legacy-comp”

tcp sat-opt scps rule

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 <method>] [rate-pacing {enable | disable}] [rulenum <rule-number>]

Parameters

srcaddr <network>	Specifies an IPv4 address and mask for the traffic source. Use the format XXX.XXX.XXX.XXX/XX.
dstaddr <network>	Specifies an IPv4 address and mask for the traffic destination. Use the format XXX.XXX.XXX.XXX/XX.
dstport <port>	Specifies 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: – SteelFusion – Interactive – RBT-Proto – Secure For details on port labels, see “port-label” on page 534.

allow-scps	Specifies an SCPS mode for this rule. ▪ **enable** - Enables a rule to optimize single-ended interception SCPS connections. ▪ **disable** - Disables a rule to optimize single-ended interception SCPS connections. If you choose this option, single-ended interception SCPS connections pass through the SteelHead unoptimized.
scps-peer-only	Specifies an SCPS peering rule. ▪ **enable** - Allows SCPS peering for single-ended interception SCPS connections. ▪ **disable** - Allows both SCPS and non-SCPS peering (for example, proxy fallback) for single-ended interception connections.
vlan <tag-id>	Specifies a VLAN tag ID for this rule. ▪ 1 to 4094 ▪ 0 (for untagged) ▪ -1 (for all)
cong-ctrl-algo <method>	Specifies 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	Specifies whether to enable or disable rate pacing. ▪ **enable** - Enables rate pacing. ▪ **disable** - Disables 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 <rule-number>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcp cong-ctrl mode,” “tcp sat-opt scps scps-table enable,” “show tcp sat-opt scps rules”

tcp sat-opt scps rule edit

Edits Space Communications Protocol Standards (SCPS) rules for satellite optimization.

Syntax

[no] tcp sat-opt scps rule edit rulenum <rule-number> [srcaddr <network>] [dstaddr <network>] [dstport <port>] [allow-scps {enable | disable}] [scps-peer-only {enable | disable}] [vlan <tag -id>] [cong-ctrl-algo <method>] [rate-pacing {enable | disable}]

Parameters

rule <rule-number>	Specifies the number in the SCPS rule table to edit.
srcaddr <network>	Specifies an IPv4 address and mask for the traffic source. Use the format XXX.XXX.XXX.XXX/XX.
dstaddr <network>	Specifies an IPv4 address and mask for the traffic destination. Use the format XXX.XXX.XXX.XXX/XX.
dstport <port>	Specifies 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: – SteelFusion – Interactive – RBT-Proto – Secure For details on port labels, see “port-label” on page 534.
allow-scps	Specifies an SCPS mode for this rule. ▪ **enable** - Enables 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 unoptimized.
scps-peer-only {enable | disable}	Specifies an SCPS peering rule. ▪ **enable** - Allows 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>	Specifies a VLAN tag ID for this rule. ▪ 1 to 4094 ▪ 0 (for untagged) ▪ -1 (for all)

cong-ctrl-algo <method>	Specifies 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	Specifies whether to enable or disable rate pacing. ▪ **enable** - Enables rate pacing. ▪ **disable** - Disables 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.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcp cong-ctrl mode,” “tcp sat-opt scps scps-table enable,” “show tcp sat-opt scps rules”

tcp sat-opt scps rule move

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>	Rule number.

Usage

SCPS optimization requires a valid SCPS license.

Example

```
amnesiac (config) # tcp sat-opt scps rule move 4 to 3
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show tcp sat-opt scps rules”

tcp sat-opt scps scps-table enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show tcp sat-opt settings”

Data store configuration commands

This section describes the commands for configuring the following data store features:

- Warming branch SteelHead Mobiles
- Encrypting the data store
- Configuring data store notification and wraparound
- Synchronizing the data store

datastore branchwarming enable

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 product family user is in a SteelHead-enabled branch office and trickles the new data back to the SteelHead Mobile product family laptop. When the user goes back on the road, they receive warm performance.

Branch warming cooperates with and optimizes transfers for a server-side SteelHead. New data transfers between the client and server are populated in the SteelHead Mobile product family data store, the branch SteelHead data store, and the server-side SteelHead data store.

When the server downloads data, the server-side SteelHead checks if either the SteelHead Mobile or the branch SteelHead has the data in their data store. If either device already has the data segments, the server-side SteelHead sends only references to the data. The SteelHead Mobile and the branch SteelHead 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 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 after logging in through a VPN network and peers with a different server-side SteelHead after logging in from the branch office, branch warming does not improve performance.

The **no** command option disables branch warming.

Example

```
amnesiac (config) # datastore branchwarming enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore branchwarming”

datastore encryption type

Enables or disables encryption of the data store and specifies the type of encryption to use.

Syntax

[no] datastore encryption type {NONE | AES_128 | AES_192 | AES_256}

Parameters

NONE	Does not encrypt the data store. Encryption types can be lower-case.
AES_128	Uses the Advanced Encryption Standard (AES) 128-bit cipher setting.
AES_192	Uses the AES 192-bit cipher setting.
AES_256	Uses the AES 256-bit cipher setting. This encryption scheme is the most secure.

Usage

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. The secure data is difficult for a third party to retrieve. Before you encrypt the data store, the secure vault must be unlocked. For details, see “secure-vault” on page 693.

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 the SteelHead 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 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 693.

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 (4.x.x). For example, an encrypted data store created in 4.1.4 would work with 4.1.2, but not with 4.0.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 User Guide*.

Example

```
amnesiac (config) # datastore encryption type AES_192
amnesiac (config) # restart clean
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore”

datastore notification enable

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 wraparound.

Example

```
amnesiac (config) # datastore notification enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore”

datastore notification wrap-around

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>	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 wraparound.

Example

```
amnesiac (config) # datastore notification wrap-around 2
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore”

datastore safety-valve threshold

Configures the data store safety-valve threshold settings.

Syntax

[no] datastore safety-valve threshold {<milliseconds> | default}

Parameters

<milliseconds>	Disk response threshold time in milliseconds.
default	Specifies the default threshold time.

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“datastore safety-valve timeout,” “show datastore safety-valve”

datastore safety-valve timeout

Configures the data store safety-valve timeout settings.

Syntax

[no] datastore safety-valve timeout {<seconds> | default}

Parameters

<seconds>	Timeout value in seconds.
default	Specifies the default timeout value.

Usage

The **no** command option disables the data store safety-valve timeout settings.

Example

```
amnesiac (config) # datastore safety-valve timeout 600
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“datastore safety-valve threshold,” “show datastore safety-valve”

show datastore safety-valve

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“datastore safety-valve threshold,” “datastore safety-valve timeout”

---

datastore sync enable

Enables pairs of SteelHeads 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 4.0, 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 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.

You configure two SteelHeads 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. 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 Deployment Guide*.

If one of the synchronized SteelHeads is under high load, some data might not be copied. For detailed information, see the *SteelHead Deployment Guide*.

If data store synchronization is interrupted for any reason (such as a network interruption or if one of the SteelHeads is taken out of service), the SteelHeads 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore”

datastore sync master

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore”

datastore sync peer-ip

Sets the IP address for the peer appliance for which you want to push replicated data.

Syntax

datastore sync peer-ip <ip-address>

Parameters

<ip-address>	Primary or the auxiliary interface IP address of a backup appliance.

Example

```
amnesiac (config) # datastore sync peer-ip 10.0.0.3
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore”

datastore sync port

Sets the port for the peer SteelHead for which you want to push replicated data.

Syntax

[no] datastore sync port <port>

Parameters

<port>	Port of the peer SteelHead. 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore”

datastore sync reconnect

Sets the reconnection interval for data store synchronization.

Syntax

[no] datastore sync reconnect <seconds>

Parameters

<seconds>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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 413.

For details, see the Management Console online help or the *SteelHead User Guide* or the *SteelHead Deployment Guide*.

Important: Riverbed recommends you contact Riverbed Support before you change these default configuration settings.

datastore codec compression adaptive

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore disk”

datastore codec compression level

Configures the data store LZ compression level.

Syntax

[no] datastore codec compression level <lz-level>

Parameters

<lz-level>	LZ compression level. The range is **0-9**.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # datastore codec compression level 3
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore disk”

datastore codec multi-core-bal

Enables data store multicore balancing.

Syntax

[no] datastore codec multi-core-bal

Parameters

None

Usage

This command enables multicore balancing, which ensures better distribution of workload across all CPUs, thereby maximizing throughput by keeping all CPUs busy. Core balancing is useful when handling a small number of high-throughput connections (approximately 25 or less) such as replication traffic. By default, this command is disabled and should be enabled only after careful consideration consulting with Sales Engineering and Support.

The **no** command option disables this feature.

Example

```
amnesiac (config) # datastore codec multi-core-bal
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore disk”

datastore disklayout fifo

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 SteelHeads, occasionally Riverbed Support recommends changing the policy to improve performance.

The client-side and server-side SteelHeads 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore disklayout”

datastore disklayout rvbdlru

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 SteelHeads, occasionally Riverbed Support recommends changing the policy to improve performance.

The client-side and server-side SteelHeads must be running RiOS v6.0.x or later.

The **no** command option disables the replacement algorithm.

Example

```
amnesiac (config) # datastore disklayout rvbdlru
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore disklayout”

datastore sdr-policy

Configures the data store SDR policy.

Syntax

[no] datastore sdr-policy [default | sdr-a | sdr-m | sdr-a-advanced]

Parameters

default	Specifies 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, and CPU load to provide more throughput. **Note:** 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 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 models; for example, 6020 - 6020. When used between two different SteelHead models, the smaller model limits the performance. **Note:** You must reboot the client-side and server-side SteelHeads if you enable SDR-M. 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 6.0 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. **Note:** 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 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 SteelHeads must be running RiOS 6.0.x or later.

The **no** command option disables data store SDR policy.

Example

```
amnesiac (config) # datastore sdr-policy sdr-a
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore sdr-policy”

datastore write-q-prior

Enables priority for deferred writes.

Before you enable the set of data replication (DR) 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore write-q-prior”

disk reset

Resets the specified disk.

Syntax

disk <disk-number> reset

Parameters

<disk-number>	Disk number to be reset.

Example

```
amnesiac (config) # disk 2 reset
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show datastore disk”

WCCP support commands

This section describes the Web Cache Communications Protocol (WCCP) support commands.

wccp adjust-mss enable

Enables the Adjust Maximum Segment Size (MSS) feature.

Syntax

[no] wccp adjust-mss enable

Parameters

None

Usage

The default for the SteelHead 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 connections. The result is dropped packets.

This command shrinks the MSS to fit accordingly.

The **no** command disables the Adjust MSS feature.

Example

```
amnesiac (config) # wccp adjust-mss enable
```

Product

SteelHead CX, SteelHead EX, Interceptor, SteelHead-v, SteelHead-c

Related Commands

"show wccp"

wccp enable

Enables WCCP support.

Syntax

[no] wccp enable

Parameters

None

Usage

For details about configuring WCCP, see the *SteelHead User Guide* and the *SteelHead 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 must join a service group at the router. A service group is a group of routers and SteelHeads which define the traffic to redirect, and the routers and SteelHeads the traffic goes through. You might use one or more service groups to redirect traffic to the SteelHeads for optimization.

RiOS 6.1 and later provides additional WCCP configuration, allowing each individual SteelHead 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 CX, SteelHead EX, Interceptor, SteelHead-v, SteelHead-c

Related Commands

"show wccp"

wccp interface service-group

Defines a new WCCP service group.

Syntax

wccp interface <interface> service-group service group <service-id> {routers <routers> | protocol <protocol> | flags <flags> | priority <priority> | ports <ports> | password <password> | weight <weight> | encap-scheme <scheme> | assign-scheme <scheme> | src-ip-mask <mask> | dst-ip-mask <mask> | src-port-mask <mask> | dst-port-mask <mask>}

Parameters

<interface>	SteelHead interface to participate in a WCCP service group. RiOS 6.1 allows multiple SteelHead interfaces to participate in WCCP on one or more routers for redundancy (RiOS 6.0 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 in-path interface can participate in the same service group. For WCCP configuration examples, see the *SteelHead Deployment Guide*. If multiple SteelHeads are used in the topology, they must be configured as neighbors.
<service-id>	Number from 0 to 255 to identify the service group on the router. A value of 0 specifies the standard HTTP service group. We recommend that you use WCCP service groups 61 and 62. The service group ID is local to the site where WCCP is used. The service group number is not sent across the WAN. Enables WCCP v2 support on all groups added to the Service Group list.
routers <routers>	Specifies a comma-separated list of IP addresses for routers. You can specify up to 32 routers.
protocol <protocol>	Specifies one of the following traffic protocols: **tcp**, **udp**, or **icmp**. The default value is tcp.
flags <flags>	Specifies a comma-separated list of the following service group 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>	Specifies 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. The priority value must be consistent across all SteelHeads within a particular service group.
ports <ports>	Specifies a comma-separated list of up to seven ports that the router will redirect. Set this parameter only if the **flags** parameter specifies either **ports-dest** or **ports-source**.
password <password>	Assigns a password to the SteelHead. 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 eight characters.
weight <weight>	Specifies a weight value in the range of 0 to 65535. You specify the percentage of connections that are redirected to a particular SteelHead interface, which is useful for traffic load balancing and failover support. The number of TCP, UDP, or ICMP connections a SteelHead supports determines its weight. The more connections a SteelHead model supports, the heavier the weight of that model. In RiOS 6.1 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 SteelHeads 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 with two WCCP in-path interfaces to receive twice the proportion of traffic, for SteelHeads with multiple in-paths connected, each of the in-path weights is divided by the number of that SteelHead interfaces participating in the service group. For example, if there are two SteelHeads 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 default value corresponds to the number of TCP connections your SteelHead supports.

weight <weight> (cont)	**Failover Support** To enable single in-path failover support with WCCP groups, define the service group weight to be 0 on the backup SteelHead. If one SteelHead has a weight 0, but another one has a non-zero weight, the SteelHead with weight 0 does not receive any redirected traffic. If all the SteelHeads 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 6.1 is to use the same weight on all interfaces from a given SteelHead 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 SteelHeads. 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 Deployment Guide*.
encap-scheme	Specifies one of the following methods for transmitting packets between a router or a switch and a SteelHead interface: ▪ **either** - Uses 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.

assign-scheme	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. We recommend 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 ▪ **mask** - Redirects traffic operations to the SteelHeads, 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 5.0.1 and earlier is limited to one SteelHead per service group. The SteelHead with the lowest in-path IP address receives all the traffic. This scheme provides high availability. You can have multiple SteelHeads in a service group but only the SteelHead with the lowest in-path IP address receives all the traffic. If the SteelHead with the lowest in-path IP address fails, the SteelHead with the next lowest in-path IP address receives all of the traffic. When the SteelHead with the lowest in-path IP address recovers, it again receives all of the traffic. Mask assignment in RiOS 5.0.2 and later supports load-balancing across multiple active SteelHeads. This scheme bases load-balancing decisions (for example, which SteelHead 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 6.1 supports load-balancing across multiple active SteelHead 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. **Note:** 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. For detailed information and best practices for using assignment schemes, see the *SteelHead Deployment Guide*.
src-ip-mask <mask>	Specifies the service group source IP mask in hexadecimal format. The default value is 0x1741.
dst-ip-mask <mask>	Specifies the service group destination IP mask in hexadecimal format.
src-port-mask <mask>	Specifies the service group source port mask in hexadecimal format.
dst-port-mask <mask>	Specifies the service group destination port mask in hexadecimal format.

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.
- If one SteelHead has a weight 0, but another one has a nonzero weight, the SteelHead with weight 0 does not receive any redirected traffic.
- To enable failover support with multi-inpath WCCP groups in RiOS 6.1, set the **weight** parameter to **0** on the backup SteelHead interface.

  If one SteelHead interface has a weight 0, but another one has a nonzero 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 CX, SteelHead EX, Interceptor, SteelHead-v, SteelHead-c

Related Commands

“show wccp,” “show wccp interface service-group”

wccp mcast-ttl

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>	Multicast TTL value.

Usage

For details about configuring WCCP, see the *SteelHead Deployment Guide*.

The **no** command option disables WCCP support.

Example

```
amnesiac (config) # wccp mcast-ttl 10
```

Product

SteelHead CX, SteelHead EX, Interceptor, SteelHead-v, SteelHead-c

Related Commands

“show wccp”

wccp override-return route-no-gre

Enables the SteelHead to accept whatever return direction is negotiated, but it returns traffic by using the in-path routing table, and will not use GRE encapsulation.

Syntax

[no] wccp override-return route-no-gre

Parameters
None

Usage
Typically, you use this command where you have an in-path gateway, which means traffic is returned to the in-path gateway. You configure the WCCP service group to specify either. By choosing either, the router and SteelHead 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 (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 and the next hop according to the routing table. For details, see the *SteelHead Deployment Guide*,

The **no** command option disables WCCP override support.

Example
```
amnesiac (config) # wccp override-return route-no-gre
```

Product
SteelHead CX, SteelHead EX, Interceptor, SteelHead-v, SteelHead-c

Related Commands
“show wccp”

---

wccp override-return sticky-no-gre
Enables the redirecting router not to use GRE encapsulation for the return traffic from the SteelHead.

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 CX, SteelHead EX, Interceptor, SteelHead-v, SteelHead-c

Related Commands
“show wccp”

Simplified routing support commands

---

in-path mac-except-locl
Disallows the SteelHead MAC address on the peer SteelHead 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 SteelHeads are 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 is on the same subnet, the SteelHead will not use the MAC address of the peer SteelHead for any simplified routing entry except for the one corresponding to the peer SteelHead IP address.

For details, see the *SteelHead Deployment Guide*.

The **no** command option disables the in-path feature.

Example

```
amnesiac (config) # in-path mac-except-locl
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path macmap-except”

---

in-path mac-match-vlan

Configures VLAN IDs in simplified routing table look-ups.

Syntax

[no] in-path mac-match-vlan

Parameters

None

Usage

When enabled, the SteelHead tracks the VLAN ID and IP address against the MAC address. For details, see the *SteelHead Deployment Guide*.

The **no** command option disables the in-path feature.

This feature is enabled by default.

Example

```
amnesiac (config) # in-path mac-match-vlan
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path mac-match-vlan”

---

in-path peer-probe-cach

Configures VLAN IDs in simplified routing table look-ups.

Syntax

[no] in-path peer-probe-cach

Parameters

None

Usage

In order for the SteelHead 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).

You can turn off probe-caching on the server-side SteelHead or on the client-side SteelHead. The difference between the two methods is one of convenience. If there are 25 client-side SteelHeads and 1 server-side SteelHead, it is easier to instruct the data center SteelHead to inform the remote SteelHeads not to perform probe-caching. The alternative is to disable probe-caching on all 25 SteelHeads in the remote offices. Enter this command on the server-side SteelHead. When enabled, the server-side SteelHead instructs the client-side SteelHead not to cache the probe-response.

For details, see the *SteelHead Deployment Guide*.

The **no** command option disables the in-path feature.

Example

```
amnesiac (config) # in-path peer-probe-cach
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path probe-caching”

---

in-path probe-caching enable

Enables probe caching.

Syntax

[no] in-path probe-caching enable

Parameters

None

Usage

For the SteelHead 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. This command instructs the client-side SteelHead to not cache the probe response.

For details, see the *SteelHead Deployment Guide*.

The **no** command option disables the in-path feature.

Example

```
amnesiac (config) # in-path probe-caching enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path probe-caching”

in-path simplified routing

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-NATed (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	Uses simplified routing entries only 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 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 is in a different subnet from the client and the server.

Without simplified routing, if a SteelHead 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. 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 in your network.
- Simplified routing requires a client-side and server-side SteelHead.

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 more information to associate IP addresses and MAC addresses (and potentially VLAN tags). For details, see “in-path peering auto” on page 404.

When deploying SteelHeads on a nontrunk link, using simplified routing is recommended but optional. However, when deploying SteelHeads 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 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 on a simple non-VLAN trunk:

```
in-path simplified routing all
!enables the new discovery protocol
in-path peering auto
```

```
in-path simplified mac-def-gw-only
in-path mac-except-locl
```

If you are putting the SteelHeads on a VLAN trunk link:

```
in-path simplified routing all
!enables the new discovery protocol
in-path peering auto
!keep LAN side traffic in its original VLAN; enabled by default
in-path vlan-conn-based
in-path simplified mac-def-gw-only
in-path mac-except-locl
!enabled by default
in-path mac-match-vlan
```

For details, see the *SteelHead Deployment Guide*.

The **no** command option disables simplified routing.

Example

```
amnesiac (config) # in-path simplified routing all
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path simplified routing”

---

in-path simplified mac-def-gw-only

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 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path macmap-tables”

Asymmetric route detection commands

in-path asym-route-tab flush

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path asym-route-tab”

in-path asym-route-tab remove

Clears a specified single route from the asymmetric routing table.

Syntax

in-path asym-rout-tab remove <entry>

Parameters

<entry>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path asym-route-tab”

in-path asymmetric routing detection enable

Enables asymmetric route detection.

Syntax

[no] in-path asymmetric routing detection enable

Parameters

None

Usage

Asymmetric route detection automatically detects and reports asymmetric routing conditions and caches this information to avoid losing connectivity between a client and a server.

For details about asymmetric routing, see the *SteelHead User Guide* and the *SteelHead Deployment Guide*.

Types of asymmetry:

Complete Asymmetry - Packets traverse both SteelHeads going from client to server but bypass both SteelHeads 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 SteelHeads going from client to server but bypass the server-side SteelHead 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 SteelHeads going from client to server but bypass the client-side SteelHead 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 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 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 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 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path asym-route-tab"

---

in-path asymmetric routing pass-through enable

Enables the pass-through feature for asymmetric routing.

Syntax

[no] in-path asymmetric routing pass-through enable

Parameters

None

Usage

Use this command to ensure connections are not passed-through the SteelHeads unoptimized. Logging occurs when asymmetric routes are detected. 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.

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. 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path asym-route-tab”

in-path cdp allow-failure enable

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 to notify the router that the SteelHead 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 stops sending CDP packets to all the routers it is attached to and connections are redirected and optimized by another SteelHead.

This can be useful when the routers are configured to redirect to a SteelHead when all routers are up but to another SteelHead when one router goes down.

For details about how to configure a SteelHead for PBR with CDP, see the *SteelHead Deployment Guide*.

The **no** command option disables CDP.

Example

```
amnesiac (config) # in-path cdp allow-failure enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path cdp”

in-path cdp enable

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 to bypass the SteelHead 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 for PBR with CDP, see the *SteelHead Deployment Guide*.

The **no** command option disables CDP.

Example

```
amnesiac (config) # in-path cdp enable
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path cdp”

in-path cdp holdtime

Configures the hold time for Cisco Discovery Protocol (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>	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, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path cdp”

in-path cdp interval

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>	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, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path cdp”

Connection forwarding

This section describes connection forwarding commands, typically used with the SteelHead Interceptor.

Note: To use connection forwarding with IPv6, both SteelHeads must be running RiOS 8.5 or later and you must enable multiple interface support. The control connection between neighbors is still IPv4 only.

steelhead communication ack-timer-cnt

Sets the interval to wait for an acknowledgment (ACK).

Syntax

[no] steelhead communication ack-timer-cnt <integer>

Parameters

<integer>	Number of intervals.

Usage

The **no** command option disables the wait interval for an ACK.

Example

```
amnesiac (config) # steelhead communication ack-timer-cnt 5
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path neighbor," "show steelhead communication"

steelhead communication ack-timer-intvl

Sets the length of time to wait for an acknowledgment (ACK).

Syntax

[no] steelhead communication ack-timer-intvl <milliseconds>

Parameters

<milliseconds>	Duration of the interval in milliseconds.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication ack-timer-intvl 5
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path neighbor"

steelhead communication advertiseresync

Resynchronizes 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 allows neighbor connections from all in-path to all in-paths. When there are multiple neighbor connections from one SteelHead to another, if one goes down the traffic is rerouted through the remaining in-path SteelHead, and traffic continues on normally.

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication advertiseresync
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path neighbor advertiseresync"

steelhead communication allow-failure

Enables the SteelHead 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 loses connectivity to a connection forwarding neighbor, the SteelHead stops attempting to optimize new connections. With the **steelhead communication allow-failure** command enabled the SteelHead continues to optimize new connections, regardless of the state of its neighbors.

For virtual in-path deployments with multiple SteelHeads, 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 cluster changes, can cause routers to change the destination SteelHead for TCP connection packets. When this happens, SteelHeads 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 SteelHeads, 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 SteelHeads on these paths must use connection forwarding to ensure that the traffic for a TCP connection is always sent to the SteelHead that is performing optimization for that connection.

If the allow-failure feature is used in a parallel physical in-path deployment, SteelHeads only optimize those connections that are routed through the paths with operating SteelHeads. TCP connections that are routed across paths without SteelHeads (or with a failed SteelHead) 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 blocks traffic along its path, forcing traffic to be rerouted onto other paths (where the remaining SteelHeads are deployed). For details about configuring the allow-failure with the fail-to-block feature, see the *SteelHead Deployment Guide*.

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication allow-failure
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path neighbor"

steelhead communication enable

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. 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 SteelHeads to communicate with each other. These SteelHeads 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 traveling between them are not optimized.

Important: When you define a neighbor, you specify the SteelHead in-path IP address, not the primary IP address.

If there are more than two possible paths, additional SteelHeads 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 acknowledgment from the furthest neighbor.

When you enable connection forwarding, multiple SteelHeads work together and share information about what connections are optimized by each SteelHead. With connection forwarding, the LAN interface forwards and receives connection forwarding packets.

SteelHeads that are configured to use connection forwarding with each other are known as connection forwarding neighbors. If a SteelHead sees a packet belonging to a connection that is optimized by a different SteelHead, it forwards it to the correct SteelHead. When a neighbor SteelHead reaches its optimization capacity limit, that SteelHead 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 SteelHeads 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. 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 model that supports multiple in-path interfaces, instead of using multiple SteelHeads with single in-path interfaces. In general, serial deployments are preferred over parallel deployments. For details about deployment best practices, see the *SteelHead Deployment Guide*.

The **no** command option disables this feature.

Example

```
amnesiac (config) # steelhead communication enable
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path neighbor”

---

steelhead communication fwd-vlan-mac

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 to include the VLAN and Ethernet header when it forwards packets to a neighbor. This command is useful when you are using connection forwarding and VLAN transparency. For details, see the *SteelHead 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 SteelHeads 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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path neighbor”

steelhead communication heartbeat enable

Configures the SteelHead 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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path neighbor”

steelhead communication keepalive count

Sets the keep-alive messages before terminating connections with the neighbor SteelHead for TCP connection forwarding.

Syntax

[no] steelhead communication keepalive count <count>

Parameters

<count>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path neighbor”

steelhead communication keepalive interval

Sets the time interval between keep-alive messages with the neighbor SteelHead for connection forwarding.

Syntax

[no] steelhead communication keepalive interval <seconds>

Parameters

<seconds>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path neighbor”

steelhead communication mode-ipv6

Enables IPv6 connection forwarding between SteelHeads and SteelHead Interceptors in a cluster.

Syntax

[no] steelhead communication mode-ipv6

Parameters

None

Usage

The **no** option of this command disables IPv6 connection forwarding between SteelHeads and SteelHead Interceptors in a cluster.

Before using this command, these tasks are required:

- Path selection must be disabled. To disable path selection, use the **no path-selection enable** command.
- Multi-interface support must be enabled. To enable multi-interface support, use the **steelhead communication multi-interface enable** command or the **steelhead interceptor communication multi-interface enable** command.
- All SteelHead neighbors must be removed. To remove a neighbor, use the **no** command option with the appropriate CLI command (for example, the **no steelhead name** or **no failover steelhead addr**).
- Remove all appliances from the connection forwarding appliance list and the failover appliance list. To remove an appliance from these lists, use the **no** command option with the appropriate CLI command (for example, **no interceptor name**, **no steelhead interceptor name**, or **no failover steelhead interceptor name**).

Use this command on each SteelHead and each SteelHead Interceptor in the cluster.

You must restart the service for your changes to take effect.

Example

```
amnesiac (config) # steelhead communication mode-ipv6
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“steelhead communication multi-interface enable,” “steelhead interceptor communication multi-interface enable,” “steelhead interceptor communication mode-ipv6,” “steelhead name,” “failover steelhead addr,” “path-selection enable”

steelhead communication multi-interface enable

Enables multiple interface support. Typically, this feature is used with the SteelHead Interceptor.

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

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path neighbor”

steelhead communication port

Sets the neighbor port for the SteelHead in connection forwarding deployments.

Syntax

[no] steelhead communication port <port>

Parameters

<port>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path neighbor”

steelhead communication read-timeout

Sets the response wait time.

Syntax

[no] steelhead communication read-timeout <milliseconds>

Parameters

<milliseconds>	Time to wait in milliseconds.

Usage

The **no** command option disables the response wait time.

Example

```
amnesiac (config) # steelhead communication read-timeout 10
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path neighbor”

steelhead communication recon-timeout

Sets the reconnect response wait time.

Syntax

[no] steelhead communication recon-timeout <milliseconds>

Parameters

<milliseconds>	Time to wait in milliseconds.

Usage

The **no** command option disables reconnect response wait time.

Example

```
amnesiac (config) # steelhead communication recon-timeout 40
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path neighbor”

steelhead name

Configures connection forwarding neighbors.

Syntax

[no] steelhead name <name> {main-ip <ip-address> [port <port>] | additional-ip <ip-address>}

Parameters

<name>	Hostname of the neighbor appliance.
main-ip <ip-address>	Specifies the main connection forwarding IPv4 address or IPv6 address of the neighbor. ▪ For IPv4 addresses, use this format: XXX.XXX.XXX.XXX/XX ▪ For IPv6 addresses, use this format: X:X:X::X/XXX
port <port>	Specifies the connection forwarding port of the neighbor.
additional-ip <ip-address>	Specifies an additional connection forwarding IP address for the neighbors.

Usage

For details about configuring connection forwarding, see the *SteelHead Deployment Guide*.

The **no** command option disables the neighbor.

Example

The following example shows a connection forwarding neighbor configured with an IPv4 address:

```
amnesiac (config) # steelhead name test main-ip 10.0.0.1 port 1234
```

The following example show a connection forwarding neighbor configured with an IPv6 address:

```
amnesiac (config) # steelhead name test main-ip 2600:809:200:47 f:20e:b6ff:fe90:209
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show in-path neighbor," "steelhead communication mode-ipv6"

in-path send-storeid enable

Creates a table of data store IDs; typically used with the SteelHead Interceptor.

Syntax

[no] in-path send-storeid enable

Parameters

None

Usage

Each time the SteelHead Interceptor receives a connection it forwards it to the appropriate SteelHead.

The **no** command disables the table of data store IDs.

Example

```
amnesiac (config) # in-path send-storeid enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"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 User Guide*.

subnet side add rule

Adds a rule to the subnet map table.

Syntax

subnet side add rule index {<rule-number> start | end} network <network-prefix> is {lan | wan}

Parameters

index {<rule-number> start | end}>	Specifies a rule number, **start**, or **end**. SteelHeads 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 takes on the connection.
network <network-prefix>	Specifies the source subnet IP address and subnet mask. ▪ For IPv4 addresses, use this format: XXX.XXX.XXX.XXX/<0-32> ▪ For IPv6 addresses, use this format: X:X:X::X/<0-128>
is {lan | wan}	Specifies whether the addresses on the subnet are on the LAN side or WAN side. In virtual in-path configurations, all traffic is flowing in and out of one physical interface.

Usage

Subnet-side rules are used in a virtual in-path deployment to support Flow Export, to support a client-side SteelHead, or to exempt certain subnets from QoS enforcement or path selection. Subnet-side rules let you configure subnets as LAN-side subnets or WAN-side subnets for a virtual in-path SteelHead. The subnet-side rules determine whether traffic originated from the LAN or the WAN-side of the SteelHead based on the source subnet. You must configure subnets on each SteelHead in a virtual in-path configuration, as the subnets for each will likely be unique.

For details on subnet-side rules, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # subnet side add rule index 4 network 10.2.2.2 is lan
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show subnet side rules”

subnet side delete rule

Deletes a subnet-side rule.

Syntax

subnet side delete rule <rule-number>

Parameters

<rule-number>	Rule number to delete.

Example

```
amnesiac (config) # subnet side delete rule 4
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show subnet side rules”

subnet side move rule

Moves a subnet-side rule.

Syntax

subnet side move rule from <rule-number> to <rule-number>

Parameters

<rule-number>	Rule number to move.

Usage

The subnet-side rules determine whether traffic originated from the LAN or the WAN side of the SteelHead based on the source subnet.

Example

```
amnesiac (config) # subnet side move rule from 4 to 3
```

Product

Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show subnet side rules”

Data flow analyzer support commands

This section describes the data flow analyzer support commands.

ip flow-export destination

Configures data flow support. Data flow support enables you to collect traffic flow data.

Syntax

[no] ip flow-export destination {<ip-address> | <hostname>} <collector-port> {export-port {aux | primary} | filter ip <ip-address> {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

<ip-address>	Specifies the export IP address the data flow collector is listening on.
<hostname>	Specifies the hostname the data flow collector is listening on.
<collector-port>	Specifies the port the data flow collector is listening on. The default value is 2055.
export-port {aux | primary}	Specifies the interface used to send data flow packets to the collector.
filter ip <ip-address>	Specifies the IP address for filter rules. Optionally, you can configure the netmask or port. ▪ For IPv4 addresses, use this format: XXX.XXX.XXX.XXX ▪ For IPv6 addresses, use this format: X:X:X::X
netmask <netmask>	Specifies the IPv4 or IPv6 netmask for filter rules.
port <port>	Specifies the port for filter rules.
filter-enable	Enables filters on the specified collector.
template refresh-rate <packets>	Specifies the number of packets sent after which templates are resent. Applicable only to collector v9.
template-timeout-rate <minutes>	Specifies the duration after which templates are resent. Applicable only to collector v9.
version <version>	Specifies the data flow collector version: ▪ **CascadeFlow** - Specifies Cascade 8.4 or later. ▪ **Cascade-comp** - Specifies Cascade 8.34 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 the SteelCentral. These versions allow automatic discovery and interface grouping for SteelHeads in the SteelCentral NetProfiler or SteelCentral Flow Gateway and support WAN and optimization reports in SteelCentral. For details, see the *SteelCentral NetProfiler and NetExpress User's Guide* and the *SteelCentral Flow Gateway User Guide*.
interface <interface>	Specifies the interface used to capture packets. The data flow collector records sent from the SteelHead appear to be sent from the IP address of the selected interface.

capture {all | optimized | passthrough}	Specifies the type of traffic to capture: ▪ **all** - Exports both optimized and nonoptimized traffic. ▪ **optimized** - Exports optimized traffic. ▪ **passthrough** - Exports pass through traffic.
lan-addrs {off | on}	Specifies 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: **off** displays the SteelHead 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 SteelHeads. **Note:** This option is not applicable to collector v9.

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 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 and the listening port of the collector.
- Ensure that you can reach the collector from the SteelHead (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 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 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ip”

ip flow-export enable

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 preoptimization and postoptimization 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.

SteelHeads 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 Deployment Guide*.

Flow export requires the following components:

- **Exporter** - When you enable flow export support, the SteelHead exports data about flows through the network.
- **Collector** - A server or appliance designed to aggregate data sent to it by the SteelHead.
- **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 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 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ip”

ip flow-export ipv6 enable

Enables NetFlow/SteelFlow collectors to collect IPv6 network statistics of individual flows that traverse your network.

Syntax

[no] ip flow-export ipv6 enable

Parameters

None

Usage

Run this command to enable flow statistic collectors such as NetFlow/SteelFlow, to collect from IPv6 addresses of SteelHead, SteelCentral Controller for SteelHead, and Interceptor. In many deployments, this feature enables you to continuously monitor the performance and behavior of pure IPv6 environments in profilers such as the SteelCentral NetProfiler.

IPv6 network statistics can be collected only from:

- NetFlow 9
- SteelFlow 9.1/CascadeFlow

You must have flow export enabled before you run this command. IPv6 traffic statistics collection can be enabled by running the CLI command or from the Flow Statistics page in the Management Console.

By default, this command is disabled. The **no** command option disables IPv6 statistics collection if it has been enabled. Once IPv6 statistics collection is disabled, the NetFlow/SteelFlow collectors revert to collecting traffic statistics only from IPv4 addresses.

For details, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # ip flow-export ipv6 enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelCentral Controller

Related Commands

“ip flow-export enable”

---

ip flow-export qos-dpi enable

Enables the SteelHead to export QoS and application statistics about individual flows to a CascadeFlow Collector.

Syntax

[no] ip flow-export qos-dpi enable

Parameters

None

Usage

SteelCentral provides 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 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 SteelCentral NetProfiler.

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 User Guide* and the *SteelCentral Product Suite Deployment Guide*.

Example

```
amnesiac (config) # ip flow-export qos-dpi enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“papi rest access_code generate,” “papi rest access_code import,” “show ip”

ip flow-setting active_to

Sets the length of time the collector retains a list of active flows.

Syntax

[no] ip flow-setting active_to <seconds>

Parameters

<seconds>	Length of life, in seconds, 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ip”

ip flow-setting inactive_to

Sets length of time the collector retains a list of inactive flows.

Syntax

[no] ip flow-setting inactive_to <seconds>

Parameters

<seconds>	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 CX, SteelHead EX, SteelHead-c

Related Commands

“show ip”

ip flow-setting max-pkt-size

Sets the maximum packet size.

Syntax

[no] ip flow-setting max-pkt-size <rate>

Parameters

<rate>	Maximum packet rate. The value must be between 1500 and 40000.

Usage

The **no** command option disables the packet size.

Example

```
amnesiac (config) # ip flow-setting max-pkt-size 2000
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ip”

Top Talkers commands

stats settings top-talkers enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show stats top-talkers”

stats settings top-talkers interval

Enables Top Talkers collection period.

Syntax

stats settings top-talkers interval <hours>

Parameters

<hours>	Interval in hours: 24 or 48 hours.

Usage

This command specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show stats top-talkers”

Application commands

This section describes the application commands that are used with path selection and QoS.

application

Defines an application and configures application settings.

Syntax

[no] application <name> [group <"group-name">] [business-crit <level>] [category <name>] [description <description>] [traffic-type <traffic-type>] [transport-prot <protocol>] [dscp <value] [vlan <vlan>] [local-port {<port> | <port-label>}] [remote-port {<port> | <port-label>}] [local-net {<subnet> | <host-label>}] [remote-net {<subnet> | <host-label>}] [app-prot <protocol>]

Parameters

<name>	Specifies the name of the application. Enter ? at the system prompt to view a list of over 1100 predefined available applications. You can also define a custom application.
group <"group-name">	Specifies the application group name: ▪ **Business Bulk** - Captures business-level file transfer applications and protocols, such as CIFS, SCCM, anti-virus updates, and over-the-network backup protocols. ▪ **Business Critical** - Captures business-level, low-latency transactional applications and protocols, such as SQL, SAP, Oracle and other database protocols, DHCP, LDAP, RADIUS, and routing and other network communication protocols. ▪ **Business Productivity** - Captures general business-level productivity applications and protocols, such as email, messaging, streaming, and broadcast audio/video, collaboration, Intranet HTTP traffic, and business cloud services O365, Google apps, SFDC, and others through a whitelist. ▪ **Business Standard** - Captures all intra-network traffic going within local subnets as defined by the uplinks on the SteelHead. Use this class to define the default path for traffic not classified by other application groups. ▪ **Business VDI** - Captures real-time interactive business-level virtual desktop interface (VDI) protocols, such as PC over IP (PCoIP), Citrix CGP and ICA, RDP, VNC, and Telnet protocols. ▪ **Business Video** - Captures business-level video conferencing applications and protocols, such as Microsoft Lync and RTP video. ▪ **Business Voice** - Captures business-level voice over IP (VoIP) applications and protocols (signaling and bearer), such as Microsoft Lync, RTP, H.323, and SIP. ▪ **Recreational** - Captures all Internet-bound traffic that has not already been classified and processed by other application groups. ▪ **Standard Bulk** - Captures general file transfer protocols, such as FTP, torrents, NNTP/usenet, NFS, and online file hosting services Dropbox, Box.net, iCloud, MegaUpload, Rapidshare, and others. ▪ **Custom Applications** - Captures user-defined applications that have not been classified into another application group. Application groups are predefined groupings of applications into the most common path selection usage scenarios. An application signature is associated to only one application group at a time. Application grouping is a powerful mechanism to group traffic profiles.
business-crit <level>	Specifies the business criticality of an application: ▪ **Lowest Criticality** - Lowest-priority service class. ▪ **Low Criticality** - Low-priority service class: for example, FTP, backup, replication, other high-throughput data transfers, and recreational applications such as audio file sharing. ▪ **Medium Criticality** - Medium-priority service class. ▪ **High Criticality** - High-priority service class. ▪ **Highest Criticality** - Highest-priority service class.

category <name>	Specifies the category name. The category groups applications by general functions: for example, mail, file transfer, social media.
description <description>	Specifies the description of the application.
traffic-type <traffic-type>	Specifies the traffic type: **any**, **optimized**, or **passthrough**.
transport-prot <protocol>	Specifies the transport protocol of traffic to match against. The default setting is **all**.
dscp <value>	Specifies the DSCP value of an application. The range is from **0** to **63** or specify **all** to use all DSCP values.
vlan <vlan>	Specifies the VLAN tag for traffic to match: ▪ Specify a numeric VLAN tag identification number from **0** to **4094**. ▪ Specify **all** to specify the rule applies to all VLANs. ▪ Specify **none** to specify the rule applies to untagged connections. RiOS supports VLAN v802.1Q. To configure VLAN tagging, configure transport rules to apply to all VLANs or to a specific VLAN. By default, rules apply to all VLAN values unless you specify a particular VLAN ID. Passthrough traffic maintains any preexisting VLAN tagging between the LAN and WAN interfaces.
local-port {<port> | <port-label>}	Specifies the local port or port label of an application.
remote-port {<port> | <port-label>}	Specifies the remote port or remote port label of an application.
local-net {<subnet> | <host-label>}	Specifies the local subnet or host label of an application. Use the format xxx.xxx.xxx.xxx/xx for subnet and mask.
remote-net {<subnet> | <host-label>}	Specifies the remote subnet or host label of an application. Use the format xxx.xxx.xxx.xxx/xx for subnet and mask.
app-prot <protocol>	Specifies the application layer protocol. The default setting is **any**.

Usage

In earlier RiOS versions, the configuration of an application was tightly coupled with QoS rules. To simplify SteelHead configuration, the definition of an application is a separate task in RiOS v9.0 and later. A separate application definition allows for the configuration of multiple rules, using the same application without having to repeat the application definition for each rule.

Application definitions are used in QoS and path selection rules. You must define the application before using it in a QoS or path selection rule.

Application definitions also enable you to group applications according to their type and business criticality, which provide a powerful way to group traffic profiles and specify policy based on the profile. You must use a single rule with an application group but can use multiple rules for individual applications. Using an application group simplifies configuration and minimizes the number of rules.

The **no** command option removes the specified custom application.

Example

```
amnesiac (config) # application new_app app-prot ASA
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Path selection commands," "QoS commands"

applications clear

Clears all configured applications.

Syntax

applications clear [confirm]

Parameters

confirm	Confirms clearing of all applications.

Usage

Use the **applications reset** command to reset all applications to the factory default if the applications have been cleared by this command.

Example

```
amnesiac (config) # applications clear
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"applications reset"

application rename

Configure a new application.

Syntax

[no] application <name> rename <new-name>

Parameters

<name>	Name of the application. Enter ? at the system prompt to view a list of predefined applications.
<new-name>	New name of the application.

Usage

You can choose a new application and the system automatically propagates it to all resources that use it, such as sites and uplinks.

Example

```
amnesiac (config) # application Facebook-Event rename Facebook-Post
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"application"

applications reset

Resets all the configured applications to the factory default applications.

Syntax

applications reset [confirm]

Parameters

confirm	Confirms resetting all applications to the factory default.

Usage

You can use this command to reset the applications to the factory default if any of the applications have been changed or if all applications have been cleared by the **applications clear** command.

Example

```
amnesiac (config) # applications reset
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"application," "applications clear"

Application statistics commands

This section describes the application statistics commands. You can also enable and disable this application statistics collection during an SCC configuration push. See the *SteelCentral Controller for SteelHead User Guide* for more information.

appstats enable

Enables statistics collection for applications.

Syntax

[no] appstats enable

Parameters

None

Usage

By default, this feature is disabled. The no command option disables application statistics collection if it has been enabled. Custom applications are not supported.

This feature does not report accurate pass-through data in an active-active serial cluster deployment.

You can also enable and disable this feature during an SCC configuration push. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac (config) # appstats enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show appstats"

Topology commands

Topology configuration provides a way to define a network configuration that is shareable between SteelHeads. Topology configuration is accessed by the path selection feature, QoS components, secure transport operations, and by other services managed within the SteelCentral Controller for SteelHead. Topology configuration provides building blocks for network connectivity that you configure separately or combine to construct more complex configurations such as path selection. You define a topology once and then reuse it as needed.

The topology provides the SteelHead with a view onto the network it is connected to. The topology consists of the network, the sites, and the uplinks to the network for the sites. Additionally, QoS profiles are linked to the sites.

A network topology includes these WAN topology properties:

- **Site** - Collection of resources that share one or more common WAN links, usually in one physical location such as a branch office or data center. Within a topology, the site defines the configuration parameters that are necessary to connect the site to the network.
- **Peer** - A SteelHead appliance. Each peer has one local site that is automatically created and cannot be deleted. A peer belongs to a site and can be connected to multiple areas through different interfaces.
- **Area** - A set of subnets reachable by one peer interface. Areas are disjoint; they cannot have subnets in common.
- **Network** - WAN networks that sites use to communicate with each other, such as MPLS, VSAT, or Internet. Within a topology, *network* is a label for connection to an available WAN.
- **Uplink** - A physical connection from a site to a WAN network, with its own upstream and downstream bandwidths. There is one default uplink for each interface.

topology clear networks

Clears all the configured networks.

Syntax

topology clear networks [**confirm**]

Parameters

confirm	Confirm to clear the configured networks.

Example

```
amnesiac (config) # topology clear networks
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show topology”

topology clear remote-sites

Clears all the configured remote sites.

Syntax

topology clear remote-sites [confirm]

Parameters

confirm	Confirms to clear the configured remote sites.

Usage

Each SteelHead peer has one local site that is automatically created and cannot be deleted.

To delete one remote site, use the **no topology site <name>** command.

Example

```
amnesiac (config) # topology clear remote-sites
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"topology clear networks," "show topology"

topology site

Configures the name and QoS profile names for a site.

Syntax

[no] topology site {<site-name> | local | default-site} [out-qos-profile <profile-name>] [in-qos-profile <profile-name>]

Parameters

<site-name>	Site name: for example, data center.
local	Specifies the local site name, which is where the SteelHead is located.
default-site	Specifies the default site, which is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed. You cannot add a new area or a new subnet to an existing area for the default site.
out-qos-profile <profile-name>	Specifies the QoS profile name for outbound QoS. These parameters link the outbound QoS configuration to the site to fine-tune the QoS behavior for the site. QoS profiles in RiOS 9.0 replace QoS service policies in previous versions. A QoS profile is a reusable set of QoS rules and classes.
in-qos-profile <profile-name>	Specifies the QoS profile name for inbound QoS. These parameters link the inbound QoS configuration to the site to fine-tune the QoS behavior for the site. QoS profiles in RiOS 9.0 replace QoS service policies in previous versions. A QoS profile is a reusable set of QoS rules and classes.

Usage

A site is a collection of resources that share one or more common WAN links, usually in one physical location. Each peer has one local site that is automatically created and cannot be deleted. A QoS profile for a site is used for all networks connected to the site.

RiOS 9.0 determines the destination site using a longest-prefix match on the site subnets. For example, if you define site 1 with 10.0.0.0/8 and site 2 with 10.1.0.0/16, then traffic to 10.1.1.1 matches site 2, not site 1. Consequently, the default site defined as 0.0.0.0 only matches traffic that does not match any other site subnets. This is in contrast to RiOS 8.6 and earlier, where you configured sites in an explicit order and the first-matching subnet indicated a match for that site.

The maximum number of QoS sites is 500.

Example

```
amnesiac (config) # topology site eastcoast out-qos-profile ProtectVoIP
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show topology site”

topology site add-area

Adds a new area for a topology site.

Syntax

topology site {<site-name> | local | default-site} add-area [peers <peers-list>] subnets <subnet-list>

Parameters

<site-name>	Site name: for example, data center.
local	Specifies the local site name, which is where the SteelHead is located.
default-site	Specifies the default site, which is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed. You cannot add a new area or a new subnet to an existing area for the default site.
peers <peers-list>	Specifies a comma separated list of peer IP addresses. These are the IP addresses of remote SteelHeads that are reachable from the SteelHead that you are configuring.
subnets <subnet-list>	Specifies a comma separated list of IP prefixes.

Usage

An area is a set of subnets and peers at the remote site that is reachable by the peer interface. Areas are disjoint and cannot have subnets in common.

Example

```
amnesiac (config) # topology site local add-area peers 10.11.100.4,10.11.200.4 subnets
10.11.0.0/16
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"topology clear remote-sites," "show topology site"

topology site area

Configures an area for a topology site.

Syntax

topology site {<name> | local | default-site} area <area-id> [add_peers <peers-list>] [del_peers <peers-list>] [add_subnets <subnets-list>] [del_subnets <subnets-list>]

Parameters

<site-name>	Site name: for example, data center.
local	Specifies the local site name, which is where the SteelHead is located.
default-site	Specifies the default site, which is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed. You cannot add a new area or a new subnet to an existing area for the default site.
peers <peers-list>	Specifies a comma-separated list of peer IP addresses. These are the IP addresses of remote SteelHeads that are reachable from the SteelHead that you are configuring.
<area_id>	Area index.
add_peers <peers-list>	Specifies a comma-separated list of IP addresses.
del_peers <peers-list>	Deletes a list of peers.
add_subnets <subnets-list>	Adds a list of subnets.
del_subnets <subnets-list>	Deletes a list of subnets.

Usage

An area is a set of subnets and peers at the remote site that is reachable by the peer interface. Areas are disjoint and cannot have subnets in common.

You cannot add a new area or a new subnet to an existing area for the default site.

Example

```
amnesiac (config) # topology site local area 53 del_peers 10.11.100.4,10.11.200.4 del_subnets
10.11.0.0/16
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"topology clear remote-sites"

topology site clear areas

Clears all the configured areas for the site.

Syntax

topology site {<site-name> | local | default-site} clear areas [confirm]

Parameters

<site-name>	Site name: for example, data center.
local	Specifies the local site name, which is where the SteelHead is located.
default-site	Specifies the default site, which is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed. You cannot add a new area or a new subnet to an existing area for the default site.
confirm	Confirms to clear the configured areas.

Usage

An area is a set of subnets and peers at the remote site that is reachable by the peer interface. Areas are disjoint and cannot have subnets in common.

Example

```
amnesiac (config) # topology site us-dc1 clear areas
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“topology clear remote-sites”

topology site clear uplinks

Clears all the configured uplinks for the site.

Syntax

topology site {<site-name> | local | default-site} clear uplinks [confirm]

Parameters

<site-name>	Site name: for example, data center.
local	Specifies the local site name, which is where the SteelHead is located.
default-site	Specifies the default site, which is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed.
confirm	Confirms to clear the configured uplinks.

Usage

An uplink is a physical connection from a site to a network, with its own upstream and downstream bandwidths. It is the last network segment connecting the local site to a WAN network. A site can have single or multiple uplinks to the same network and can connect to multiple networks.

Example

```
amnesiac (config) # topology site us-dc1 clear uplinks
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“topology clear remote-sites”

topology site rename

Renames a site to a new name.

Syntax

topology site {<site-name> | local | default-site} rename <new-name>

Parameters

<site-name>	Site name: for example, data center.
local	Specifies the local site name, which is where the SteelHead is located.
default-site	Specifies the default site, which is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed.
<new-name>	Specifies the new site name.

Usage

You can rename a site and the name is automatically propagated to all resources that use it such as QoS and path-selection configurations.

Example

```
amnesiac (config) # topology site US-DC1 rename US-DC2
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“topology site”

topology site uplink

Configures the uplink parameters for a remote site.

Syntax

topology site {<site-name> | local | default-site} uplink <uplink-name> network <name> bandwidth_up <kbps> bandwidth_down <kbps> [gateway <ip-address>] [probing_bw <kbps>]

Parameters

<site-name>	Site name: for example, data center.
local	Specifies the local site name, which is where the SteelHead is located.
default-site	Specifies the default site, which is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed.
<uplink-name>	Specifies the uplink name.
network <name>	Specifies the network name. My_WAN is the default network name.
bandwidth_up <kbps>	Specifies the upload bandwidth in kilobits per second for the uplink.
bandwidth_down <kbps>	Specifies the download bandwidth in kilobits per second for the uplink.
gateway <ip-address>	Specifies the gateway IP address.
probing_bw <kbps>	Specifies the path selection probing bandwidth in kilobits per second. This value rate limits the probes sent by the SteelHead on a per uplink basis to 128 kbps per uplink by default. This setting only applies to probes sent by a SteelHead but does not apply to incoming probes.

Usage

An uplink is a physical connection from a site to a network, with its own upstream and downstream bandwidths. It is the last network segment connecting the local site to a WAN network. A site can have single or multiple uplinks to the same network and can connect to multiple networks.

RiOS 9.0 determines the destination site using a longest-prefix match on the site subnets. For example, if you define site 1 with 10.0.0.0/8 and site 2 with 10.1.0.0/16, then traffic to 10.1.1.1 matches site 2, not site 1. Consequently, the default site defined as 0.0.0.0 only matches traffic that does not match any other site subnets. This is in contrast to RiOS 8.6 and earlier, where you configured sites in an explicit order and the first-matching subnet indicated a match for that site.

Remote uplinks are important to QoS because they define the available bandwidth for remote sites. RiOS uses the specified bandwidth definition to precompute the end-to-end bottleneck bandwidth for QoS.

Example

```
amnesiac (config) # topology site dc1 uplink inpath0_0 network My_WAN bandwidth_up 1000000
bandwidth_down 1000000 gateway 0.0.0.0 probing_bw 122
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“topology site uplink interface,” “show topology site”

topology site uplink interface

Configures the site uplink parameters for the local site.

Syntax

topology site {<site-name> | local | default-site} uplink <uplink-name> network <name> interface <interface-name> bandwidth_up <kbps> bandwidth_down <kbps> [gateway <ip-address>] [gre_tunnel {yes | no}] [probe_dscp <dscp>] [probe_timeout <timeout>] [probe_threshold <threshold>]

Parameters

<site-name>	Site name: for example, data center.
local	Specifies the local site name, which is where the SteelHead is located.
default-site	Specifies the default site, which is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed.
<uplink-name>	Uplink name.
network <name>	Specifies the network name.
gateway <ip-address>	Specifies the gateway IP address.
interface <interface-name>	Specifies the interface name. There is one default uplink for each interface.
bandwidth_up <kbps>	Specifies the upload bandwidth in kilobits per second.
bandwidth_down <kbps>	Specifies the download bandwidth in kilobits per second.
gre_tunnel yes	Enables GRE tunneling for this uplink.
gre_tunnel no	Disables GRE tunneling for this uplink.
probe_dscp <dscp>	Specifies the DSCP value (0 to 63) for path monitoring probes used for path selection.
probe_timeout <timeout>	Specifies the time to wait for a probe response, in seconds, before a path-selection probe is considered lost. The default timeout value is 2 seconds.
probe_threshold <threshold>	Specifies the number of path-selection 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 3 probes.

Usage

An uplink is a physical connection from a site to a network, with its own upstream and downstream bandwidths.

In the local site, you configure the uplink bandwidth for uploading and downloading data and with the IP address of the gateway to the network the uplink connects to. If you do not have the gateway configured, the default gateway of the in-path interface is used.

Example

```
amnesiac (config) # topology site local uplink inpath0_0 network My_WAN interface inpath0_0
bandwidth_up 1000000 bandwidth_down 1000000 gateway 10.2.1.1 probe_dscp 10 probe_timeout 8
probe_threshold 4
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show topology uplink,” “show topology site”

topology site uplink rename

Renames an uplink name to a new name.

Syntax

topology site {<site-name> | local | default-site} uplink <name> rename <new-name>

Parameters

<site-name>	Site name: for example, data center.
local	Specifies the local site name, which is where the SteelHead is located.
default-site	Specifies the default site, which is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed.
<name>	Uplink name.
<new-name>	New uplink name.

Example

```
amnesiac (config) # topology site eastcoast uplink inpath0_0 rename MPLS1
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"topology site"

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. You define a path, called an uplink, by specifying a WAN egress point and providing a direction for the egressing packets to take. 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 or direct Internet 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 optimization service and functions even if you pause the optimization service or if the optimization service becomes unavailable.

path-selection channel

Configures the channel configuration settings on the SteelHead. A channel is an overlay tunnel between SteelHeads and SteelHead Interceptors that provide the SteelHeads a way to reach the configured uplink.

Syntax

[no] path-selection channel gateway-ip <ipv4-address> interface <interface-name> neighbor-ip <ipv4-address> [probe-timeout <seconds>] [probe-threshold <number>]

Parameters

gateway-ip <ipv4-address>	Specifies the gateway IPv4 address to reach the configured uplink. This is the IP address of an uplink that is Layer 2 reachable by at least one interface on a SteelHead Interceptor appliance.
interface <interface-name>	Specifies the relay interface over which the SteelHead reaches the uplink. Use the same in-path interface as used for the uplink configuration for the gateway IP address in the local site.
neighbor-ip <ipv4-address>	Specifies the IPv4 address of the in-path interface on the Interceptor that is Layer 2 away from the gateway IP address.
probe-timeout <seconds>	Specifies the time to wait for a probe response, in seconds, before the system considers the channel to be unavailable. The default timeout value is 2 seconds. Path selection uses ICMP pings to probe the channels. If the ping responses do not make it back within this timeout setting and the system loses the number of packets defined by the threshold value, it considers the channel to be down.
probe-threshold <number>	Specifies the number of timed-out probes before a channel is considered down or the number of received probes before a channel is considered up. The default is 2 probes.

Usage

Path selection can operate in SteelHead Interceptor cluster deployments where one or more SteelHeads are collaborating with one or more Interceptors to select paths dynamically. Because enabling path selection on a SteelHead that is part of a SteelHead Interceptor cluster requires an optimization service restart, we recommend configuring the SteelHead Interceptor before enabling path selection on a SteelHead.

Use this command on the SteelHead to define a cluster channel to an Interceptor. The WAN router or gateway must be the next hop to the Interceptor (not directly reachable by the SteelHead). In a cluster channel, the gateway is reachable by at least one interface on the Interceptor. SteelHeads tunnel packets to the Interceptor and instruct the appliance to send packets to that gateway directly. The Interceptor redirects all connections requiring path selection to the SteelHead for the lifetime of the connection. The SteelHead performs path selection on these traffic flows and eventually delivers them on the WAN through an Interceptor.

The channel can be up or down. Multiple channels can point to one uplink but only one channel can be active at a given time. You can configure 128 unique channels for path selection.

The SteelHead can automatically detect if it is placed in an Interceptor cluster that supports path selection. The SteelHead Interceptor 5.0 is the first Interceptor release to support path selection. For details about using path selection with SteelHead Interceptor clusters, see the *SteelHead Interceptor Deployment Guide* and the *SteelHead User Guide*.

Example

```
amnesiac (config) # path-selection channel gateway-ip 10.2.1.1 interface inpath0_0 neighbor-ip
10.3.2.1 probe-timeout 5 probe-threshold 4
```

Product

SteelHead CX, SteelHead EX, Interceptor, SteelHead-v, SteelHead-c

Related Commands

“show path-selection channels”

path-selection clear-rules

Clears all the configured path selection rules.

Syntax

[no] path-selection clear-rules [confirm]

Parameters

confirm	Confirms clearing the path-selection rules.

Example

```
amnesiac (config) # path-selection clear-rules
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"path-selection rule site application," "show path-selection settings"

path-selection enable

Enables the path selection feature.

Syntax

[no] path-selection enable

Parameters

None

Usage

Using the path selection feature, you can more accurately control traffic flow across multiple WAN circuits. At a high level, you can configure multiple paths for each connection by specifying rules based on various parameters.

Path selection is a transparent operation to the client, server, and any networking devices such as routers or switches. When you configure path selection, the SteelHead can alter the next hop gateway transparently for the client traffic. This granular path manipulation enables you to better use and more accurately control traffic flow across multiple WAN circuits.

Path selection configuration is highly dependent on the network, site, and uplink configurations, defined by the **topology** commands. You must complete topology configuration according to your physical network design. The SteelHead automatically probes through each uplink you configure at the local site. This probe is the mechanism by which the SteelHead automatically configures the path that is available. The SteelHead probes from each uplink towards each configured remote site that you configure.

Path selection is disabled by default. Use the **no** command option disables 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 User Guide* and the *SteelHead Deployment Guide*.

Example

```
amnesiac (config) # path-selection enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"Topology commands," "path-selection rule site application," "show path-selection settings," "show path-selection status"

path-selection rule site application

Configures path-selection rules for a remote site and application.

Syntax

[no] path-selection rule site {<site-name> | default-site | any} application <application>
[uplink-1-name <name>] [uplink-1-dscp <value>]
[uplink-2-name <name>] [uplink-2-dscp <value>]
[uplink-3-name <name>] [uplink-3-dscp <value>]
[default-action {drop | relay}] [position <position>]

Parameters

<site-name>	Site name: for example, data center.
default-site	Specifies the default site, which is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed. If you use the default site for path selection, Riverbed recommends defining a peer SteelHead IP address that belongs to the default site. This configuration helps path selection make a more accurate evaluation of the health of the path leading to the default site.
any	Indicates any site applies to traffic bound for all sites, including the default site.
<application>	Application. Enter ? at the system prompt to view a list of predefined applications.
uplink-1-name <name>	Specifies the name of uplink 1 for the path-selection rule.
uplink-1-dscp <value>	Specifies the DSCP value for uplink 1. The DSCP values are **0** to **63** or **preserve**. Preserve means that the DSCP level or IP ToS value found on the pass-through traffic is unchanged when it passes through the SteelHead. You must select DSCP values if the service providers are applying QoS metrics based on DSCP marking and each provider is using a different type of metric.
uplink-2-name <name>	Specifies the name of uplink 2 for the path-selection rule.
uplink-2-dscp <value>	Specifies the DSCP value for uplink 2. The DSCP values are **0** to **63** or **preserve**.
uplink-3-name <name>	Specifies the name of uplink 3 for the path-selection rule.
uplink-3-dscp <value>	Specifies the DSCP value for uplink 3. The DSCP values are **0** to **63** or **preserve.**
default-action	Specifies the default action for the path-selection rule if the rule is matched and all specified paths are down: ▪ **drop -** Discards all packets matching this rule. ▪ **relay** - Routes packets normally using the default path. If not configured, the default behavior is relay without applying path selection.
position <position>	Specifies the position in which the rule is consulted: 1 - <maximum position>.

Usage

To configure path selection, you define path-selection rules to direct any application to any site. Path selection rules direct matching traffic onto specific uplinks. Traffic is matched by a combination of application and destination site.

You can specify up to three uplinks per path-selection rule and three DSCP values per site. Path selection only uses local uplinks.

Each rule is identified with a destination site and application. You can create multiple rules for a site. When the combination of the site and application does not already exist, the command adds a new rule. Otherwise, it edits the existing path-selection rule. When editing a path-selection rule, fields not entered in the edit command retain their values after the update.

Example

```
amnesiac (config) # path-selection rule site New_York application http uplink-1-name inpath0_0
uplink-1-dscp preserve uplink-2-name inpath0_1 uplink-2-dscp preserve default-action relay
amnesiac (config) # path-selection rule site Default-Site application ASA uplink-1-name inpath0_0
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Application commands,” “QoS commands,” “show path-selection rules”

---

path-selection settings bypass non-local-trpy enable

Enables the bypass of nonlocal 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 deployment, configure this command on the second SteelHead, referred to as the middle file engine (MFE). See the *SteelHead Deployment Guide* for more information.

This command is disabled by default.

Example

```
amnesiac (config) # path-selection settings bypass non-local-tryp enable
```

Product

SteelHead CX, SteelHead EX

Related Commands

“path-selection enable,” “show path-selection settings”

---

path-selection settings path-reflect conn-setup enable

Enables path reflection for an optimized connection setup.

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 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 CX, SteelHead EX

Related Commands

“show path-selection settings”

---

path-selection settings path-reflect probe enable

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 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 CX, SteelHead EX

Related Commands

“show path-selection settings”

---

path-selection settings probe ricochet

Configures path monitoring settings to probe for ricochet behavior.

Syntax

[no] path-selection settings probe ricochet <learn>

Parameters

<learn>	▪ **on-any** - Learns from all WAN egress probe requests on any in-path interface. ▪ **first-on-any** - Learns from the first WAN egress probe request on any in-path interface. ▪ **first-on-cfg** - Learns from the first WAN egress probe request on the configured in-path interface. ▪ **drop** - Drops path-selection ricochet probes. This is the default behavior.

Usage

Path selection does not handle the ricochet of probe packets across relay interfaces. Dropping the ricochet probes is the default behavior.

Example

```
amnesiac (config) # path-selection settings probe ricochet on-any
```

Product

SteelHead CX, SteelHead EX

Related Commands

“show path-selection settings”

path-selection settings ttl-decrement enable

Enables the decrement of the time-to-live (TTL) of IP packets.

Syntax

[no] path-selection settings ttl-decrement enable

Parameters

None

Usage

Use the **no** form of the command to disable the decrement of the TTL.

Example

```
amnesiac (config) # path-selection settings ttl-decrement enable
```

Product

SteelHead CX, SteelHead EX

Related Commands

“show path-selection settings”

path-selection settings tunnel adjust-mss enable

Enables a TCP maximum segment size (MSS) adjustment when path tunnels are configured for path selection.

Syntax

[no] path-selection settings tunnel adjust-mss enable

Parameters

None

Usage

IP fragmentation of GRE packets can occur when the encapsulated packets exceed the MTU. When you configure an uplink with the tunnel mode set to GRE, the SteelHead automatically applies an MSS value to the traffic and prevents fragmentation from occurring. This automatically applied MSS value ensures that, in most environments, packets are not fragmented, even with the extra GRE overhead.

The **no** command option turns off the automatic MSS adjustment. Use this command to reenable the MSS adjustment if it has been disabled.

The MSS adjustment is on by default. As a best practice, leave the MSS adjustment on.

See the *SteelHead Deployment Guide* for more information about MTU sizing.

Example

```
amnesiac (config) # path-selection settings tunnel adjust-mss enable
```

Product

SteelHead CX, SteelHead EX

Related Commands

“show path-selection settings”

---

path-selection-transit-bypass enable

Turns off path selection rules for traffic at the transit site.

Syntax

[**no**] **path-selection-transit-bypass enable**

Parameters

None

Usage

Transit traffic is defined as traffic that is not sourced or destined locally. In a topology where some of the sites do not have SteelHeads, behavior can occur where path selection rules are applied asymmetrically, which can lead to asymmetrical GRE-encapsulated traffic. This behavior can cause issues with firewalls such as dropped connections.

This command allows the system to push general path selection rules but selectively turn off path selection for transit site traffic. You need to define subnets as part of the local site configuration. The system identifies transit traffic by checking subnets to see if the traffic is sourced or destined locally.

When this command is enabled and transit traffic is bypassed, no path selection matching of rules is applied to transit traffic, which results in traffic being relayed with no failover. Path selection rules are applied to local site traffic even if this command is enabled.

If transit traffic is not bypassed, the SteelHead sees inner channel traffic. DPI does not work on inner channel traffic so application-based path selection will not work on the transit site for optimized connections. Consider this behavior when configuring path selection rules for transit traffic.

This command is disabled by default. Path selection rules are applied to transit site traffic unless you enable this command. Use the **no** command option to disable this command if it has been enabled.

Example

```
amnesiac (config) # path-selection-transit-bypass enable
Bypass transit path selection: Yes
Path Selection Bypass is now enabled but will not apply to preexisting optimized connections.
```

Product

SteelHead CX, SteelHead EX, SteelHead-c

Related Commands

"show path-selection-transit-bypass status"

QoS commands

For details about QoS features and deployment, see the *SteelHead User Guide* and the *SteelHead Deployment Guide*.

---

qos clear-profiles

Clears all the configured QoS profiles.

Syntax

qos clear-profiles [confirm]

Parameters

confirm	Confirm the clearing of the profiles.

Usage

QoS profiles in RiOS 9.0 replace QoS service policies in previous versions.

Example

```
amnesiac (config) # qos clear-profiles
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"qos profile," "qos profile class"

---

qos control-packets

Configures WAN control packet settings.

Syntax

[no] qos control-packets dscp <dscp>

Parameters

dscp <dscp>	Specifies the DSCP marking for control packets. The DSCP values are 0-64 or 255 (reflect).

Usage

This command defines the global DSCP marking.

Example

```
amnesiac (config) # qos control-packets dscp 4
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show qos settings"

qos dscp-marking enable

Enables QoS differentiated services code point (DSCP) marking.

Syntax

[no] qos dscp-marking enable

Parameters

None

Usage

This command enables global QoS DSCP marking. By default, the setup of optimized connections and the out-of-band control connections are not marked with a DSCP value. Existing traffic marked with a DSCP value is classified into the default class.

If your existing network provides multiple classes of service based on DSCP values, and you are integrating a SteelHead into your environment, you can use this global DCSP feature to prevent dropped packets and other undesired effects.

The **no** version of the command disables DSCP marking.

Example

```
amnesiac (config) # qos dscp-marking enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show qos settings”

qos inbound bandwidth site

Configures the inbound QoS bandwidth for the specified site.

Syntax

[no] qos inbound bandwidth <bandwidth> site {<site-name> | local | default-site} [interface <interface-name>]

Parameters

<bandwidth>	Bandwidth for inbound QoS.
<site-name>	Site name: for example, data center.
local	Specifies the local site name, which is where the SteelHead is located.
default-site	Specifies the default site, which is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed.
interface <interface-name>	Specifies the interface name.

Usage

The system enables inbound and outbound QoS on all in-path interfaces by default (except the primary interface).

Inbound QoS supports in-path interfaces only; it does not support primary or auxiliary interfaces.

Uplinks connect the site to a network. A site can have a single or multiple uplinks to the same network and can connect to multiple networks. You can use multiple uplinks to the same network for redundancy. You must specify, per uplink, the bandwidth available for uploading and downloading data. The values of the configured bandwidth are used by RiOS to calculate the bandwidth available for traffic for inbound and outbound QoS configurations. In combination with the bandwidth configuration of the local sites uplink, the SteelHead can calculate the oversubscription factor in case the sum of the bandwidths of the remote sites to a network is greater than the bandwidth of the local site to the same network.

This configuration is a simplification compared to RiOS versions prior to 9.0 because the oversubscription factor is automatically computed and applied to the sites with the initial configuration of sites and when a new site is added.

When there is no user configured site bandwidth, the bandwidth is calculated based on the remote site uplink bandwidth, the local site uplink bandwidth, and network topology such as whether the remote site and local site share the same network.

The **no** command option removes the user configured site bandwidth.

Example

```
amnesiac (config) # qos inbound bandwidth 10000 site client_site interface wan0_0
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos outbound bandwidth site,” “show qos bandwidth”

qos inbound interface enable

Enables inbound QoS on the specified interface.

Syntax

[no] qos inbound interface <interface-name> enable

Parameters

<interface-name>	Interface name.

Usage

The system enables inbound and outbound QoS on all in-path interfaces by default (except the primary interface).

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos inbound shaping enable,” “show qos settings”

qos inbound shaping enable

Enables QoS inbound traffic shaping.

Syntax

[no] qos inbound shaping enable

Parameters

None

Usage

Inbound traffic shaping enables QoS classification to allocate bandwidth and prioritize traffic flowing into the LAN network behind the SteelHead. This behavior provides the benefits of QoS for environments that cannot meet their QoS requirements with outbound QoS. The **no** command option disables QoS inbound traffic shaping.

Use the **show qos settings** command to verify if inbound traffic shaping is enabled.

Example

```
amnesiac (config) # qos inbound shaping enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"qos inbound interface enable," "show qos settings"

qos outbound bandwidth site

Configures the outbound QoS bandwidth for the specified site.

Syntax

[no] qos outbound bandwidth <bandwidth> site {<site-name> | local | default-site} [interface <interface-name>]

Parameters

<bandwidth>	Bandwidth for outbound QoS.
<site-name>	Site name: for example, data center.
local	Specifies the local site name, which is where the SteelHead is located.
default-site	Specifies the default site, which is the match anything, catch-all site that is used if nothing else matches. This site 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. The default site cannot be removed.
interface <interface-name>	Specifies the interface.

Usage

The system enables inbound and outbound QoS on all in-path interfaces by default (except the primary interface).

Traffic is not classified until at least one WAN interface is enabled.

Uplinks connect the site to a network. A site can have a single or multiple uplinks to the same network and can connect to multiple networks. You can use multiple uplinks to the same network for redundancy. You must specify, per uplink, the bandwidth available for uploading and downloading data. The values of the configured bandwidth are used by RiOS to calculate the bandwidth available for traffic for inbound and outbound QoS configurations. In combination with the bandwidth configuration of the local sites uplink, the SteelHead can calculate the oversubscription factor in case the sum of the bandwidths of the remote sites to a network is greater than the bandwidth of the local site to the same network.

This configuration is a simplification compared to RiOS versions prior to 9.0 because the oversubscription factor is automatically computed and applied to the sites with the initial configuration of sites and when a new site is added.

When there is no user configured site bandwidth, the bandwidth is calculated based on the remote site uplink bandwidth, the local site uplink bandwidth, and network topology such as whether the remote site and local site share the same network.

The **no** command option removes the user configured site bandwidth.

Example

```
amnesiac (config) # qos outbound bandwidth 10000 site client_site interface primary
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos inbound bandwidth site,” “show qos settings”

qos outbound interface enable

Enables outbound QoS on the specified interface.

Syntax

[no] qos outbound interface <interface-name> enable

Parameters

<interface-name>	Interface name.

Usage

The system enables inbound and outbound QoS on all in-path interfaces by default (except the primary interface).

Traffic is not classified until at least one WAN interface is enabled.

Example

```
amnesiac (config) # qos outbound interface wan0_0 enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos outbound shaping enable,” “show qos settings”

qos outbound shaping enable

Enables QoS outbound traffic shaping.

Syntax

[no] qos outbound shaping enable

Parameters

None

Usage

Outbound traffic shaping enables QoS classification to control the priority of different types of network traffic and to ensure that the SteelHead gives certain network traffic (for example, Voice over IP) higher priority than other network traffic. The **no** version disables QoS outbound traffic shaping.

Use the **show qos settings** command to verify if outbound traffic shaping is enabled.

Example

```
amnesiac (config) # qos outbound shaping enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos outbound interface enable,” “show qos settings”

qos profile

Configures the QoS profile name.

Syntax

[no] qos profile <name>

Parameters

<name>	QoS profile name.

Usage

A QoS profile is a collection of QoS classes and rules that are associated with a given site. You can use the same QoS profile for multiple sites as well as inbound and outbound QoS. However, usually inbound QoS and outbound QoS have different functions so it is likely that you need to configure a separate QoS profile for inbound QoS.

You can link a QoS profile to a site by using the **topology site** command. Use the **show qos profiles** to display information about the QoS profile.

Example

```
amnesiac (config) # qos profile westcoast
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“topology site,” “show qos profile”

qos profile class

Configures the QoS class for a profile.

Syntax

[no] qos profile <name> class <class-name> [parent <class-name>]

Parameters

<name>	QoS profile name.
<class-name>	QoS class name. The QoS class indicates how delay-sensitive a traffic class is to the QoS scheduler. Select a class for the profile from the following (highest priority to lowest): ▪ **Real Time** - Specifies the real-time traffic class. Give this value to your highest priority traffic: for example, VoIP, or video conferencing. ▪ **Interactive** - Specifies an interactive traffic class: for example, Citrix, RDP, telnet and ssh. ▪ **Business Critical** - Specifies the business critical traffic class: for example, Thick Client Applications, ERPs, and CRMs. ▪ **Normal** - Specifies a normal-priority traffic class: for example, Internet browsing, file sharing, and email. ▪ **Low Priority** - Specifies 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** - Specifies the lowest priority. These are minimum service class guarantees; if better service is available, it is provided. For example, if a class is specified as low priority and the higher-priority classes are not active, then the low-priority class receives the highest possible available priority for the current traffic conditions. This parameter controls the priority of the class relative to the other classes.
parent <class-name>	Specifies the parent class name for the configured class. You cannot change the parent class for an existing child class. To remove the parent class, you must delete all rules for the corresponding child classes first.

Usage

A QoS profile contains one or more classes. Classes model the network requirements for applications that exhibit similar characteristics and have similar requirements: minimum bandwidth, maximum bandwidth, and latency priority. For example, the real-time class contains voice and video traffic.

Specifying the parent for a child class enables the 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 real-time priority, the child will inherit the business priority from its parent, and will use a real-time priority only with respect to its siblings. For more information, see the *SteelHead User Guide* and the *SteelHead Deployment Guide*.

Example

```
amnesiac (config) # qos profile branchwest class normal
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"qos profile class-params," "show qos profile"

qos profile class rename

Renames the QoS class in a profile.

Syntax

qos profile <name> class <class-name> rename <new-name>

Parameters

<name>	QoS profile name.
<class-name>	Class name.
<new-name>	New class name.

Usage

You can rename the QoS class in the profile and the class is automatically propagated to all resources that use the profile, such as sites and uplinks.

Example

```
amnesiac (config) # qos profile branch1 class Normal rename Best Effort
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"qos profile class," "show qos profile"

qos profile class-params

Configures the QoS class parameters for the specified profile.

Syntax

qos profile <name> class-params class <class-name> [priority <priority-id>] [min-bw <min-bw-percent>] [max-bw <max-bw-percent>] [ob-queue <method>] [ob-queue-length <length>] [out-dscp <out-dscp-value>] [conn-limit <optimized-connection-number>] [link-share <link-share-weight>] [ib-queue-length <length>]

Parameters

<name>	QoS profile name.
class <class-name>	Specifies the QoS class name. The QoS class indicates how delay-sensitive a traffic class is to the QoS scheduler. Select a service class for the profile from the following (highest priority to lowest): ▪ **Real Time** - Specifies real-time traffic class. Give this value to your highest priority traffic; for example, VoIP, or video conferencing. ▪ **Interactive** - Specifies an interactive traffic class: for example, Citrix, RDP, telnet and ssh. ▪ **Business Critical** - Specifies the business critical traffic class: for example, Thick Client Applications, ERPs, and CRMs. ▪ **Normal** - Specifies a normal priority traffic class: for example, Internet browsing, file sharing, and email. ▪ **Low Priority** - Specifies 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** - Specifies the lowest priority. These are minimum service class guarantees; if better service is available, it is provided: for example, if a class is specified as low priority and the higher priority classes are not active, then the low priority class receives the highest possible available priority for the current traffic conditions. This parameter controls the priority of the class relative to the other classes.

priority <priority-id>	Modifies QoS class priority settings. The priority range is from 1 to 6, where 1 is the highest and 6 is the lowest priority.
min-bw <min-bw-percent>	Specifies the QoS class guaranteed minimum bandwidth setting (as a percentage). 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. A default class is automatically created with minimum bandwidth of 10 percent. Traffic that does not match any of the rules is put into the default class. We recommend that you change the minimum default bandwidth of the default class to the appropriate value. You can adjust the value as low as 0%. The system rounds decimal numbers to 5 points.
max-bw <max -bw-percent>	Specifies the maximum allowed bandwidth (as a percentage) a QoS class receives as a percentage of the parent class guaranteed maximum bandwidth. The limit is applied even if there is excess bandwidth available. The system rounds decimal numbers to 5 points.
ob-queue <method>	Selects one of the following outbound queue methods for the leaf class (the queue does not apply to the inner class): ▪ **sfq** - Stochastic Fair Queuing (SFQ) is the default queue for all classes. Determines SteelHead 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. ▪ **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. ▪ **mx-tcp** - 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. See the *SteelHead User Guide* and the *SteelHead Deployment Guide* for information about usage scenarios and configuration details for MX-TCP.
ob-queue-length <length>	Specifies the outbound QoS class queue length. By default, each class has a queue length of 1024. Riverbed recommends that you consult with Riverbed Support or your sales engineer before you set this parameter.
out-dscp <out-dscp-value>	Specifies the QoS class outbound DSCP value. The DSCP values are **0-63** or **preserve**. Preserve is the default setting for a service class. Preserve means that the DSCP level or IP ToS value found on pass-through traffic is unchanged when it passes through the SteelHead.

conn-limit <optimized-connection-number>	Specifies 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. 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. In RiOS 9.0 and later, this parameter is only available through the CLI.
link-share <link-share-weight>	Specifies 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 that classes with a lower link share weight.
ib-queue-length <length>	Specifies the QoS class inbound queue length. By default, each class has a queue length of 1024. Riverbed recommends that you consult with Riverbed Support or your sales engineer before you set this parameter.

Usage

The minimum bandwidth must fall within the bandwidth limit for the SteelHead. Excess bandwidth is allocated based on the relative ratios of minimum bandwidth. The total minimum guaranteed bandwidth of all QoS classes must be less than or equal to 100% of the parent class. A default class is automatically created with minimum bandwidth of 10%. Traffic that does not match any of the rules is put into the default class.

Example

```
amnesiac (config) # qos profile profile0 class-params class class5 priority 5 min-bw 0.0 max-bw
100.0 ob-queue SFQ ob-queue-length 1024 out-dscp Preserve
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos profile class,” “show qos profile”

qos profile clear-classes

Clears all the configured QoS classes for the specified profile.

Syntax

qos profile <name> clear-classes [confirm]

Parameters

<name>	QoS profile name.
confirm	Confirms clearing the QoS classes.

Example

```
amnesiac (config) # qos profile legacy_profile clear-classes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"qos profile rule," "show qos profile"

qos profile clear-rules

Clears all the configured QoS rules for the specified profile.

Syntax

qos profile <name> clear-rules [confirm]

Parameters

<name>	QoS profile name.
confirm	Confirms clearing the QoS profile rule.

Example

```
amnesiac (config) # qos profile legacy_profile clear-rules
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"qos profile rule," "show qos profile"

qos profile rename

Renames the QoS profile to a new name.

Syntax

qos profile <name> rename <new-name>

Parameters

<name>	QoS profile name.
<new-name>	New name for the QoS profile.

Usage

You can rename a profile and the profile name is automatically propagated to all resources that use it such as sites and uplinks.

Example

```
amnesiac (config) # qos profile eastcoast rename newjersey
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"qos profile class," "show qos profile"

qos profiles reset

Resets the default profile back to the factory default settings.

Syntax

qos profiles reset [confirm]

Parameters

confirm	Confirms resetting to the factory default settings. You must run this keyword within 10 seconds to confirm this action.

Usage

This command only resets the default profile. User-created profiles are not reset by this command.

Example

```
amnesiac (config) # qos profiles reset
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show qos profile"

qos profile rule

Modifies a rule for a QoS profile.

Syntax

[no] qos profile <name> rule application <app-name> [class <class-name>] [dscp <value>] [position <position>]

Parameters

<name>	QoS profile name.
application <app-name>	Specifies the name of the application. Enter ? at the system prompt to view a list of more than 1100 available applications.

class <class-name>	Configures the class name for traffic matching this rule. The QoS class indicates how delay-sensitive a traffic class is to the QoS scheduler. Select a service class for the profile from the following (highest priority to lowest): ▪ **Real Time** - Specifies real-time traffic class. Give this value to your highest priority traffic; for example, VoIP, or video conferencing. ▪ **Interactive** - Specifies an interactive traffic class: for example, Citrix, RDP, telnet and ssh. ▪ **Business Critical** - Specifies the business critical traffic class: for example, Thick Client Applications, ERPs, and CRMs. ▪ **Normal** - Specifies a normal priority traffic class: for example, Internet browsing, file sharing, and email. ▪ **Low Priority** - Specifies 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** - Specifies the lowest priority. ▪ **default** - Uses whichever class is currently set for the default rule. By default, this is Low Priority. You can change it by modifying the default rule. These are minimum service class guarantees; if better service is available, it is provided: for example, if a class is specified as low priority and the higher priority classes are not active, then the low priority class receives the highest possible available priority for the current traffic conditions. This parameter controls the priority of the class relative to the other classes.
dscp <value>	Specifies the DSCP value. The DSCP values are **0-63**, **preserve**, or **inherit** (inherit from class). Preserve means that the DSCP level or IP ToS value found on the pass-through traffic is unchanged when it passes through the SteelHead.
position <position>	Specifies the position in which the rule is consulted: 1 - <maximum position>.

Usage

This command adds, edits, or deletes a rule from a QoS profile. You can create multiple QoS rules for a profile and these rules are followed in the configured order. SteelHeads support up to 2000 rules and up to 500 sites.

Example

```
amnesiac (config) # qos profile central rule application about.com class Normal position 2
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“qos profile,” “show qos profile”

qos reclassify applications

Reclassifies pre-existing traffic flows to match a new QoS configuration change.

Syntax

qos reclassify applications

Parameters

None

Usage

This command enables the QoS process on the SteelHead to dynamically reclassify pre-existing traffic flows to match the new configuration after a QoS configuration change.

Example

```
amnesiac (config) # qos reclassify applications
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"qos profile," "show qos profile"

Network services commands

---

rps enable

Enables the Receive Packet Steering (RPS) feature for all interfaces.

Syntax

[no] rps enable

Parameters

None

Usage

RPS improves path selection throughput by distributing the packet processing load across all CPU cores. We recommend enabling this command on all Interceptors and SteelHeads in a cluster. No error is reported if you don't configure the command on both the appliances but we recommend this configuration for best path selection throughput.

This command is disabled by default. No service restart is required.

Example

```
amnesiac (config) # rps enable
```

Product

Interceptor, SteelHead CX, SteelHead EX

Related Commands

"show rps"

Secure transport commands

Secure transport enables simple, manageable and large-scale VPN deployments. The SteelHead controller is a centralized service running on the SteelHead and is only configurable through the CLI. The SteelCentral Controller for SteelHead (SCC) manages the appliances participating in a secure transport group. This secure transport group is a set of SteelHeads that share the same cryptographic key material and have connectivity between each other. An SSL license is required for secure transport deployment. See the *SteelCentral Controller for SteelHead User Guide* for more information on how to centrally manage secure transport.

The secure transport client starts automatically with no manual configuration required. You can view the secure transport group configuration information by using the **show stp-client** commands. You can view the status of the secure transport client by using the **show stp-client status** command.

scc enable

Enables auto-registration with the SCC for secure transport operations.

Syntax

[no] scc enable

Parameters

None

Usage

The SteelCentral Controller for SteelHead is required to manage secure transport operations and deployment. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac (config) # scc enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show scc”

scc hostname

Configures the hostname for the SCC.

Syntax

[no] scc hostname <hostname>

Parameters

<hostname>	Hostname.

Usage

The SteelCentral Controller for SteelHead is required to manage secure transport operations and deployment. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac (config) # scc hostname chief-scc4
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show scc”

no stp-client enable

Disables the secure transport client.

Syntax

no stp-client enable

Parameters

None

Usage

The secure transport service is enabled by default. Use this command to disable the service.

In RiOS 9.0 and later, IPSec secure peering and the secure transport service are mutually exclusive. Before you enable IPSec secure peering, you must disable the secure transport service.

The SteelCentral Controller for SteelHead is required to manage secure transport operations and deployment. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac (config) # no stp-client enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-c, SteelHead-v

Related Commands

“show stp-client settings”

stp-client controller in-path enable

Configures the in-path control channel for connectivity from the client to the controller.

Syntax

[**no**] **stp-client controller in-path enable** [**private <interface-1> public <interface-2>**]

Parameters

private <interface-1>	Specifies the interface in which to reach the private IP address of the controller.
public <interface-2>	Specifies the interface in which to reach the public IP address of the controller.

Usage

This command enables the secure transport client to connect to the controller through multiple interfaces. When enabled, all interfaces are available for controller connectivity. The default behavior of this command is to attempt to connect to the controller through the private IP address via all interfaces first and then, if that fails, connect through the public IP address of the controller. You can override this behavior and specify which interface you want to use for connectivity to the controller.

You must restart the secure transport service by using the **stp-client restart** command for your changes to take effect.

This command is disabled by default. By default, the client attempts to connect to the controller through the management interface.

Example

In the following example, the secure transport client attempts to connect to the private IP address of the controller through the inpath0_0 interface. If that fails, the secure transport client attempts to connect to the public IP address of the controller through the mgmt0_0 interface.

```
amnesiac (config) # stp-client controller in-path enable private inpath0_0 public mgmt0_0
amnesiac (config) # stp-client restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show stp-client settings," "stp-client restart"

---

stp-client restart

Restarts the secure transport client.

Syntax

stp-client restart

Parameters

None

Usage

This command can be used at any time to restart the secure transport client process.

You must run this command for the **stp-client controller in-path enable** command to take effect.

Example

```
amnesiac (config) # stp-client restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"stp-client controller in-path enable"

---

stp-client stc enable

Enables the secure transport concentrator on the appliance.

Syntax

[no] stp-client stc enable

Parameters

None

Usage

When there are multiple SteelHeads in a site, you can configure one of the SteelHeads as a secure transport concentrator to perform encryption and decryption of traffic.

We strongly recommend that you use the SCC GUI to configure the secure transport concentrator and remote SteelHeads that you are monitoring and configuring using the SCC. See the *SteelCentral Controller for SteelHead Deployment Guide* for information and configuration details.

Example

```
amnesiac (config) # stp-client stc enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show stp-client settings"

stp-controller address

Configures the IP addresses for the SteelHead controller.

Syntax

[no] stp-controller address private-ip <private-ip-address> [public-ip <public-ip-address> port <port>]

Parameters

private-ip <private-ip-address>	Specifies an IP address that is bound to the management interface of the SteelHead that you have chosen to be the SteelHead controller. The SteelHead controller IP address can be bound to an in-path address if management over the in-path interface is enabled (that is, the SteelHead is managed via the in-path address).
public-ip <public-ip-address> port <port>	Specifies a publicly reachable IP address and port that are translated via NAT to the management interface on the SteelHead running the SteelHead controller.

Usage

Use this command to configure the IP addresses of the SteelHead appliance acting as the SteelHead controller. You must enable the SteelHead controller first by entering the **stp-controller enable** command.

Example

```
amnesiac (config) # stp-controller address private-ip 172.16.249.132 public-ip 10.33.249.139 port
4500
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show stp-controller address,” “stp-controller enable”

stp-controller enable

Enables the SteelHead controller service.

Syntax

[no] stp-controller enable

Parameters

None

Usage

The SteelHead controller is a centralized service running on the SteelHead that coordinates the secure transport operation. The controller must be reachable by other SteelHeads and only one active controller is allowed per deployment.

The SteelHead controller service is disabled by default and is only configurable through the CLI.

The SteelCentral Controller for SteelHead is required to manage the secure transport deployment. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac (config) # stp-controller enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show stp-controller status"

Web proxy commands

Web proxy transparently intercepts all traffic bound to the Internet and provides optimization services such as persistent web caching, caching video content, SSL decryption to enable content caching, and logging services through audit trails. Web proxy improves HTTP performance and reduces congestion on Internet traffic. It also provides performance benefits when you access HTTP(S) servers on the Internet directly from a branch office. It provides visibility to all Internet activity at any given branch as long as that destined traffic passes through the web proxy.

You can configure the web proxy feature on the SteelHead using the command-line interface without relying on an SCC. However, this method only supports HTTP proxying, as HTTPS decryption is not possible without the Certificate Authority Authorization Service (CAAS) configured on the SCC.

See the *SteelCentral Controller for SteelHead User Guide* for more information on managing web proxy operations.

Note: Web proxy commands are supported on the SteelHead xx55 and xx70 models. Starting in RiOS 9.6, web proxy is also supported on the new VCX10 to VCX90 virtual appliance models as long as they are licensed appropriately and the management disk is large enough to allocate at least 5 GB of space for the web proxy cache.

web-proxy audit-log enable

Configures the syslog server settings to provide web proxy audit logging.

Syntax

[no] web-proxy audit-log remote-address <remote-address> remote-port <port> [format <format>] enable

Parameters

remote-address <remote-address>	Specifies the IPv4 address or the domain name of the remote syslog server.
remote-port <port>	Specifies the remote port of the remote syslog server.
format <format>	Specifies one of the following logging formats: ▪ **common** - Common log format. This is the default format. ▪ **squid** - Squid log format ▪ **extended** - Extended log format ▪ **extended2** - Extended 2 log format

Usage

You can capture HTTP requests in various formats for audit and compliance purposes. HTTP and decrypted HTTPS requests are logged in common log format by default.

Example

```
amnesiac (config) # web-proxy audit-log remote-address 10.5.36.89 remote-port 88 format squid enable
```

Product

SteelHead CX

Related Commands

“show web-proxy audit-log settings”

web-proxy cache enable

Enables web proxy SSL and HTTP caching.

Syntax

[no] web-proxy cache enable

Parameters

None

Usage

This feature allows web object caching of HTTP content and content that is SSL encrypted.

The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac (config) # web-proxy cache enable
```

Product

SteelHead CX

Related Commands

“show web-proxy ssl”

web-proxy cache size

Configures the web proxy cache size.

Syntax

web-proxy cache size <size>

Parameters

<size>	Size of the cache in gigabytes (GB). This command only accepts up to two decimal places after the decimal. For example, 12 is accepted and 12.28 is accepted, but 12.285 is not accepted.

Usage

The management disk must be large enough to allocate at least 5 GB of space for the web proxy cache. Using this command purges the existing cache.

You can decrease (down to 5 GB) or enlarge the cache size up to the current license limit of the VCX model (licenses range from 200 GB to 800 GB). If the configured cache size is larger than what the disk can support an alarm is raised. For example, if you configure a web proxy cache size of 15 GB but the actual available space on the disk is 5 GB then the actual cache size is 5 GB because this is what the disk can support.

The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac (config) # web-proxy cache size 6.14
```

```
amnesiac > show web-proxy cache size
Web-proxy min license allowed cache size (GB): 5.00
Web-proxy max license allowed cache size (GB): 200.00
Web-proxy configured cache size (GB): 6.14
Web-proxy actual cache size (GB): 6.14
```

In the following example, an error message is generated when you configure a cache size below the minimum required:

```
amnesiac (config) # web-proxy cache size 4
% Invalid webproxy cache size, cache size needs to be between 5GB and 200GB
```

Product

SteelHead-v

Related Commands

“show web-proxy cache size,” “web-proxy enable”

---

web-proxy enable

Enables the web proxy service.

Syntax

[**no**] **web-proxy enable**

Parameters

None

Usage

The web proxy service is disabled by default.

Enable web proxy on the client-side appliance with auto-discovery and pass-through rules to use a single-ended Web proxy to transparently intercept all traffic bound to the Internet. Web proxy improves performance by providing optimization services such as web object caching and SSL decryption to enable content caching and logging services.

The proxy cache is separate from the RiOS data store. When objects for a given website are already present in the cache, the system terminates the connection locally and serves the content from the cache. This saves the connection setup time and also reduces the bytes to be fetched over the WAN. The cache content is persistent and will survive SteelHead reboots and service restarts.

You can also use domain labels with the web proxy in your in-path rules to reduce the load to the proxy using a finer, more granular traffic selection.

The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac (config) # web-proxy enable
```

Product

SteelHead CX

Related Commands

“in-path rule auto-discover,” “in-path rule pass-through,” “show web-proxy status”

---

web-proxy parent automatic enable

Enables the interception of explicitly proxied connections.

Syntax

[no] web-proxy parent automatic enable

Parameters

None

Usage

Many customers either have an explicit proxy server at the data center or incorporate the transparent upstream proxy in their current infrastructure. This command enables the Riverbed web proxy feature to inter-operate explicitly with an upstream web proxy. In this deployment, clients are aware that requests go through a proxy. Web proxy redirects connections to the parent proxy.

A web proxy parent proxy deployment can be either automatic or manual but not both.

Example

```
amnesiac (config) # web-proxy parent automatic enable
```

Product

SteelHead CX

Related Commands

"web-proxy parent automatic whitelist," "web-proxy parent manual enable," "show web-proxy parent status"

web-proxy parent automatic whitelist

Configures the parent proxy automatic mode whitelist to allow caching of HTTP traffic.

Syntax

[no] web-proxy parent automatic whitelist { <host-name> | <ip-address> }

Parameters

<host-name>	Specifies the host name of the parent proxy. You can specify host names in a comma-separated list. Specify the list of host names in order of preference.
<ip-address>	Specified IPv4 address of the trusted parent proxy. You can specify IP addresses in a comma-separated list. Specify the list of IP addresses in order of preference.

Usage

When web proxy is configured in automatic mode on the SteelHead CX and the clients are configured to use a PAC file (or proxy), only secure (HTTPS) content is cached. To cache non-secure content, use this command to add a list of IP addresses of proxies that the clients are configured to use.

You can use the **show web-proxy parent status** command to view this configured whitelist.

Example

```
amnesiac (config) # web-proxy parent automatic whitelist address 1.1.1.1,2.2.2.2,3.3.3.3
```

Product

SteelHead CX

Related Commands

"web-proxy parent automatic enable," "show web-proxy parent status"

web-proxy parent manual enable

Enables the interception of transparently proxied connections.

Syntax

[no] web-proxy parent manual enable

Parameters

None

Usage

Many customers either have an explicit proxy server at the data center or incorporate the transparent upstream proxy in their current infrastructure. This command enables the Riverbed web proxy feature to inter-operate with an upstream web proxy. In this deployment, web proxy is transparent and clients are not aware that requests go through a proxy. Web proxy redirects connections to the configured parent proxy except for any domains specified by the **web-proxy parent manual excludes domain** command.

A web proxy parent proxy deployment can be either automatic or manual but not both.

Example

```
amnesiac (config) # web-proxy parent manual enable
```

Product

SteelHead CX

Related Commands

"web-proxy parent automatic enable," "web-proxy parent manual http," "web-proxy parent manual https," "web-proxy parent manual excludes domain," "show web-proxy parent status"

web-proxy parent manual excludes domain

Configures which domains to exclude from sending to the parent proxy.

Syntax

[no] web-proxy parent manual excludes domain <domain-name>

Parameters

<domain-name>	Domain name. The domain names can be hostnames (for example, www.hostname.com) or wildcard hostnames (for example, *.riverbed.com).

Usage

This command creates an exclusion bypass list to exclude the configured domains from being sent to the parent proxies. Instead, connections to these domains go directly to the Internet.

Example

```
amnesiac (config) # web-proxy parent manual excludes domain facebook.com
amnesiac (config) # web-proxy parent manual enable
```

Product

SteelHead CX

Related Commands

"web-proxy parent manual enable," "show web-proxy parent status"

web-proxy parent manual http

Configures the IP address or hostname of the HTTP parent proxy.

Syntax

[no] web-proxy parent manual http {<host-name> | <ip-address>} port <port-number>

Parameters

<host-name>	Host name of the parent proxy. You can specify host names in a comma-separated list. Specify the list of host names in order of preference.
<ip-address>	IPv4 address of the parent proxy. You can specify IP addresses in a comma-separated list. Specify the list of IP addresses in order of preference.
port <port-number>	Specifies the port number of the parent proxy.

Usage

The web proxy needs to trust the certificates issued by the parent proxy to make any connections.

Example

```
amnesiac (config) # web-proxy parent manual http 104.129.194.38 port 443
amnesiac (config) # web-proxy parent manual enable
```

Product

SteelHead CX

Related Commands

"web-proxy parent manual enable," "web-proxy parent manual https," "show web-proxy parent status"

web-proxy parent manual https

Configures the IP address or hostname of the HTTPS parent proxy.

Syntax

[no] web-proxy parent manual https {<hostname> | <ip-address>} port <port-number>

Parameters

<hostname>	Hostname of the parent proxy. You can specify hostnames in a comma-separated list. Specify the list of hostnames in order of preference.
<ip-address>	IPv4 address of the parent proxy. You can IP addresses in a comma-separated list. Specify the list of IP addresses in order of preference.
port <port-number>	Specifies the port number of the parent proxy.

Usage

The web proxy needs to trust the certificates issued by the parent proxy to make any connections.

Example

```
amnesiac (config) # web-proxy parent manual https cws port 8080
amnesiac (config) # web-proxy parent manual enable
```

Product

SteelHead CX

Related Commands

"web-proxy parent manual enable," "web-proxy parent manual http," "show web-proxy parent status"

web-proxy ssl enable

Enables web proxy SSL decryption for sites in the domain whitelist.

Syntax

[no] web-proxy ssl enable

Parameters

None

Usage

The SteelCentral Controller for SteelHead is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac (config) # web-proxy ssl enable
```

Product

SteelHead CX

Related Commands

"show web-proxy ssl"

web-proxy ssl-domain

Configures the web proxy SSL domain whitelist.

Syntax

[no] web-proxy ssl-domain <domain-name> [include-san]

Parameters

<domain-name>	Domain name. The domain names can be hostnames (for example, www.hostname.com) or wildcard hostnames (for example, *.riverbed.com).
include-san	Includes the subject alternative name field for a given domain in order to optimize the sub-domains. This option is disabled by default.

Usage

The CA service on the SteelCentral Controller for SteelHead must be configured and accessible before you configure this command.

The SCC is required to manage web proxy operations. See the *SteelCentral Controller for SteelHead User Guide* for more information.

Example

```
amnesiac (config) # web-proxy ssl-domain *.googlevideo.com
```

Product

SteelHead CX

Related Commands

"show web-proxy ssl-domains"

web-proxy youtube enable

Enables web proxy YouTube caching.

Syntax

[no] web-proxy youtube enable

Parameters

None

Usage

YouTube caching is handled as a special case given its growing popularity in the enterprise. When web proxy is enabled, YouTube caching is enabled by default and requires no manual intervention. YouTube traffic is typically encrypted so you should ensure that HTTPS optimization is enabled. YouTube caching performs regular expression-based caching to identify YouTube content to cache.

You must add the following domains to the HTTPS domain whitelist:

- *.googlevideo.com
- *.youtube.com

You can configure the domains on the SCC or by using the **web-proxy ssl-domain** command on the SteelHead. If you use the SCC, the CAAS must be configured and accessible to the SCC.

Example

```
amnesiac (config) # web-proxy youtube enable
```

Product

SteelHead CX

Related Commands

“web-proxy ssl-domain,” “show web-proxy youtube”

Domain label commands

domain-label

Configures domain label settings.

Syntax

[no] domain-label <name> domain <domain-name>

Parameters

<name>	Name of the domain label. ■ Domain labels are case sensitive and can be any string consisting of letters, numbers, the underscore (_), or the hyphen (-). Don't use spaces in domain labels. ■ A domain label can be up to 64 characters long. ■ Domain label changes (that is, adding and removing domain names inside a label) are applied immediately by the rules that use the domain labels that you have modified. ■ You can create up to 63 unique domain labels. ■ Domain labels aren't compatible with IPv6.
<domain-name>	Domain name. The domain names can be hostnames (for example, www.hostname.com) or wildcard hostnames (for example, *.riverbed.com). ■ Domain names can appear in multiple domain labels. ■ Domain names must include a top-level domain, for example, .com or .org. No wildcard is allowed in the top-level domain, for example, microsoft.* ■ A maximum 64 characters per domain name is allowed. ■ Domain names must have some characters in the second-level domain names, for example *.outlook.com, *.sharepoint*.com, but not *.com ■ A domain name can be up to 64 characters long. ■ Matching on the domain name is case in-sensitive. ■ Do not use consecutive periods or consecutive wildcards. ■ Do not use IP addresses.

Usage

A domain label is a group of Internet domains with optional wildcards to define a wider group. For example a domain called Office365 can match:

- *.microsoft.com
- *.office365.com
- *office.com

You use these domain labels in your in-path rules to simplify in-path rule management. Domain labels are compatible with auto-discover, passthrough, and fixed-target in-path rules. Domain labels are useful if many services are hosted by the same IP address or are hard to separate into distinct subnets. If you know which domains your traffic is going to, you set up your in-path rule to match those domains based on the domain label.

Domain labels do not replace the destination IP address in an in-path rule. The in-path rule still sets the destination IP/subnet (or uses a host label or port to set the destination). The in-path rule matches the destination IP address or port first, and then matches the domain label as a secondary check. The rule must match both the destination and the domain label.

Domain labels in an in-path rule automatically apply to HTTP and HTTPS (ports 80 and 443 by default) for optimization when the port field is set to "All Ports". If you specify a different port number in your in-path rule, the rule honors that port number.

On a downgrade, all domain label information is lost.

The client-side SteelHeads and server-side SteelHeads must be running RiOS 9.2.

The **no** command option removes the domain label. You cannot remove a domain label if it is used in an in-path rule. You must first remove all domain-label configurations from the in-path rules.

Example

```
amnesiac (config) # domain-label Bag domain *company.com
amnesiac (config) # in-path rule auto-discover dst-domain Bag
```

Product

SteelHead CX, SteelHead EX, SteelHead-v

Related Commands

“In-path and virtual in-path support commands,” “show domain-label,” “show domain-labels”

Host label commands

host-label

Configures host label settings.

Syntax

[no] host-label <name> {hostname {<hostname> | '<hostname>,...>'} [subnet <X.X.X.X/XX> | 'subnet <X.X.X.X/XX>,...'] | subnet {<X.X.X.X/XX> | 'subnet <X.X.X.X/XX>,...'} [hostname {<hostname> | '<hostname>,...>']}

Parameters

<name>	Name of the host label. ▪ Host labels are case sensitive and can be any string consisting of letters, numbers, the underscore (_), or the hyphen (-). There can't be spaces in host labels. There is no limit on the number of host labels you can configure. ▪ Entries in a host label can be an IP address, a subnet, or an FQDN (fully qualified domain name). ▪ To avoid confusion, don't use a number for a host label. ▪ Host labels that are used in QoS or in-path 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. ▪ Host labels aren't compatible with IPv6. ▪ RiOS versions 9.2.1 and later include a predefined host label, **_cloud-accel-saas_**, that detects any IP addresses that carry Cloud Accelerator-enabled SaaS traffic automatically. As SaaS applications are added or deleted, the host label is automatically updated with the list of associated IP addresses. This host label mitigates the requirement that domain rules and Cloud Acceleration be mutually exclusive. You can use this host label in the i**n-path rule auto-discover** command.
hostname <hostname> |'<hostname>,...>'	Specifies a hostname or a comma-separated list of hostnames for this label. You must enclose comma-separated lists in single quotation marks ('). ▪ Hostnames are case insensitive. ▪ You can use up to 100 unique hostnames. A hostname can appear in multiple host labels. ▪ A host label can contain up to 64 subnets and hostnames.
subnet <X.X.X.X/XX> | 'subnet <X.X.X.X/XX>,...'	Specifies an IPv4 subnet for the specified host label or a comma-separated list of IPv4 subnets. Use the format X.X.X.X/XX. You must enclose comma-separated lists in single quotation marks ('). Only IPv4 subnets are allowed.

Usage

Host labels are names given to lists of hosts (IPv4 subnets and hostnames) that you can specify to streamline configuration when configuring QoS or in-path 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.

Host labels are compatible with auto-discover, passthrough, and fixed target in-path rules. A host label allows one in-path rule to match many destination subnets or hostnames.

Hostnames referenced in a host label are automatically resolved through a DNS query. The system resolves them immediately after you add a new host label or after you edit an existing host label. The system also resolves hostnames automatically, once daily. If you want to resolve a hostname immediately, use the **resolve host-labels** command.

You can control the refresh period for DNS queries for hostnames using the **host-labels refresh-intvl** command.

Example

```
amnesiac (config) # host-label rvbd hostname www.riverbed.com
amnesiac (config) # in-path rule auto-discover dst-host rvbd
```

Product

SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“In-path and virtual in-path support commands,” “host-labels refresh-intvl,” “resolve host-labels,” “show host-label”

host-labels refresh-intvl

Configures the hostname DNS refresh interval.

Syntax

[no] host-labels refresh-intvl <minutes>

Parameters

<minutes>	Refresh interval in minutes. The minimum interval is 5 min and the maximum is 1440 min (one day).

Usage

For FQDNs, DNS results (IP addresses) can change. DNS queries for FQDNs are performed every 24 hours by default. Use this command to control the DNS refresh period. To minimize DNS lookups going onto the network, set up a DNS service on the SteelHead. Results will be cached so frequent queries will be made only for results that have a short TTL (time to live).

Example

```
amnesiac (config) # host-labels refresh-intvl 420
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show host-labels”

resolve host-labels

Forces the system to resolve host labels immediately.

Syntax

resolve host-labels

Parameters

None

Usage

RiOS resolves hostnames through a DNS server immediately after you add a new host label or after you edit an existing host label. RiOS also automatically re-resolves hostnames once daily. You can use this command to force a resolve operation instead of waiting for the daily automatic resolve operation. After this command is executed, RiOS resets the next automatic resolve to occur 24 hours (by default) later.

Example

```
amnesiac # resolve host-labels
```

Product

SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"host-label," "show host-label"

Port label commands

This section describes the port label commands.

port-label

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>	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>	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 automatically passes through traffic on commonly secure ports (for example, SSH, HTTPS, and SMTPS). For a list of secure ports, see Appendix , "SteelHead Ports."

Interactive - Contains ports that belong to the system label for interactive ports. The SteelHead automatically passes through traffic on interactive ports (for example, Telnet, TCP ECHO, remote logging, and shell). For a list of interactive ports, see Appendix , "SteelHead 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 (SteelHead Interceptor), 7570 (SteelCentral Controller for SteelHead Mobile).

FTP - Contains ports that automatically pass through traffic on FTP ports 20 and 21.

SteelFusion - Contains ports that automatically pass through traffic on SteelFusion ports 7950-7954 (data transfers), and 7970 (management). For a list of SteelFusion ports, see "SteelFusion Ports".

You can use the **port-label <name> port <port>** command to add or modify ports in a port label. For example you define port label myexample by entering:

```
(config)# port-label myexample port 2-9,14
```

If you want to add ports to the myexample port label:

```
(config)# port-label myexample port 10-20
```

If you run the **show port-label myexample** 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 myexample port 22,443,990-995,3077-3078
amnesiac (config) # show port-label myexample
Port Label: myexample
22,443,990-995,3077-3078
```

Product

SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show port-label”

FTP support commands

protocol ftp port

Configures FTP port settings.

Syntax

[no] protocol ftp port <port>

Parameters

<port>	FTP port number.

Usage

The **no** command option disables the FTP port.

Example

```
amnesiac (config) # protocol ftp port 2243
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ftp”

protocol ftp port enable

Enables FTP port settings.

Syntax

[no] protocol ftp port <port> enable

Parameters

<port>	FTP port.

Usage

The **no** command option disables the FTP port.

Example

```
amnesiac (config) # protocol ftp port 2243 enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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 554.
- MAPI 2007 encrypted traffic optimization authentication. For details, see "MAPI support commands" on page 598.

domain cancel-event

Cancels domain action.

Syntax

domain cancel-event

Parameters

None

Example

```
amnesiac (config) # domain cancel-event
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show domain"

domain check

Configures the system to require a domain check upon startup.

Syntax

[no] domain check

Parameters

None

Example

```
amnesiac (config) # domain check
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show domain"

domain join

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>	Specifies the domain of which to make the SteelHead a member of. Typically, this is your company domain name. RiOS supports Windows 2000 or later domains.
login <login>	Specifies 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>	Specifies 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>	Specifies the organization name (for example, the company name).
join-type	Specifies the join account type in which the server-side SteelHead 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** - Specifies Active Directory integrated mode for Windows 2008 and later. ▪ **win2k3-mode** - Specifies 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>	Specifies 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>	Specifies 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 can join a Windows domain or local workgroup. You configure the SteelHead 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 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.

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 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. As part of the configuration, the data volume and ACLs from the origin-file server are copied to the SteelHead.

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 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, 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.

For details about domains and PFS, see the *SteelHead User Guide* and the *SteelHead Deployment Guide*.

Example

```
amnesiac (config) # domain join domain-name signing.test login admin password mypassword dc-list
mytestdc1
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“domain rejoin,” “show domain”

domain leave

Enables the system to leave a domain.

Syntax

domain leave

Parameters

None

Example

```
amnesiac (config) # domain leave
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show domain"

domain rejoin

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>	Specifies 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>	Specifies the domain password. The password is not stored.
dc-list <dc-list>	Specifies 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	Specifies the join account type in which the server-side SteelHead 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** - Specifies Active Directory integrated (Windows 2008 and later). ▪ **win2k3-mode** - Specifies Active Directory integrated (Windows 2003). If you do not specify a join type, the SteelHead 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>	Specifies 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>	Specifies 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 rejoins the same domain as specified by the **domain join** command.

Example

```
amnesiac (config) # domain rejoin login admin password mypassword
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“domain join,” “show domain”

---

domain require

Configures the system to require a domain.

Syntax

[no] domain require

Parameters

None

Example

```
amnesiac (config) # domain require
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show domain”

---

domain settings

Configures domain settings.

Syntax

[no] domain settings {dc-list <dc-list> | default-domain | kerberos {enctype [aes128] [aes256] [arcfour] | realm <realm-name> kdc-list <list>} | log-level <0-10> | max-log-size <kilobytes>} | no-ipv6-lookups| pwd-refresh-int <no-of-days>}

Parameters

dc-list <dc-list>	Specifies a list of domain controller names, separated by commas.
default-domain	Use the default domain if no other domain is configured.
kerberos enctype [aes128] [aes256] [arcfour]	Specifies the Kerberos encryption type. The following encryption types can be specified: ▪ **aes128** - specifies the aes128-cts-hmac-sha1-96 cipher ▪ **aes256** - specifies the aes256-cts-hmac-sha1-96 cipher ▪ **arcfour** - specifies the arcfour-hmac-md5 cipher Entering no encryption type removes the existing encryption type.
kerberos realm <realm-name> kdc-list <list>	Specifies Kerberos configuration settings such as the realm and the key distribution center (KDC) list. The KDC is part of the Windows domain controller and provides the authentication service and the ticket-granting service. Clients and servers trust KDCs to maintain shared keys and construct properly encrypted tickets granting clients access to services.
log-level <0-10>	Specifies the level of detail for the log. The **log-level 10** option provides the most debug messages related to domain authentication. Use this level to collect debug-level messages when troubleshooting a problem. Increasing the log level can result in dropped connections or an authentication time out.
max-log-size <kilobytes>	Specifies the maximum size of the log file. This setting increases the buffer to hold domain authentication debug messages.
no-ipv6-lookups	Disable IPv6 lookups. When enabled, this setting prevents unnecessary IPv6 lookups between the server-side SteelHead and the DNS server.
pwd-refresh-int <no-of-days>	Specifies the password refresh interval in number of days.

Usage

The SteelHead rejoins the same domain as specified by the **domain join** command. The **no** version of the command disables the domain setting.

Example

```
amnesiac (config) # domain settings kerberos realm test.auth kdc-list dc1,dc2,dc3
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“domain join,” “show domain”

protocol domain-auth encrypt-upgd

Changes the encryption algorithm for all service account passwords from Data Encryption Standard (DES) to Advanced Encryption Standard (AES).

Syntax

protocol domain-auth encrypt-upgd

Parameters

None

Usage

AES encryption adopts key lengths up to 256 bits, enhancing security and compliance capabilities.

Run this command in SteelHead 9.8.0 or later to enable AES for all existing service account passwords. You do not need to enable AES again for subsequent upgrades to later versions.

If you downgrade to SteelHead 9.7.0 or earlier, delete all service account users and add them again to revert to DES encryption.

This setting is disabled by default. Once enabled, you cannot disable AES.

Example

```
protocol domain-auth encrypt-upgd
```

Product

SteelHead CX, SteelHead EX, SteelHead-c, SteelHead-v

workgroup account add

Adds a local user to the local workgroup.

Syntax

workgroup account add user-name <local-user> password <password>

Parameters

user-name <local-user>	Specifies a local username for the Local Workgroup.
password <password>	Specifies a local password for the Local Workgroup.

Example

```
amnesiac (config) # workgroup account add user-name myuser password mypass
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show workgroup account,” “show workgroup configuration,” “show workgroup status”

workgroup account modify

Modifies a local user settings for the local workgroup.

Syntax

workgroup account modify username <local-user> password <password>

Parameters

username <local-user>	Specifies a local username for the Local Workgroup.
password <password>	Specifies a local password for the Local Workgroup.

Example

```
amnesiac (config) # workgroup account modify username myuser password userpass
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show workgroup account,” “show workgroup configuration,” “show workgroup status”

workgroup account remove

Removes a local user from the local workgroup.

Syntax

workgroup account remove username <local-user> password <password>

Parameters

username <local-user>	Specifies a local username for the domain.
password <password>	Specifies a local password for the domain.

Example

```
amnesiac (config) # workgroup account remove username myuser password userpass
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show workgroup account,” “show workgroup configuration,” “show workgroup status”

workgroup join

Configures the system to join a Windows local workgroup.

Syntax

workgroup join <workgroup>

Parameters

<workgroup>	Specifies the name of the Local Workgroup you want to join. If you configure in Local Workgroup mode the SteelHead does not need to join a domain. Local Workgroup accounts are used by clients when they connect to the SteelHead. **Note:** PFS, MAPI 2007, SMB signing, or SMB2/3 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, you can configure the system to join a local workgroup.

Usage

In Local Workgroup mode, you define a workgroup and add individual users that have access to the SteelHead. The SteelHead does not join a Windows domain.

Use Local Workgroup mode in environments where you do not want the SteelHead 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. The Local Workgroup account permissions might not match the permissions on the origin-file server.

Example

```
amnesiac (config) # workgroup join myworkgroup
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show workgroup account,” “show workgroup configuration,” “show workgroup status”

---

workgroup leave

Configures the system to leave a Windows workgroup.

Syntax

workgroup leave

Parameters

None

Example

```
amnesiac (config) # workgroup leave
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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 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 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

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	Adds servers to the msDS-Allowed-ToDelegateTo Active Directory attribute.
delete-server	Deletes servers from the msDS-Allowed-ToDelegateTo Active Directory attribute.
<name>	Username of the domain administrator.
adminpass <password>	Specifies the password of the domain administrator.
domain <name>	Specifies the domain name of the delegation domain.
dc <dcname>	Specifies the name of the domain controller.
service	Specifies a service: ▪ **cifs** - CIFS service ▪ **exchangeMDB** - Exchange service
serverlist <serverlist>	Specifies a list of delegation server names, separated by commas.

Usage

Use this 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol domain-auth auto-conf delegation"

protocol domain-auth auto-conf delegation domain

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	Adds servers to the msDS-Allowed-ToDelegateTo Active Directory attribute.
delete-server	Deletes servers from the msDS-Allowed-ToDelegateTo Active Directory attribute.
domain <name>	Specifies the name of the delegation domain.
dc <dcname>	Specifies the name of the domain controller.
service	Specifies a service: ▪ **cifs** - CIFS service ▪ **exchangeMDB** - Exchange service
serverlist <serverlist>	Specifies a list of delegation server names, by commas.

Usage

Use this 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol domain-auth auto-conf delegation"

protocol domain-auth auto-conf delegation setup-user

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>	Specifies the username of the domain administrator.
adminpass <password>	Specifies the password of the domain administrator.
domain <name>	Specifies the delegation domain in which you want to give the user delegation privileges, as in the following example: DELEGATION.TEST
dc <dcname>	Specifies the name of the domain controller.

Usage

This command reads the configuration of the delegation user on the SteelHead and configures the backend domain controller in Active Directory with the same settings.

This command adds privileges per the configuration on the SteelHead. For example, if autodelegation is configured on the SteelHead, 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol domain-auth auto-conf delegation”

---

protocol domain-auth auto-conf easy-auth

Enables an automated domain authentication configuration process for the server-side SteelHead.

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>	Specifies 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>	Specifies the username of the domain administrator.
adminpass <password>	Specifies the password of the domain administrator. The password is case sensitive.
join-domain <name>	Specifies the fully qualified domain name of the Active Directory domain in which to make the SteelHead a member.
dc <dc-name>	Specifies the name of the domain controller to contact.
join-type	Specifies the join account type by which the server-side SteelHead can join the Windows domain in one of the following roles: ▪ **win2k8-mode** - Specifies Active Directory integrated mode (Windows 2008 and later). ▪ **win2k3-mode** - Specifies Active Directory integrated mode (Windows 2003). This is the default setting.
short-name <name>	Specifies 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 configuration for domain authentication. By entering only one command, you can perform these steps:

- Test the DNS configuration.
- Join the server-side SteelHead 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 User Guide* and the *SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol domain-auth auto-conf easy-auth"

protocol domain-auth auto-conf replication

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>	Specifies the administrator username.
adminpass <password>	Specifies the domain administrator password.
domain <domain>	Specifies the replication domain in which you want to give the user replication privileges, as in the following example: REPLICATION.TEST
dc <dc-name>	Specifies a domain controller.

Usage

This command reads the configuration of the replication user on the SteelHead 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 auto-conf replication adminuser Administrator adminpass
password domain replication.test dc replication-dc1
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol domain-auth auto-conf replication"

protocol domain-auth configure load-balancing

Configures load-balancing settings across multiple domain controllers.

Syntax

[no] protocol domain-auth configure load-balancing [max-num-dc <number>]

Parameters

max-num-dc <number>	Specifies the maximum number of DCs to load balance across. The range is from 1 to 8. The default value is four domain controllers. Specifying a value of 1 disables the load-balancing feature.

Usage

This command enables the server-side SteelHead to discover and connect simultaneously to multiple DCs. When you use this command, the server-side SteelHead balances the traffic load across multiple DCs within the same domain. This load-balancing process helps improve the throughput of domain authentication operations and lessens the load on the joined DCs.

Statically configured DCs on the SteelHead take precedence over an automatically discovered list. You can create a static list by specifying one or more DCs on the server-side SteelHead during the join domain procedure, or by using the **domain settings dc-list** command option. If no statically configured DCs are configured, the SteelHead can automatically discover DCs after it has joined a domain by performing a DNS lookup.

This command is disabled by default. You must restart the optimization service for your changes to take effect. The **no** command option disables load balancing if it has been enabled.

Example

```
amnesiac (config) # protocol domain-auth configure load-balancing max-num-dc 6
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“domain settings,” “show protocol domain-auth load-balancing configuration,” “show protocol domain-auth configure load-balancing”

protocol domain-auth test authentication

Attempts to authenticate the user to the joined domain controller.

Syntax

protocol domain-auth test authentication username <username> password <password> [domain <domain> | shortdom <shortdom>]

Parameters

username <username>	Specifies the username. The maximum length is 20 characters. The username cannot contain any of the following characters: / \ [ ] : ; | = , + * ? < > @ " **Note:** The system translates the username into uppercase to match the registered server realm information.
password <password>	Specifies a password.
domain <domain>	Specifies the fully qualified domain name.
shortdom <shortdom>	Specifies the short domain name.

Usage

This 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 username administrator password
myzy294pass5 domain il-vcs44-domain.test
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol domain-auth test authentication”

protocol domain-auth test delegation server-privs

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>	Specifies the delegation domain in which you want to make the delegate user a trusted member, as in the following example: `SIGNING.TEST`
server <server>	Specifies a delegate server hostname.
server-ip <server-ip>	Specifies the delegate server IP address.
service	Specifies a service: ▪ **cifs** - CIFS service ▪ **exchangeMDB** - Exchange service
enduser <enduser>	Specifies the end username 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 and the AD environment must have correct privileges to obtain Kerberos tickets for the CIFS or exchange server and perform the subsequent authentication.

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol domain-auth test delegation server-privs”

protocol domain-auth test delegation setup

Tests the delegation user authentication setup.

Syntax

protocol domain-auth test delegation setup domain <domain> dc <dc-name>

Parameters

domain <domain>	Specifies 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>	Specifies a domain controller.

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol domain-auth test delegation setup”

protocol domain-auth test dns

Tests SteelHead DNS settings.

Syntax

protocol domain-auth test dns join-domain <domain>

Parameters

None

Parameters

join-domain <domain>	Specifies the FQDN of the join domain: `JOIN.TEST`

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol domain-auth test dns”

protocol domain-auth test join

Checks to determine whether the SteelHead is joined to the domain.

Syntax

protocol domain-auth test join

Parameters

None

Usage

This command tests whether the domain join configuration of the SteelHead is valid on the backend domain controller(s) in Active Directory.

Example

```
amnesiac (config) # protocol domain-auth test join
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol domain-auth test join”

protocol domain-auth test replication prp

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>	Specifies the replication domain: `REPLICATION.TEST`
dc <dcname>	Specifies the name of the domain controller.
rserver <rserver>	Specifies the server account to replicate.

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol domain-auth test replication prp”

protocol domain-auth test replication try-repl

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>	Specifies the replication domain in which you want to make the replication user a trusted member, as in the following example: `REPLICATION.TEST`
shortdom <shortdom>	Specifies the short domain name.
rserver <rserver>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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 User Guide* and “CIFS prepopulation support commands”.

ip fqdn override

Sets the fully qualified domain name.

Syntax

[no] ip fqdn override <domain-name>

Parameters

<domain-name>	Specifies 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

Controller, SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show domain”

protocol cifs applock enable

Enables the CIFS application lock mechanism. RiOS 5.5.x or later 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. This feature is enabled by default.

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. The client-side SteelHead must be running RiOS 5.5 or later.

Example

```
amnesiac (config) # protocol cifs applock enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs applock”

protocol cifs clear-read-resp enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs”

protocol cifs disable write optimization

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 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.

If you do not disable write-through, the SteelHead acknowledges writes before they are fully committed to disk, to speed up the write operation. The SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs”

---

protocol cifs dw-throttling enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs”

protocol cifs enable

Enables CIFS optimization. CIFS optimization is enabled by default.

Syntax

[no] protocol cifs enable

Parameters

None

Usage

RiOS 5.5x and later includes settings to optimize Microsoft Office and CIFS traffic with SMB signing enabled.

RiOS 6.0 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.

Note: Latency optimization must be enabled (or disabled) on both SteelHeads.

Example

```
amnesiac (config) # protocol cifs enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs”

protocol cifs ext-dir-cache enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol cifs ext-dir-cache," "protocol cifs enable"

protocol cifs mac oplock enable

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 only optimizes data where exclusive access is available (in other words, when locks are granted). When an oplock is not available, the SteelHead 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, SteelHeads 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show prepop"

protocol cifs nosupport

Sets a specified OS as unsupported for optimization.

Syntax

protocol cifs nosupport {client | server} {add | remove} <os-name>

Parameters

client	Disables OS support on the client.
server	Disables OS support on the server.
add	Adds OS support from the specified location.
remove	Removes OS support from the specified location.
<os-name>	OS type: **longhorn, vista, win2k3, winxp, win2k, win98, wnt4, wnt3, winunk, emc, mac, macunk, linux, novell, samba, snap, unix, bsd, ibmas400**

Example

```
amnesiac (config) # protocol cifs nosupport client add win2k
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol cifs nosupport client," "show protocol cifs nosupport server"

---

protocol cifs oopen enable

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 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 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, SteelHeads 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 or if it does not go through a SteelHead (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 559.

The **no** command option disables CIFS overlapping opens.

Example

```
amnesiac (config) # protocol cifs oopen enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol cifs oopen"

---

protocol cifs oopen extension

Configures file extensions to include or exclude from overlapping open optimization.

Syntax

protocol cifs oopen extension {add <extension> [setting-always <policy>] | modify <extension> setting <policy> | remove <extension>}

Parameters

add <extension>	Specifies a list of file extensions to include in overlapping opens optimization.
setting-always <policy>	Specifies 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 <extension> setting <policy>	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 <extension>	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 optimizes data to which exclusive access is available (in other words, when locks are granted). When an oplock is not available, the SteelHead 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 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 or if it does not go through a SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs oopen”

protocol cifs oopen policy

Changes the default CIFS overlapping open policy.

Syntax

[no] protocol cifs oopen policy {allow | deny}

Parameters

allow	Allows CIFS overlapping open policy.
deny	Denies CIFS overlapping open policy.

Usage

The default policy is to deny overlapping open optimization.

Example

```
amnesiac (config) # protocol cifs oopen policy allow
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs oopen”

protocol cifs secure-sig-opt enable

Enables Security Signature negotiations between the 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 SteelHeads).

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. domain controllers default to **Required**.

If your deployment requires SMB signing, see the *SteelHead User 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs”

protocol cifs smb signing enable

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 5.5 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 User Guide*.

You can enable the RiOS SMB signing feature on a server-side SteelHead to alleviate latency in file access with CIFS acceleration while maintaining message security signatures. With SMB signing on, the SteelHead 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 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 6.0 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 has joined. RiOS 6.1 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 and any configured servers participating in the signed session. The client-side SteelHead uses NTLM and will negotiate down to NTLM from Kerberos if supported. The client-side SteelHead does not use Kerberos.

Prerequisites

- With RiOS SMB signing enabled, SteelHeads sign the traffic between the client and the client-side SteelHead and between the server and the server-side SteelHead. The traffic is not signed between the SteelHeads, but the SteelHeads implement their own integrity mechanisms. For maximum security, Riverbed recommends that you use IPSec encryption to secure the traffic between the SteelHeads.
- 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.

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 User 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 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 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 is routed to the DNS and the domain controller.
5. Verify the DNS settings:

- You must be able to ping the server-side SteelHead, by name, from a CIFS server joined to the same domain that the server-side SteelHead will join. If you cannot, create an entry in the DNS server for the server-side SteelHead.
- You must be able to ping the domain controller, by name, whose domain the server-side SteelHead 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 539.
7. If you configured SMB signing in delegation mode, set up the domain controller and SPN. For detailed information, see the *SteelHead User 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 User Guide*.
9. If you configured SMB signing in delegation mode, add delegate users on the SteelHead.
10. Enable SMB signing on the server-side SteelHeads.

For detailed procedures, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # protocol cifs smb signing enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol cifs smb signing status"

---

protocol cifs smb signing mode-type

Configures SMB signing mode as either transparent or delegation.

Syntax

[no] protocol cifs smb signing mode-type <mode>

Parameters

<mode>	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 6.0 and later; however, if you enabled SMB signing in RiOS 5.5 and upgraded to 6.0 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 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 5.5.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 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs smb signing status,” “Windows domain authentication delegation commands”

protocol cifs smb signing native-krb enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs smb signing status,” “Windows domain authentication delegation commands”

protocol cifs smb signing ntlm-bypass enable

Enables the pass through of NTLM connections during SMB signing.

Syntax

[no] protocol cifs smb signing ntlm-bypass enable

Parameters

None

Usage

This command supports customers who need to comply with Security Technical Implementation Guides (STIGs) SRG-NET-000521-ALG-000002 that require that NTLM authenticated traffic be bypassed. STIG compliance is provided on a per-protocol level so you can selectively choose which protocol needs to run in STIG compliance mode.

This command is disabled by default. You configure this command on the server-side SteelHead and it requires a service restart.

The **no** command option disables NTLM pass through of connections.

Example

```
amnesiac (config) # protocol cifs smb signing ntlm-bypass enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs smb signing status”

protocol cifs smbv1-mode enable

Enables SMBv1 backward compatibility mode, which allows a SteelHead 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. Use this command 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 SteelHeads 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:

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs”

protocol cifs spoolss enable

Enables CIFS print-spool subsystem optimization.

Syntax

[**no**] **protocol cifs spoolss enable**

Parameters

None

Usage

This command 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 command requires an optimization service restart.

Example

```
amnesiac (config) # protocol cifs spoolss enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs spoolss”

protocol smb2 caseless enable

Enables case insensitive behavior in the processing of path names.

Syntax

[**no**] **protocol smb2 caseless enable**

Usage

SMB2 is a case-insensitive protocol and the SteelHead SMB2/3 implementation is case sensitive. This implementation can cause inconsistent behavior because some applications change the case of the path name and these path names could be treated as different objects rather than the same object. This command enables case-insensitive comparison of path names.

Only the ASCII character set is supported. When this command is enabled, do not use non-ASCII characters in the path names because this might result in undefined behavior. If you need to use non-ASCII characters in the path names, disable this command if it has been enabled.

This command is disabled by default. You only need to configure it on the client-side SteelHead and must restart the optimization service after running this command. Both client-side and server-side SteelHeads must be running version 9.5 or later. For details on SMB2, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # protocol smb2 caseless enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol smb2"

---

protocol smb2 dfs enable

Configures the SteelHead to optimize Distributed File System (DFS) shares.

Syntax

[no] protocol smb2 dfs enable

Usage

DFS is a technology Microsoft uses for achieving high availability and logical distribution of files. DFS runs over SMB/SMB2 and allows clients to access files from secondary servers if the primary server goes down or from the server nearest to the client making the request. The default behavior is to forward the traffic with DFS capability to the server without providing latency optimization to the connections.

You configure this command on the client-side SteelHead and both client-side and server-side SteelHeads must be running RiOS 9.5 or later. You must enable SMB2/3 optimization before configuring this command.

This command is disabled by default. Restart the optimization service after running this command. For details on SMB2/3, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # protocol smb2 dfs enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol smb2"

---

protocol smb2 enable

Enables optimization of SMB2 traffic for native SMB2 clients and servers.

Syntax

[no] protocol smb2 enable

Usage

You must restart the optimization service after running this command. For details on SMB2, see the *SteelHead User Guide* and "protocol cifs smb signing enable" on page 561.

Example

```
amnesiac (config) # protocol smb2 enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol smb2”

protocol smb2 signing enable

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 User Guide* and “protocol cifs smb signing enable” on page 561.

When upgrading from RiOS 6.1 to 6.5 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol cifs smb signing enable,” “protocol cifs smbv1-mode enable,” “show protocol smb2”

protocol smb2 signing mode-type

Configures the RiOS SMB2 signing mode.

Syntax

[no] protocol smb2 signing mode-type {transparent | delegation}

Parameters

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 5.5 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 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 5.5.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 and Kerberos between the server-side SteelHead and the server.

Usage

You can enable the RiOS SMB2 signing feature on a server-side SteelHead 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.

By default, RiOS SMB2 signing is disabled.

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 User Guide*.

Example

```
amnesiac (config) # protocol smb2 signing mode-type transparent
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol cifs smb signing status,” “**protocol domain-auth delegation auto-mode enable,**” “Windows domain authentication delegation commands”

protocol smb2 signing native-krb downgrade enable

Enables an SMB2 signing downgrade.

Syntax

[**no**] **protocol smb2 signing native-krb downgrade enable**

Usage

You must enable SMB2 and join a domain before enabling SMB2 signing. This command enables an SMB2 signing downgrade after an end-to-end Kerberos failure.

For details on SMB2, see the *SteelHead User Guide* and “protocol cifs smb signing enable” on page 561.

Example

```
amnesiac (config) # protocol smb2 signing native-krb downgrade enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol cifs smb signing enable," "protocol cifs smbv1-mode enable," "show protocol smb2"

---

protocol smb2 signing native-krb enable

Enables end-to-end Kerberos for SMB2 signing.

Syntax

[no] protocol smb2 signing native-krb enable

Usage

You must enable SMB2 and join a domain before enabling SMB2 signing. This command enables SMB2/3 signing with end-to-end authentication using Kerberos. The server-side SteelHead uses Kerberos to authenticate users.

For details on SMB2, see the *SteelHead User Guide* and "protocol cifs smb signing enable" on page 561.

Example

```
amnesiac (config) # protocol smb2 signing native-krb enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol cifs smb signing enable," "protocol cifs smbv1-mode enable," "show protocol smb2"

---

protocol smb2 signing ntlm-bypass enable

Enables the pass through of NTLM connections during SMB2 signing.

Syntax

[no] protocol smb2 signing ntlm-bypass enable

Usage

You must enable SMB2 and join a domain before enabling SMB2 signing. For details on SMB2, see the *SteelHead User Guide* and "protocol cifs smb signing enable" on page 561.

This command supports customers who need to comply with Security Technical Implementation Guides (STIGs) SRG-NET-000521-ALG-000002 that require that NTLM authenticated traffic be bypassed. STIG compliance is provided on a per-protocol level so you can selectively choose which protocol needs to run in STIG compliance mode.

This command is disabled by default. You configure this command on the server-side SteelHead and it requires a service restart.

The **no** command option disables NTLM pass through of connections during SMB2 signing.

Example

```
amnesiac (config) # protocol smb2 signing ntlm-bypass enable
amnesiac (config) # protocol smb2 signing enable
amnesiac (config) # service restart
```

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol cifs smb signing status"

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

protocol smb2 strip-8dot3

Enables the removal of short names from the find data.

Syntax

[no] protocol smb2 strip-8dot3

Parameters

None

Usage

Use this 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 to remove the short names from the find data.

You must enable SMB2 before using this command.

For details on SMB2, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # protocol smb2 enable
amnesiac (config) # protocol smb2 strip-8dot3
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol smb2”

protocol smb2 smb3-support enable

Enables optimization of SMB3 traffic.

Syntax

[no] protocol smb2 smb3-support enable

Usage

RiOS 8.5 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 User Guide*.

Example

```
amnesiac (config) # protocol smb2 enable
amnesiac (config) # protocol smb2 smb3-support enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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

Enables CIFS prepopulation.

Syntax

[no] prepop enable

Parameters

None

Usage

The prepopulation operation effectively performs the first SteelHead read of the data on the prepopulation share. Subsequently, the SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show prepop”

---

prepop share cancel-event

Cancels CIFS prepopulation synchronization and verification for a share.

Syntax

prepop share cancel-event remote-path <remote-path>

Parameters

remote-path <remote-path>	Remote path of a share for which to cancel events. Use the format `'\\server\share'`.

Example

```
amnesiac (config) # prepop share cancel-event remote-path '\\10.11.61.66\backup'
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show prepop”

prepop share configure

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>	Specifies the remote path of the share to be synchronized. Use the format `'\\server\share'`.
server-account <login>	Specifies the login, if any, required to access the share.
server-password <password>	Specifies the corresponding password, if any, to access the share.
interval <number-of-seconds>	Specifies the number of seconds for the synchronization interval.
comment "<text-comment>"	Describes the share, for administrative purposes.
start-time <date and time>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show prepop”

prepop share dry-run

Enables a dry run of a share synchronization.

Syntax

prepop share dry-run remote-path <remote-path>

Parameters

remote-path <remote-path>	Specifies the remote path of the share. Use the format `'\\server\share'`.

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show prepop log dry-run”

prepop share manual-sync

Performs manual synchronization for a remote share.

Syntax

prepop share manual-sync remote-path <remote-path>

Parameters

remote-path <remote-path>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show prepop”

prepop share modify

Modifies prepopulation settings for a share.

Syntax

prepop share modify {remote-path <remote-path> server-account <login> server-password <password> interval <seconds> comment "<text-comment>" | start-time <date-and-time> | max-duration <seconds> | max-sync-size <bytes> | syncing <true | false>}

Parameters

remote-path <remote-path>	Specifies the remote path of the share to be synchronized. Use the format `'\\server\share'`.
server-account <login>	Specifies the login, if any, required to access the share.
server-password <password>	Specifies the corresponding password, if any, to access the share.
interval <seconds>	Specifies 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>	Specifies a start time for synchronization in the format `'yyyy/mm/dd hh:mm:ss'`.
max-duration <seconds>	Specifies the maximum duration, in seconds, for the synchronization to occur.
max-sync-size <bytes>	Specifies 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	Enables synchronization of a share.
syncing false	Disables synchronization of a share.

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show prepop”

prepop share policy

Creates a policy with the specified name.

Syntax

[no] prepop share policy remote-path <remote-path> policy-name <policy-name> [rule <rule>]

Parameters

remote-path <remote-path>	Specifies the remote path of the share. Use the format `'\\server\share'`.
policy-name <policy-name>	Specifies the policy name.
<rule>	Specifies the policy rule index.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show prepop share policy”

prepop share policy access-time

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>	Specifies the remote path of the share. Use the format `'\\server\share'`.
policy-name <policy-name>	Specifies a policy name.
sync-relative <time>	Specifies the time relative to synchronization, in the following format: `'hh:mm:ss'`
time <time>	Specifies the reference time in the following format: `'yyyy/mm/dd hh:mm:ss'`
compare-op	Specifies the compare operator: ▪ **before** - Before the specified time ▪ **after** - After the specified time

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show prepop share policy”

prepop share policy create-time

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>	Specifies the remote path of the share. Use the format `'\\server\share'`.
policy-name <policy-name>	Specifies a policy name.
sync-relative <time>	Specifies the time relative to synchronization, in the following format: `'hh:mm:ss'`
time <time>	Specifies reference time in the following format: `'yyyy/mm/dd hh:mm:ss'`
compare-op	Specifies the compare operator: ▪ **before** - Before the specified time ▪ **after** - After the specified time

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show prepop share policy”

prepop share policy file-name

Adds a filename 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>	Specifies the remote path of the share. Use the format `'\\server\share'`.
policy-name <policy-name>	Specifies a policy name.
<file-name>	Specifies a filename or a list of filenames separated by semicolons. The filename can contain a wildcard character: for example, *001.doc; *pdf.
compare-op	Specifies the compare operator: ▪ **matches** - Matches the filename. ▪ **not-matches** - Does not match the filename.

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show prepop share policy”

prepop share policy file-size

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>	Specifies the remote path of the share. Use the format `'\\server\share'`.
policy-name <policy-name>	Specifies a policy name.
<file-size>	Specifies a file size.
compare-op	Specifies the compare operator: ▪ **less** - Less than or equal to the file size ▪ **greater** - Greater than or equal to the file size

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show prepop"

prepop share policy write-time

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>	Specifies the remote path of the share. Use the format: `'\\server\share'`.
policy-name <policy-name>	Specifies a policy name.
sync-relative <time>	Specifies the time relative to synchronization, in the following format: `'hh:mm:ss'`
time <time>	Specifies the reference time in the following format: `'yyyy/mm/dd hh:mm:ss'`
compare-op	Specifies the compare operator: ▪ **before** - Before the specified time ▪ **after** - After the specified time

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show prepop share policy"

prepop share snapshot

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>	Specifies the remote path of the share. Use the format `'\\server\share'`.
status true	Enables synchronization from the latest share snapshot.
status false	Disables synchronization from the latest share snapshot.

Usage

This command enables or disables synchronization from the latest snapshot of the share needing prepopulation when the 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show prepop”

protocol cifs prepop enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show prepop”

HTTP support commands

protocol http auto-config clear-stats

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http”

protocol http auto-config enable

Configures an optimal HTTP automatic configuration scheme per host.

Syntax

[no] protocol http auto-config enable

Parameters

None

Usage

HTTP automatic configuration 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http”

protocol http auto-config selection

Configures the per-host autoconfiguration selection settings.

Syntax

[no] protocol http auto-config selection {obj-pref-table | parse-prefetch |url-learning | reuse-auth | stream-split | strip-auth-hdr | gratuitous-401| force-nego-ntlm| strip-compress |insert-cookie | insrt-keep-aliv | FPSE | WebDAV | FSSHTTP}

Parameters

obj-pref-table	Enables 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 responds to these IMS checks and HTTP requests, reducing round trips across the WAN.
parse-prefetch	Enables Parse and Prefetch, which parses the base HTML page received from the server and prefetches any embedded objects to the client-side SteelHead. 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 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	Enables 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 keepalives), 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	Allows 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.
stream-split	Enables the client-side SteelHead to split Silverlight smooth streaming, Adobe Flash HTTP dynamic streams, and Apple HTTP Live Streaming (HLS). This control includes support for Microsoft Silverlight video and Silverlight extensions support on Internet Information 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 control. For details, see the *SteelHead Deployment Guide - Protocols*.

strip-auth-hdr	Removes 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	Prevents a WAN round trip by issuing the first 401 containing the realm choices from the client-side SteelHead. We recommend 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	Forces NTLM In the case of negotiated Kerberos and NTLM authentication. 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. We recommend enabling **strip-auth-hdr** with this option. This setting is disabled by default.
strip-compress	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 data-reduction algorithms. Specify **yes** to enable this feature; specify **no** to disable it. This setting is enabled by default.
insert-cookie	Adds a cookie to HTTP applications that do not already have one. HTTP applications frequently use cookies to monitor sessions. The SteelHead uses cookies to distinguish one user session from another. If an HTTP application does not use cookies, the client SteelHead inserts one so that it can track requests from the same client. By default, this setting is disabled.
insrt-keep-aliv	Uses 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	Enables or disables SharePoint Front Page Server Extensions Protocol (FPSE) on a subnet or hostname. RiOS 8.5 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	Enables or disables 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	Enables or disables 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http auto-config selection”

protocol http enable

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 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 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 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 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 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 removes unfetchable objects from the URL Learning Knowledge Base.
- **Object Prefetch Table** - The SteelHead stores object prefetches from HTTP GET requests for cascading style sheets, static images, and Java scripts. This helps the client-side SteelHead 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 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 User Guide*.

The **no** command option disables HTTP module support.

Example

```
amnesiac (config) # protocol http enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http”

protocol http metadata-resp extension

Specifies the object extensions to add. By default, the SteelHead prefetches .css, .gif, .jpg, .js, and .png.

Syntax

[no] protocol http metadata-resp extension <extension>

Parameters

<extension>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http”

protocol http metadata-resp max-time

Sets the maximum number of seconds that HTTP optimization stores the object information.

Syntax

[no] protocol http metadata-resp max-time <seconds>

Parameters

<seconds>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http”

protocol http metadata-resp min-time

Sets the minimum number of seconds that HTTP optimization stores the object information.

Syntax

[no] protocol http metadata-resp min-time <seconds>

Parameters

<seconds>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http”

protocol http metadata-resp mode

Configures the object caching mode for the HTTP optimization cache.

Syntax

[no] protocol http metadata-resp mode {all | use-list | none}

Parameters

all	Caches all allowable objects.
use-list	Caches objects matching the extension list.
none	Does 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http”

protocol http native-krb enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol http"

protocol http prefetch

Specifies 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>	Specifies a file extension to add to the list of file types to prefetch.
tag <tag> attribute <tag-attribute>	Specifies 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 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol http"

protocol http prepop list

Adds an HTTP prepopulation list.

Syntax

[no] protocol http prepop list <list-name>

Parameters

<list-name>	HTTP prepopulation 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 trainingvideos
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http prepop,” “show protocol http prepop status”

protocol http prepop list cancel

Cancels a prepopulation operation on the specified list.

Syntax

protocol http prepop list <list-name> cancel

Parameters

<list-name>	HTTP prepopulation list name.

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol http prepop list start,” “show protocol http prepop,” “show protocol http prepop status”

protocol http prepop list start

Starts a prepopulation operation on the URLs in the specified list.

Syntax

protocol http prepop list <list-name> start

Parameters

<list-name>	HTTP prepopulation 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol http prepop list cancel," "show protocol http prepop," "show protocol http prepop status"

protocol http prepop list url

Adds a URL from the HTTP prepopulation list.

Syntax

[no] protocol http prepop list <list-name> url <url>

Parameters

<list-name>	List name.
<url>	URL to add or delete from the HTTP prepopulation list. 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 8.5 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 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http prepop,” “show protocol http prepop status”

---

protocol http prepop verify-svr-cert enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http prepop verify-svr-cert”

---

protocol http servers flush

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http”

---

protocol http server-table

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>}] [stream-split {<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>	Specifies one of the following for the HTTP server subnet: ▪ **<IPv4 network>** - IPv4 network. Use the format X.X.X.X/<0-32>. ▪ **<IPv6 network> -** IPv6 network. Use the format X:X:X: :X/<0-128>. ▪ **all-ipv4 -** All IPv4 network. ▪ **all-ipv6 -** All IPv6 network.
hostname <name>	Specifies the hostname.
hostname all	Specifies all hostnames.
obj-pref-table <yes | no>	Enables or disables 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 responds to these IMS checks and HTTP requests, reducing round trips across the WAN.
parse-prefetch <yes | no>	Enables or disables Parse and Prefetch, which parses the base HTML page received from the server and prefetches any embedded objects to the client-side SteelHead. 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 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>	Enables or disables 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 keepalives), 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>	Allows 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.

stream-split <yes | no>	Enables or disables the client-side SteelHead to split Silverlight smooth streaming, Adobe Flash HTTP dynamic streams, and Apple HTTP Live Streaming (HLS) video. This option includes support for Microsoft Silverlight video and Silverlight extensions support on Internet Information Server (IIS) version 7.5 installed on 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 Deployment Guide - Protocols.*
strip-auth-hdr <yes | no>	Removes 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>	Prevents a WAN round trip by issuing the first 401 containing the realm choices from the client-side SteelHead. 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 data-reduction algorithms. This setting is enabled by default.
insert-cookie <yes | no>	Adds a cookie to HTTP applications that do not already have one. HTTP applications frequently use cookies to monitor sessions. The SteelHead uses cookies to distinguish one user session from another. If an HTTP application does not use cookies, the client SteelHead 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>	Uses 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>	Enables or disables SharePoint Front Page Server Extensions Protocol (FPSE) on a subnet or hostname. RiOS 8.5 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>	Enables or disables 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http,” “show protocol http server-table”

protocol http space-in-uri enable

Enables HTTP to parse the space in the URI.

Syntax

[no] protocol http space-in-uri enable

Parameters

None

Usage

The **no** command option disallows HTTP to parse the space in the URI.

Example

```
amnesiac (config) # protocol http space-in-uri enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol http”

Oracle forms support commands

protocol oracle-forms enable

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 User Guide*.

The SteelHead 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 5.5.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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol oracle-forms http-enable," "show protocol oracle-forms"

---

protocol oracle-forms http-enable

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 User 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol oracle-forms"

MAPI support commands

This section describes the MAPI support commands.

admission control mapi enable

Enables MAPI over HTTP admission control support.

Syntax

[no] admission control mapi enable

Parameters

None

Usage

This command enables the SteelHead appliances to process MAPI over HTTP traffic when SteelHeads enter admission control status. These memory enhancements allow MAPI over HTTP optimization to degrade gracefully as the SteelHead nears capacity. MAPI over HTTP optimization is maintained for as many users as possible without pushing the SteelHead over capacity.

MAPI over HTTP admission control is disabled by default.

This command only affects the SteelHead where the command is executed. We recommend enabling MAPI admission control on both the client and server-side SteelHeads.

Example

```
amnesiac (config) # admission control mapi enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show admission”

protocol mapi enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol mapi”

protocol mapi encrypted delegation enable

Provides encrypted MAPI optimization using the Kerberos delegation facility.

Syntax

[no] protocol mapi encrypted delegation enable

Parameters

None

Usage

Enable this command if you are encrypting MAPI traffic for Windows 7 or earlier client versions. Both the server-side and client-side SteelHeads must be running RiOS 6.1.

In RiOS 6.1, 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 User Guide*.

Delegation mode requires additional configuration. For details, see “Windows domain authentication delegation commands” on page 645.

You must restart the optimization service for your changes to take effect.

The **no** command option disables encrypted MAPI optimization.

Example

```
amnesiac (config) # protocol mapi encrypted delegation enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“Windows domain authentication delegation commands”

protocol mapi encrypted enable

Enables encrypted MAPI RPC traffic optimization between Outlook and Exchange.

Syntax

[no] protocol mapi encrypted enable

Parameters

None

Usage

The basic steps to enable encrypted optimization are:

- The server-side SteelHead 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.
- Restart the SteelHead.

Notes:

- When this option and MAPI Exchange 2007 acceleration are enabled on either SteelHead, MAPI Exchange 2007 acceleration remains in effect for unencrypted connections.
- By default, this feature supports NTLM authentication.
- The SteelHead 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.

By default, this option is disabled. The **no** command option disables this option if it has been enabled.

Example

```
amnesiac (config) # protocol mapi encrypted enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol mapi”

---

protocol mapi encrypted multi-auth enable

Enables multiple authentication context support for encrypted MAPI authorization traffic.

Syntax

[**no**] **protocol mapi encrypted multi-auth enable**

Parameters

None

Usage

MAPI allows multiple protocols to run over an individual TCP session and a TCP connection with the same TCP source and destination port.

You must restart the optimization service for your changes to take effect.

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol mapi encrypted multi-auth enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol mapi”

protocol mapi encrypted native-krb enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol mapi”

protocol mapi encrypted ntlm-auth enable

Enables NTLM authorization for encrypted MAPI RPC traffic between Outlook and Exchange.

Syntax

[no] protocol mapi encrypted ntlm-auth enable

Parameters

None

Usage

You must restart the optimization service for your changes to take effect.

This command is enabled by default. The **no** command option disables this option.

Example

```
amnesiac (config) # no protocol mapi encrypted ntlm-auth enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol mapi”

protocol mapi encrypted ntlm-bypass enable

Enables the bypass of NTLM-authenticated encrypted MAPI traffic.

Syntax

[no] protocol mapi encrypted ntlm-bypass enable

Usage

This command supports customers who need to comply with Security Technical Implementation Guides (STIGs) SRG-NET-000521-ALG-000002 that require that NTLM authenticated traffic be bypassed. When NTLM authentication is used on an encrypted MAPI connection, the connection is bypassed and no optimization is performed.

STIG compliance is provided on a per-protocol level so you can selectively choose which protocols need to run in STIG compliance mode.

This command is disabled by default. You configure this command on the server-side SteelHead and it requires a service restart when enabled or disabled.

The **no** command option disables the bypass of NTLM-authenticated traffic if it has been enabled.

Example

```
amnesiac (config) # protocol mapi encrypted ntlm-bypass enable
amnesiac (config) # service restart
```

Related Commands

"show protocol mapi"

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

---

protocol mapi multi-context enable

Enables multiple context support for MAPI traffic.

Syntax

[**no**] **protocol mapi multi-context enable**

Parameters

None

Usage

MAPI allows multiple protocols to run over an individual TCP session and a TCP connection with the same TCP source and destination port. *Multiple context* is when a client requests a new protocol over the same TCP connection. Enabling multiple context support for MAPI minimizes the number of TCP connections consumed per client. RiOS 9.0 and later supports multiple context. Riverbed recommends that you enable this feature in an Exchange 2013 environment. Enabling this feature does not have any adverse effect on nonmultiple context traffic. For more information, see the *SteelHead Deployment Guide - Protocols*.

You must restart the optimization service for your changes to take effect.

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol mapi multi-context enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol mapi encrypted multi-auth enable," "protocol mapi outlook-anywhr multi-context enable," "show protocol mapi"

protocol mapi outlook-anywhr auto-detect

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 User Guide*.

Example

```
amnesiac (config) # protocol mapi outlook-anywhr auto-detect
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol mapi”

protocol mapi outlook-anywhr enable

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 command, 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. For more information on Outlook Anywhere, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # protocol mapi outlook-anywhr enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol http enable," "show protocol mapi"

protocol mapi outlook-anywhr ex365domain

Configures a list of DNS domain names of the Exchange 365 server for Outlook Anywhere.

Syntax

[no] protocol mapi outlook-anywhr ex365domain <domain>

Parameters

<domain>	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 User Guide*.

Example

```
amnesiac (config) # protocol mapi outlook-anywhr ".office365.com,.outlook.com"
```

Product

SteelHead CX, SteelHead EX SteelHead-v, SteelHead-c

Related Commands

"show protocol mapi," "protocol http enable"

protocol mapi outlook-anywhr multi-context enable

Enables multiple context support for Outlook Anywhere traffic.

Syntax

[no] protocol mapi outlook-anywhr multi-context enable

Parameters

None

Usage

Both MAPI and Outlook Anywhere allows multiple protocols to run over an individual TCP session and a TCP connection with the same TCP source and destination port. *Multiple context* is when a client requests a new protocol over the same TCP connection. Enabling multiple context support for Outlook Anywhere traffic minimizes the number of TCP connections consumed per client. RiOS 9.0 and later supports multiple context. Riverbed recommends that you enable this feature in an Exchange 2013 environment. Enabling this feature does not have any adverse effect on non-multiple context traffic. For more information, see the *SteelHead Deployment Guide - Protocols*.

You must restart the optimization service for your changes to take effect.

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol mapi outlook-anywhr multi-context enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol mapi encrypted multi-auth enable,” “protocol mapi multi-context enable,” “show protocol mapi”

protocol mapi port

Sets the incoming MAPI Exchange port.

Syntax

[no] protocol mapi port <port>

Parameters

<port>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol mapi”

protocol mapi port-remap enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol mapi"

protocol mapi prepop enable

Enables MAPI transparent prepopulation.

Syntax

[no] protocol mapi prepop enable

Parameters

None

Usage

This command 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol mapi," "show prepop"

protocol mapi prepop max-connections

Sets the maximum number of connections for MAPI transparent prepopulation.

Syntax

[no] protocol mapi prepop max-connections <number>

Parameters

<number>	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. The default value varies by model; for example, on a 5520 the default is 3750.

Usage

You must configure the maximum connections on both the client and server-side of the network.

The **no** command option resets max-connections to the default.

Example

```
amnesiac (config) # protocol mapi prepop max-connections 3300
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol mapi," "show prepop"

protocol mapi prepop poll-interval

Sets the polling interval for MAPI transparent prepopulation.

Syntax

[no] **protocol mapi prepop poll-interval <minutes>**

Parameters

<minutes>	Polling interval in minutes. The default value is 20.

Usage

The **no** command option resets the polling interval to the default.

Example

```
amnesiac (config) # no protocol mapi prepop poll-interval 22
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol mapi," "show prepop"

protocol mapi prepop timeout

Sets the time out period for MAPI transparent prepopulation.

Syntax

[no] **protocol mapi prepop timeout <hours>**

Parameters

<hours>	Time out period in hours.

Usage

The **no** command option resets the prepopulation time out to the default but does not disable MAPI prepopulation support.

Example

```
amnesiac (config) # no protocol mapi prepop timeout 93
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol mapi," "show prepop"

protocol mapi strip level2

Removes the MAPI Exchange DCE /RPC authentication Level 2 (Connect) data from requests on the client-side SteelHead.

Syntax

[no] protocol mapi strip level2

Parameters

None

Usage

Microsoft Outlook can use the Distributed Computing/Remote Procedure Calls (DCE/RPC) authentication level 2 (connect) on requests to send a cryptographic signature. The MAPI optimization service does not correctly handle this authentication level. This command removes the DCE/RPC authentication level-2 data from requests on the client-side SteelHead.

Example

```
amnesiac (config) # protocol mapi strip level2
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol mapi”

Exchange optimization services protocol commands

protocol eos moh enable

Enables bandwidth and latency optimization for the MAPI over HTTP transport protocol.

Syntax

[no] protocol eos moh enable

Parameters

None

Usage

MAPI over HTTP improves reliability and stability of connections by moving the transport layer to the HTTP model. Enter this command on the client-side SteelHead to enable bandwidth and latency optimization for the MAPI over HTTP transport protocol. Microsoft implemented this transport protocol in Exchange Server 2013 SP1, Outlook 2013 SP1, and added support to Outlook 2010 update (KB 2878264).

You must also create an in-path rule using the Exchange Autodetect latency optimization policy to differentiate and optimize this traffic.

For MAPI transport protocol optimization, enable SSL optimization and install the SSL server certificate for the Exchange Server on the server-side SteelHead. Both the client-side and server-side SteelHeads must be running RiOS 9.2 for MAPI over HTTP latency optimization.

If you pair a SteelHead running RiOS 9.2 with a SteelHead running 9.1, only HTTP bandwidth optimization is supported.

This command is disabled by default.

Example

```
amnesiac (config) # protocol eos moh enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“in-path rule auto-discover,” “in-path rule pass-through,” “show protocol eos”

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 these commands.

---

protocol ms-sql default-rule query-rule

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>	Specifies an MS-SQL protocol query-rule ID.
action-id <action-id>	Specifies an MS-SQL protocol query-rule action-id.
arg-offset <arg-offset>	Specifies 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 action-id 3 enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ms-sql”

---

protocol ms-sql default-rule rpc-rule

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>	Specifies an MS-SQL protocol RPC-rule ID.
action-id <action-id>	Specifies an ID that uniquely identifies a match.
arg-offset <arg-offset>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ms-sql”

protocol ms-sql enable

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 command.

The **no** command option disables SQL blade support.

Example

```
amnesiac (config) # protocol ms-sql enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ms-sql”

protocol ms-sql fetch-next enable

Enables pre-fetching requests to request the next row in MS Project. The server-side SteelHead pre-fetches sequential row results and the client-side SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ms-sql”

protocol ms-sql num-preack

Specifies the maximum number of **sp_execute** (or save project) requests to preacknowledge before waiting for a server response to be returned.

Syntax

[no] protocol ms-sql num-preack <number-preack>

Parameters

<number-preack>	Maximum number of pre-acknowledgments. The default value is 5.

Usage

You can enable pre-acknowledgment 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-acknowledgments from the server.

The **no** command option disables pre-acknowledgment.

Example

```
amnesiac (config) # protocol ms-sql num-preack 6
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ms-sql”

protocol ms-sql port

Specifies the server port to listen on for SQL requests.

Syntax

[no] protocol ms-sql port <port>

Parameters

<port>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol ms-sql"

protocol ms-sql query-act rule-id action-id num-reps

Specifies 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>	Specifies the rule identification number that uniquely identifies the rule.
action-id <action-id>	Specifies the action identification number that uniquely identifies this action within the rule.
num-reps <num-reps>	Specifies 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>	Specifies the MS-SQL cache miss policy.
allow-preack {true | false}	Specifies whether to allow the MS-SQL pre-acknowledgment (**true**) or not (**false**).
scope {sfe | cfe}	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ms-sql”

protocol ms-sql query-arg-act rule-id action-id arg-offset expr

Specifies 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>	Specifies the rule identification number that uniquely identifies the rule.
action-id <action-id>	Specifies the action identification number that uniquely identifies this action within the rule.
arg-offset <arg-offset>	Specifies the SQL query argument to be modified.
expr <expression>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ms-sql”

protocol ms-sql query-rule rule-id app-name-regex query-regex

Specifies 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>	Specifies the rule identification number that uniquely identifies the rule.
app-name-regex <app-name>	Specifies the client application name (standard string expression).
query-regex <query-regex>	Specifies a 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ms-sql”

protocol ms-sql rpc-act rule-id action-id

Specifies 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>	Specifies the rule identification number that uniquely identifies the rule.
action-id <action-id>	Specifies the action identification number that uniquely identifies this action within the rule.
num-reps <num-reps>	Specifies 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>	Specifies the MS-SQL cache miss policy.
allow-preack {true | false}	Specifies whether to allow the MS-SQL preacknowledgment (**true**) or not (**false**).
allow-prefetch {true | false}	Specifies whether to allow MS-SQL pre-fetch (**true**) or not (**false**).
scope {sfe | cfe}	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol ms-sql"

protocol ms-sql rpc-arg rule-id action-id arg-offset expr

Specifies 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> arg-offset expr <expr>

Parameters

<rule-id>	Rule identification number that uniquely identifies the rule.
<action-id>	Action identification number that uniquely identifies this action within the rule.
<expr>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol ms-sql"

protocol ms-sql rpc-arg-act rule-id arg-offset expr

Specifies an 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 identification number that uniquely identifies the rule.
<arg-offset>	RPC argument parameter.
expr <expr>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ms-sql”

protocol ms-sql rpc-rule rule-id app-name-regex

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>	Specifies the rule identification number that uniquely identifies the rule.
<app-name>	Specifies the client application name (standard string expression).
rpc-id <rpc-id>	Specifies the RPC identifier.
num-params <num-params>	Specifies the expected number of parameters in the SQL query.
rpc-query-regex <regex-match-for-rpc-query-string>	Specifies the RPC name (standard string expression).
cursor-type <cursor-type>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ms-sql”

protocol ms-sql support-app

Specifies 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>	Specifies the name of the application to be supported by the MS-SQL blade.
collation <collation>	Specifies MS-SQL protocol collation mode settings.
misc <misc>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ms-sql”

NFS support commands

protocol nfs alarm v2-v4 clear

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol nfs”

protocol nfs default server

Configures default settings for NFS servers.

Syntax

[no] protocol nfs default server {direntry-map | policy {custom | global_rw | read_only} | read-ahead {small-files | transfer-size <size>} | read-dir {optimize | read-size <size>} | threshold multiple <multiple> | write {optimize | max-data <max>}}

Parameters

direntry-map	Enables the directory entry map.
policy {custom | global_rw | read_only}	Specifies 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** - Specifies 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 SteelHeads) 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 |transfer-size <size>}	Enables read-ahead for small files; sets the transfer size in bytes.
read-dir {optimize | read-size <size>}	Enables read optimization for the directory; sets the read size in bytes.
threshold multiple <multiple>	Specifies the threshold multiple.
write {optimize | 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol nfs”

protocol nfs default volume

Configures default settings for the NFS volumes.

Syntax

[no] protocol nfs default volume {perm-cache | policy {custom | global-rw} |root-squash}

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 to optimize traffic without violating the permissions model.
policy {custom | global-rw}	Specifies 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** - Specifies 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 SteelHeads) 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	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol nfs”

protocol nfs enable

Enables the NFS optimizer. The NFS optimizer provides latency optimization improvements for NFS operations primarily by prefetching data, storing it on the client SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol nfs”

protocol nfs max-directories

Sets the maximum size of NFS directories.

Syntax

[no] protocol nfs max-directories <bytes>

Parameters

<bytes>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol nfs”

protocol nfs max-symlinks

Specify, in bytes, the maximum size of NFS symbolic link directories.

Syntax

[no] protocol nfs max-symlinks <bytes>

Parameters

<bytes>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol nfs”

protocol nfs memory

Specifies, 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

soft-limit <percent>	Specifies the soft-limit percentage size to establish the warning threshold.
hard-limit <percent>	Specifies the hard-limit percentage size to establish the error threshold.

Usage

The **no** command option resets the limit to the default.

Example

```
amnesiac (config) # protocol nfs memory hard-limit 95
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol nfs”

protocol nfs server

Configures settings for the specified NFS server.

Syntax

[no] protocol nfs server <name> {default volume {enable | perm-cache | policy {custom | global-rw | read-only} | root-squash| direntrymap | ip <address> | policy {custom | global-rw | read-only} | read-ahead {small-files | transfer-size <size>} | read-dir {optimize | read-size <size>} | threshold multiple <multiple> | volume id <fsid> [perm-cache | policy {custom | global-rw | read-only} | root-squash] | write {optimize | max-data <max>}}

Parameters

<name>	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 <type>	Specifies the default volume policy type: ▪ **custom** - Enables you to turn on or off the root squash feature for NFS volumes from this server. ▪ **global-rw** - Specifies global read-write policy. This policy 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 SteelHeads) 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).
direntry-map	Enables the directory entry map.
ip <address>	Specifies the IP address of the NFS server.
policy <policy>	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** - Specifies global read-write policy. This policy 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 SteelHeads) 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 |transfer-size <size>]	Enables read-ahead for small files; sets the transfer size in bytes.
read-dir [optimize | read-size <size>]	Enables read optimization for the directory and sets the read size in bytes.
threshold multiple <multiple>	Specifies the threshold multiple.
volume id <fsid>	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 SteelHeads) 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 | 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol nfs”

protocol nfs v2-v4-alarm

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol nfs”

Lotus Notes commands

protocol notes enable

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 SteelHeads must be running RiOS 5.5.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 SteelHeads must be running RiOS v6.0.x or later. The client-side and server-side SteelHeads 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 SteelHeads are secure.

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol notes enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol notes pull-repl enable,” “show protocol notes”

protocol notes encrypt blacklist remove-ip

Removes the specified IP address from the blacklist.

Syntax

protocol notes encrypt blacklist remove-ip {<ip-address> | all}

Parameters

<ip-address>	IP address to remove from the blacklist.
all	Clears the blacklist.

Example

```
amnesiac (config) # protocol notes encrypt blacklist remove-ip 10.1.1.2
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol notes encrypt enable," "show protocol notes encrypt"

protocol notes encrypt enable

Enables encrypted Lotus Notes optimization.

Syntax

[no] protocol notes encrypt enable

Parameters

None

Usage

This command disables encrypted Lotus Notes.

Example

```
amnesiac (config) # protocol notes encrypt enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol notes enable," "show protocol notes encrypt"

protocol notes encrypt import server-id

Imports the specified server ID file.

Syntax

protocol notes encrypt import server-id <url> [password <password>]

Parameters

<url>	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>	Specifies an alphanumeric password if the server ID file is encrypted with a password.

Usage

This 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol notes enable," "show protocol notes encrypt"

protocol notes encrypt remove server-id

Removes the decrypted information for an imported server ID from the SteelHead.

Syntax

protocol notes encrypt remove server-id <servername>

Parameters

<servername>	Server name to remove.

Usage

Use this command if you need to remove the decrypted information from the SteelHead.

Example

```
amnesiac (config) # protocol notes encrypt remove server-id CN=gcs-120/O=acme
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol notes enable," "show protocol notes encrypt"

protocol notes encrypt server-port

Sets the unencrypted server port setting used by the server-side SteelHead.

Syntax

[no] protocol notes encrypt server-port <port-number>

Parameters

<port-number>	Port number.

Usage

Use this command to specify which unencrypted port on the Domino server the server-side SteelHead 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 Deployment Guide - Protocols.*

Example

```
amnesiac (config) # protocol notes encrypt server-port 1352
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol notes enable," "show protocol notes encrypt"

protocol notes port

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>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol notes enable," "protocol notes port," "protocol notes pull-repl enable," "show protocol notes"

protocol notes pull-repl enable

Enables pull replication for Lotus Notes protocol connections.

Syntax

[no] protocol notes pull-repl enable

Parameters

None

Usage

In pull replication, the current SteelHead requests information from the source SteelHead. The request specifies the information that the current SteelHead needs, based on its knowledge of changes already received from the source SteelHead and from all other domain controllers in the domain. When the current SteelHead receives information from the source, it updates that information. The current SteelHead's next request to the source SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol notes"

Citrix support commands

This section describes the Citrix support commands.

---

protocol citrix auto-msi enable

Enables Citrix autonegotiate multi-stream ICA.

Syntax

[no] protocol citrix auto-msi enable

Parameters

None

Usage

Enable this command on the client-side SteelHead to use four connections for a single Citrix session. By default, the Citrix clients use one TCP connection for a Citrix session (unless the XenApp/Desktop server is configured for multi-stream ICA).

When enabled, the SteelHead identifies the priority of each connection to allow for finer QoS shaping and marking of Citrix traffic. You can use this feature with both inbound and outbound QoS on the server-side and client-side SteelHead. Both SteelHeads must be running RiOS 9.1. You can also use this feature with path selection to select and prioritize four separate TCP connections.

The Citrix deployment must support multi-stream ICA: the clients must be running Citrix Receiver 3.0 or later. The servers must be running XenApp 6.5 or later or XenDesktop 5.5 or later.

This feature is applicable for CGP and ICA connections.

No configuration is required on the server-side SteelHead. This command does not require an optimization service restart.

Example

```
amnesiac (config) # protocol citrix citrix auto-msi enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol citrix"

protocol citrix cdm enable

Enables Citrix client device mapping.

Syntax

[no] protocol citrix cdm enable

Parameters

None

Usage

Use this 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.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol citrix enable"

protocol citrix enable

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 Deployment Guide - Protocols*.

The **no** command option disables Citrix optimization.

Example

```
amnesiac (config) # protocol citrix enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol citrix"

protocol citrix ica

Configures the Citrix ICA port for optimization.

Syntax

[no] protocol citrix ica port <port>

Parameters

<port>	Citrix ICA port for optimization. The default value is 1494.

Usage

Typically, you do not need to modify the port. The **no** command option reverts to the default port.

Example

```
amnesiac (config) # protocol citrix ica port 1222
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol citrix"

protocol citrix multiport enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol citrix”

protocol citrix multiport priority

Configures the priority and port for Citrix multiport ICA support.

Syntax

[no] protocol citrix multiport priority <priority> port <port>

Parameters

<priority>	Priority number. The range is from 0 through 3.
port <port>	Specifies the Citrix ICA port. Port 2598 is the default port for Citrix priority 0.

Usage

The priority and port parameters specified by this 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol citrix”

protocol citrix secure-ica enable

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 534.

The **no** command option disables SecureICA.

Example

```
amnesiac (config) # protocol citrix secure-ica enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol citrix”

protocol citrix session reliability port

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>	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 in order to classify the traffic correctly. For details, see *SteelHead User 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol citrix”

protocol citrix smallpkts enable

Enables Citrix low-overhead traffic optimization.

Syntax

[no] protocol citrix smallpkts enable

Parameters

None

Usage

Riverbed recommends that you enable enhanced data reduction for low-overhead real-time Citrix traffic that is sent in small packets 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol citrix”

FCIP support commands

This section describes the Fiber Channel over IP (FCIP) support commands. For details on FCIP optimization, see the *SteelHead User Guide* and the *SteelHead Deployment Guide - Protocols*.

protocol fcip enable

Enables FCIP 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 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 Deployment Guide*.

You configure the RiOS FCIP storage optimization module on the SteelHead 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 SteelHeads.

If you have enabled or disabled FCIP optimization or changed a port, you must restart the optimization service.

The **no** command option disables FCIP optimization.

For details, see the *SteelHead User Guide* and the *SteelHead Deployment Guide*.

Example

```
amnesiac (config) # protocol fcip enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol fcip rules," "show protocol fcip settings"

protocol fcip ports

Add ports to the list of FCIP ports.

Syntax

[no] protocol fcip ports <port-list>

Parameters

<port-list>	List of port numbers separated by commas. 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 User Guide* and the *SteelHead Deployment Guide*.

Use the **no** command option to delete one or more port number settings.

Example

```
amnesiac (config) # protocol fcip ports 3225,3226,3227,3228
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol fcip rules," "show protocol fcip settings"

protocol fcip rule

Configures FCIP rules.

Syntax

[no] protocol fcip rule src-ip <ip-address> dst-ip <ip-address> [dif <enable | disable>] [dif-blocksize <bytes>]

Parameters

src-ip <ip-address>	Specifies 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-address>	Specifies the connection destination IP address of the FCIP gateway tunnel endpoints. Use the format XXX.XXX.XXX.XXX.
dif <enable | disable>	Enables or disables this option to isolate and optimize the DIFs embedded within the FCIP data workload.
dif-blocksize <bytes>	Specifies 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 User Guide* and the *SteelHead Deployment Guide*.

Example

```
amnesiac (config) # protocol fcip rule src-ip 1.1.1.1 dst-ip 2.2.2.2 dif enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol fcip enable," "protocol fcip ports," "show protocol fcip rules," "show protocol fcip settings"

protocol fcip stat-port

Set the port for FCIP aggregate statistics.

Syntax

[no] protocol fcip stat-port <port>

Parameters

<port>	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 User Guide* and the *SteelHead Deployment Guide*.

Example

```
amnesiac (config) # protocol fcip stat-port 1243
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol fcip rules,” “show protocol fcip settings”

SRDF support commands

This section describes the Symmetrix Remote Data Facility (SRDF) support commands. For details on SRDF optimization, see the *SteelHead User Guide* and the *SteelHead Deployment Guide*.

protocol srdf enable

Enables 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 637.

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 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 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 633.

You configure the SRDF storage optimization module on the SteelHead 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 SteelHeads.

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 User Guide* and the *SteelHead Deployment Guide*.

The **no** command option disables SRDF optimization.

Example

```
amnesiac (config) # protocol srdf enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol srdf rules,” “show protocol srdf settings”

protocol srdf ports

Add ports to the list of SRDF ports.

Syntax

[no] protocol srdf ports <port-list>

Parameters

<port-list>	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 User Guide* and the *SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol srdf rules,” “show protocol srdf settings”

protocol srdf rule

Adds or deletes a manual SRDF rule.

Syntax

[no] protocol srdf rule src-ip <ip-address> dst-ip <ip-address> [dif {enable | disable}] [dif-blocksize <bytes>]

Parameters

src-ip <ip-address>	Specifies 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-address>	Specifies 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	Enables this option to isolate and optimize the Data Integrity Fields embedded within the SRDF data workload. For example, VMAX.
dif disable	Enables this option to isolate and optimize the Data Integrity Fields embedded within the SRDF data workload. For example, VMAX.
dif-blocksize <bytes>	Specifies 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 User Guide* and the *SteelHead Deployment Guide*.

Example

```
amnesiac (config) # protocol srdf rule src-ip 1.1.1.1 dst-ip 2.2.2.2 dif enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol srdf rules”, “show protocol srdf settings”

protocol srdf symm id address

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-address>

Parameters

<group-id>	Symmetrix ID. The Symmetrix ID is an alpha-numeric string (for example, a standard Symmetrix serial number: 000194900363).
<ip-address>	IP address of the Symmetrix DMX or VMAX GigE ports (RE ports) originating the replication.

Usage

A Symmetrix ID allows the SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol srdf symm”

protocol srdf symm id base-rdf-group

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 <name> base-rdf-group <base>

Parameters

<name>	Symmetrix ID. The Symmetrix ID is an alpha-numeric string (for example, a standard Symmetrix serial number: 000194900363).
<base>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol srdf symm”

protocol srdf symm id rdf_group

Adds a selective optimization Remote Data Facility (RDF) rule for traffic coming from Symmetrix GigE ports (RE ports).

Syntax

[no] protocol srdf symm id <name> rdf_group <rdf-group> optimization {sdr-default | lz-only | none} [description <description>]

Parameters

<name>	Symmetrix ID. The Symmetrix ID is an alpha-numeric string (for example, a standard Symmetrix serial number: 000194900363).
<rdf-group>	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 <policy>	Specifies an optimization policy: ▪ **sdr-default** - Enables SDR and LZ compression. The default value is **sdr-default**. ▪ **lz-only** - Enables LZ compression only. There is no SDR optimization with this setting. ▪ **none** - Disables SDR and LZ compression.
description <"description">	Provides a description about the RDF rule. The description must be enclosed with quotation marks ("). 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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. SnapMirror optimization support is for environments using NetApp Data ONTAP v7 or Data ONTAP v8 operating in 7-mode.

---

protocol snapmirror enable

Enables support for SnapMirror data replication optimization on the SteelHead.

Syntax

[no] protocol snapmirror enable

Parameters

None

Usage

RiOS 8.5 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 8.5.

The **no** command option 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol snapmirror”

---

protocol snapmirror filer address

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>	Name of the filer.
<ipv4-address>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol snapmirror”

protocol snapmirror filer

Configures SnapMirror settings for a filer.

Syntax

[**no**] **protocol snapmirror filer <name>** [**optimization <policy>**] [**priority <policy>**] [**description <description>**]

Parameters

<name>	Name of the filer.
optimization <policy>	Specifies an optimization policy for the filer: ▪ **sdr-default** - Enables SDR and LZ compression. The default value is **sdr-default**. ▪ **lz-only** - Enable LZ compression only. There is no SDR optimization with this setting. ▪ **none** - Disables SDR and LZ compression.
priority <policy>	Specifies 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>	Specifies a filer description or provides 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** command option 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 snapmirror filer ksnap1 address 10.11.100.1
amnesiac (config) # protocol snapmirror filer ksnap1 optimization lz-only priority medium
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol snapmirror”

protocol snapmirror filer volume

Configures SnapMirror settings for a volume.

Syntax

[no] protocol snapmirror filer <name> volume <volume> [optimization <policy>] [priority <policy>] [description <description>]

Parameters

<name>	Name of the filer.
volume <volume>	Name of the volume.
optimization <policy>	Specifies an optimization policy used only as a volume policy: ▪ **sdr-default** - Enables SDR and LZ compression. ▪ **lz-only** - Enables LZ compression only. There is no SDR optimization with this setting. ▪ **filer-default** - Matches the optimization policy of the filer. This is the default policy for a volume. ▪ **none** - Disables SDR and LZ compression.
priority <policy>	Specifies 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>	Specifies a volume description or use to 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 snapmirror filer ksnap1 address 10.11.100.1
amnesiac (config) # protocol snapmirror 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol snapmirror”

protocol snapmirror ports

Adds ports to the list of SnapMirror ports.

Syntax

[**no**] **protocol snapmirror ports <port-list>**

Parameters

<port-list>	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** command option 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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 User 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

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 User Guide*.

Use this mode if you have previously enabled SMB Signing with RiOS 5.5.x, SMB2 signing, or if you are enabling MAPI encryption for Windows 7 in RiOS v6.1 or later.

The **no** command option disables auto-delegation mode.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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

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>	Specifies the delegation domain in which you want to make the delegate user a trusted member, for example: `SIGNING.TEST`
user <username>	Specifies the delegate username. The maximum length is 20 characters. The username cannot contain any of the following characters: / \ [ ] : ; | = , + * ? < > @ " **Note:** The system translates the username into uppercase to match the registered server realm information.
password <password>	Specifies 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 User Guide*.

Use this mode if you have previously enabled SMB signing with RiOS 5.5.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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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

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-address>

Parameters

<ip-address>	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 User 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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

Allows delegated Windows Domain authentication to only the specified servers.

Syntax

[no] protocol domain-auth delegation rule dlg-only <ip-address>

Parameters

<ip-address>	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 User 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol domain-auth delegation rules,” “show protocol domain-auth delegation rules,” “show protocol domain-auth oneway-trust”

protocol domain-auth delegation rule select

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	Applies the rule defined by the "protocol domain-auth delegation rule dlg-only" command.
dlg-all-except	Applies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"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

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol domain-auth delegation auto-mode"

protocol domain-auth migrate

Migrates domain authentication credentials to the secure vault.

Syntax

protocol domain-auth migrate

Parameters

None

Usage

This command configures the SteelHead to use the secure vault for domain authentication credentials.

Example

```
amnesiac (config) # protocol domain-auth migrate
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol domain-auth credentials location”

---

protocol domain-auth restricted-krb enable

Enables 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 Deployment Guide - Protocols* for more information on deployment scenarios.

Example

```
amnesiac (config) # protocol domain-auth restricted-krb enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol domain-auth restricted-krb”

---

protocol domain-auth oneway-trust

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

dns-name<domain>	Specifies the hostname of the delegation domain.
netbios-name <netbios-name>	Specifies the NetBIOS domain name of the delegation domain.
all	Clears all entries in the one-way trust list. **Note:** The **all** keyword 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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 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

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>	Specifies the Active Directory replication domain. The domain name must be in Active Directory domain name format. The SteelHead replicates accounts from this domain.
user-domain <user-domain>	Specifies 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>	Specifies the replication username. The maximum length is 20 characters. The username cannot contain any of the following characters: / \ [ ] : ; | = , + * ? < > @ " **Note:** The system translates the username into uppercase to match the registered server realm information.
password <password>	Specifies the user account password.
rodc <true | false>	Functions 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>	Specifies the Windows domain controller for this domain.

Usage

Kerberos end-to-end authentication 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol domain-auth replication replicate-user”

Remote packet analysis integration commands

cascade shark enable

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.

The SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“user shark,” “show cascade shark”

user shark

Configures the Shark user account settings.

Syntax

[no] user shark [comment | disable | gecos | nopassword | password <cleartext> | password 0 <cleartext>| password 7 <encrypted-string>]

Parameters

comment <comment>	Adds a comment to the user account.
disable	Disables the user account.
gecos	Sets the gecos option.
nopassword	Allows login to this account without a password.
password	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“cascade shark enable,” “show cascade shark”

DNS cache commands

dns cache clear

Clears the content of DNS the cache.

Syntax

dns cache clear

Parameters

None

Example

```
amnesiac (config) # dns cache clear
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show dns cache,” “show dns forwarders,” “show dns interfaces,” “show dns settings”

dns cache freeze enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show dns cache,” “show dns forwarders,” “show dns interfaces,” “show dns settings”

dns cache frozen-min-ttl

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>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show dns cache,” “show dns forwarders,” “show dns interfaces,” “show dns settings”

dns cache fwd enable

Enables caching of DNS entries.

Syntax

[no] dns cache fwd enable

Parameters

None

Usage

The **no** command option disables the cache responses from forwarding name servers.

Example

```
amnesiac (config) # dns cache fwd enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show dns cache,” “show dns forwarders,” “show dns interfaces,” “show dns settings”

dns cache max-ncache-ttl

Sets maximum time a negative response can be cached.

Syntax

[no] dns cache max-ncache-ttl <seconds>

Parameters

<seconds>	Number of seconds a negative response caches. The range is from 2 to 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show dns cache,” “show dns forwarders,” “show dns interfaces,” “show dns settings”

dns cache max-ttl

Sets the maximum time a response can be cached.

Syntax

[no] dns cache max-ttl <seconds>

Parameters

<seconds>	Number of seconds a response caches. The range is from 2 to 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show dns cache,” “show dns forwarders,” “show dns interfaces,” “show dns settings”

dns cache min-ncache-ttl

Sets minimum time that a negative response can be cached.

Syntax

[no] dns cache min-ncache-ttl <seconds>

Parameters

<seconds>	Number of seconds a negative response can be cached. The range is from 0 to 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show dns cache,” “show dns forwarders,” “show dns interfaces,” “show dns settings”

dns cache min-ttl

Sets the minimum time that a response can be cached.

Syntax

[no] dns cache min-ttl <seconds>

Parameters

<seconds>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show dns cache,” “show dns forwarders,” “show dns interfaces,” “show dns settings”

dns cache size

Sets the size of the DNS cache in bytes.

Syntax

[no] dns cache size <bytes>

Parameters

<bytes>	Size of the DNS cache in bytes. The range is from 524288 to 2097152.

Usage

The **no** command option resets the value to the default.

Example

```
amnesiac (config) # dns cache size 2097152
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show dns cache,” “show dns forwarders,” “show dns interfaces,” “show dns settings”

dns enable

Enables a DNS server. Forwards name resolution requests to a DNS name server, then stores the address information locally in the SteelHead. 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. 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands
“show dns cache,” “show dns forwarders,” “show dns interfaces,” “show dns settings”

dns forwarder
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-address> [idx <index>] | move <index> to <index> | remove <index>}

Parameters

add <ip-address>	Specifies the IP address of the forwarder. A forwarder is a DNS server to which the SteelHead caching-name server will forward requests. Forwarder is added to the end of the index of forwarders by default.
idx <index>	Specifies the order in which the SteelHead contacts forwarder by assigning the forwarder a numeric position in the forwarder index. The SteelHead 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>	Specifies the index number of the forwarder. Moves a forwarder from one index position to another.
remove <index>	Removes a forwarder from the index or an index list separated by commas.

Usage
You can also access this command from enable mode.

Example
```
amnesiac (config) # dns forwarder add 10.0.0.1 idx 2
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings," "show stats dns"

dns forwarder enable

Sets the ID of the forwarder IP address to enable.

Syntax

[no] dns forwarder enable <integer>

Parameters

<integer>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns fwd-fail-count

Sets the number of consecutive dropped requests until a forwarder is considered down.

Syntax

[no] dns fwd-fail-count <requests>

Parameters

<requests>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns fwd-fail-dtxn enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show dns cache,” “show dns forwarders,” “show dns interfaces,” “show dns settings”

dns fwd-fail-time

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>	Number of seconds for a 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show dns cache,” “show dns forwarders,” “show dns interfaces,” “show dns settings”

dns fwd-tm-staydown

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>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns interface

Sets the interfaces on which DNS is enabled.

Syntax

dns interface {add <interface> | remove <interface>}

Parameters

add <interface>	Specifies the name of the interface to add.
remove <interface>	Specifies the name of the interface to remove.

Example

```
amnesiac (config) # dns interface add aux
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns root-fallback enable

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 name servers.

Example

```
amnesiac (config) # dns root-fallback enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

dns round-robin enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show dns cache," "show dns forwarders," "show dns interfaces," "show dns settings"

IPSec commands

ip security authentication policy

Sets the authentication algorithms in order of priority.

Syntax

ip security authentication policy <method-1> [<method 2>]

Parameters

<method-1>	Primary policy method: ▪ **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.
<method-2>	Secondary policy method: **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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show ip"

ip security enable

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 in your network for which you want to establish a secure connection. You must also specify a shared secret on each peer SteelHead.

If you NAT traffic between SteelHeads, you cannot use the IPSec channel between the appliances because the NAT changes the packet headers, causing IPSec to reject them.

Note: RiOS 6.0 and later also provides support for SSL peering beyond traditional HTTPS traffic. For details, see "Secure peering (secure inner channel) commands" on page 698.

The **no** command option disables IPSec support.

Example

```
amnesiac (config) # ip security enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show ip"

ip security encryption policy

Sets the encryption algorithms in order of priority.

Syntax

ip security encryption policy <algorithm> [<alt-algorithm>]

Parameters

<algorithm>	Primary algorithm. If you do not have a valid SSL license key (also called the Enhanced Cryptography License key) installed on your SteelHead, 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, you can specify any of the above encryption algorithms or any of the following more secure encryption algorithms: ▪ **3des -** 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.
<alt-algorithm>	Alternate algorithm. If you do not have a valid SSL license key (also called the Enhanced Cryptography License key) installed on your SteelHead, 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, you can specify any of the above encryption algorithms or any of the following more secure encryption algorithms: ▪ **3des -** 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 680.

Example

```
amnesiac (config) # ip security encryption policy null_enc
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ip”

ip security peer ip

Sets the peer SteelHead for which you want to make a secure connection.

Syntax

[no] ip security peer ip <ip-address>

Parameters

<ip-address>	Peer IP address.

Usage

If IPSec is enabled on this SteelHead, then it must also be enabled on all SteelHeads in the IP security peers list; otherwise this SteelHead 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 SteelHeads that are configured to use IPSec security, the Peers list does not display the peer SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ip”

ip security pfs enable

Enables Perfect Forward Secrecy.

Syntax

[no] ip security pfs enable

Parameters

None

Usage

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. The **no** command option disables Perfect Forward Secrecy**.**

Example

```
amnesiac (config) # ip security pfs enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show ip”

ip security rekey interval

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>	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 option resets the interval to the default.

Example

```
amnesiac (config) # ip security rekey interval 30
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show ip"

ip security shared secret

Sets the shared secret used to negotiate and renegotiate secret keys.

Syntax

ip security shared secret <secret-key>

Parameters

<secret-key>	Secret key to ensure Perfect Forward Secrecy security.

Usage

All SteelHeads that need to communicate to each other using IPSec must have the same key. This command must be set before IPSec is enabled.

Example

```
amnesiac (config) # ip security shared secret xxxx
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show ip"

SSL support commands

no protocol ssl backend bypass-table

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>	Specifies 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 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl backend bypass-table”

protocol ssl backend alpn-forward enable

Allows the SteelHead to recognize the Application Layer Protocol Negotiation (ALPN) extension field. This extension allows the application layer to negotiate which protocol will be used within the TLS connection.

Syntax

[**no**] **protocol ssl backend alpn-forward enable**

Parameters

None

Usage

HTTP/2 over TLS uses the ALPN extension field. To provide SSL/TLS decryption, the SteelHead needs to support this extension for data reduction optimization.

ALPN support requires that TLSv1.2 be enabled on both the client-side and server-side SteelHead and the server-side SteelHead must be running RiOS 9.6.

This feature is enabled by default. Use this command if it has been disabled and you need this functionality.

To view current settings, use the command **show protocol ssl backend** command.

Example

```
amnesiac (config) # protocol ssl backend alpn-forward enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl backend”

protocol ssl backend bypass-interval

Sets the bypass interval after failed server handshakes.

Syntax

[no] protocol ssl backend bypass-interval <seconds>

Parameters

<seconds>	Bypass interval in seconds.

Usage

To view current settings, use the command **show protocol ssl backend** command.

Example

```
amnesiac (config) # protocol ssl backend bypass-interval 60
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl backend”

protocol ssl backend bypass-table max-size

Configures the SSL bypass table size.

Syntax

[no] protocol ssl backend bypass-table max-size <max-size>

Parameters

<max-size>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl backend bypass-table”

protocol ssl backend bypass-table no-cert-intvl

Sets the bypass interval for servers for which no suitable certificate was found.

Syntax

[no] protocol ssl backend bypass-table no-cert-intvl <seconds>

Parameters

<seconds>	Interval in seconds.

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # protocol ssl backend bypass-table no-cert-intvl 120
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl backend bypass-table”

protocol ssl backend client cipher-string

Sets the cipher for use with back-end clients.

Syntax

[no] protocol ssl backend client cipher-string <cipher-string> cipher-num <cipher-number>

Parameters

<cipher-string>	Cipher string for use with clients. For a complete list, enter **protocol ssl backend client cipher-string ?**.
cipher-num <cipher-number>	Specifies the cipher number from **1-N** or **end**.

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # protocol ssl backend client cipher-string DEFAULT cipher-num 1
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl backend”

protocol ssl backend client-tls-1.2

Enables Transport Layer Security (TLS) versions 1.1 and 1.2 encryption protocol support between the SSL client and the SteelHead.

Syntax

[no] protocol ssl backend client-tls-1.2

Parameters

None

Usage

TLS version 1.2 is enabled by default starting in RiOS 9.2. This update is automatic for new manufactures and software updates.

For releases prior to RiOS 9.2, you must enable this command on both the server-side and client-side SteelHeads for PKD mode support of TLSv1.2. TLSv1.2 connections from the client are bypassed if support is not enabled on both appliances.

This command determines how the SteelHeads handle the SSL connection from the client. This activity is normally negotiated at the server-side SteelHead. In distributed termination mode, the client-side SteelHead can also negotiate the SSL connections.

Use the **show running-config** command to determine whether or not this command is enabled. This command requires an optimization service restart.

Example

```
amnesiac (config) # protocol ssl backend client-tls-1.2
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol ssl backend server-tls-1.2,” “secure-peering peer-tls-1.2,” “show protocol ssl backend,” “show running-config”

---

protocol ssl backend proxy-san-match enable

Enables the checking of the subject alternative name (SAN) field with the origin server certificate in proxy certificates.

Syntax

[no] protocol ssl backend proxy-san-match enable

Parameters

None

Usage

This command configures the SteelHead to include the SAN fields of proxy certificates when selecting the suitable certificate to use for an SSL server being optimized. By default, only the common name (CN) field is used to match the SSL server. Depending on the set of server certificates you want to optimize, this option can reduce the required number of proxy certificates on the SteelHead.

Please work with Riverbed Technical Support before implementing this command.

Example

```
amnesiac (config) # protocol ssl backend proxy-san-match enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl backend”

---

protocol ssl backend server chain-cert cache enable

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 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. By default, this option is disabled.

Enable this command 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 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 certificate chain caching.

Example

```
amnesiac (config) # protocol ssl backend server chain-cert cache enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl backend”

protocol ssl backend server cipher-string

Configures back-end SSL server settings.

Syntax

[no] protocol ssl backend server cipher-string <string> [cipher-num <number>]

Parameters

cipher-string <string>	Specifies 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>	Specifies a number to set the order of the list. The number must be an integer greater or equal to 1-N, or **end**.

Usage

Use this command to 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl backend client cipher-strings”

protocol ssl backend server renegotiation null-cert enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl backend”

protocol ssl backend server-tls-1.2

Enables TLS versions 1.1 and 1.2 encryption protocol support between the SSL server and the server-side SteelHead.

Syntax

[no] protocol ssl backend server-tls-1.2

Parameters

None

Usage

Use this command in traditional SSL mode to control how the server-side SteelHead negotiates its SSL connections to the server.

TLS versions 1.1 and 1.2 support is enabled by default. Use the **show running-config** command to determine whether or not this command is enabled.

Example

```
amnesiac (config) # protocol ssl backend server-tls-1.2
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“protocol ssl backend client-tls-1.2,” “secure-peering peer-tls-1.2,” “show protocol ssl backend,” “show running-config”

protocol ssl backend sni enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl backend”

protocol ssl backend server ocsp

Enables Online Certificate Status Protocol (OCSP) stapling.

Syntax

protocol ssl backend server ocsp <level> [off]

Parameters

<level>	Specify one of these stapling levels: ▪ **loose** - If the origin server does not support OCSP, the connection is not dropped. ▪ **strict** - If the origin server does not support OCSP, the connection is bypassed (dropped, not optimizable). ▪ **strict_AIA** - If the certificate included an Authority Information Access (AIA) field but the origin server failed to send an OCSP response, the connection is bypassed. If the certificate did not include an AIA field and the origin server failed to send an OCSP response, the connection is not dropped because the server-side SteelHead does not expect an OCSP response.
[off]	Disables OCSP if it has been enabled. By default, OCSP is disabled.

Usage

OCSP is an alternative approach to obtain certificate status from the OCSP servers instead of the origin server’s Public Key Infrastructure (PKI).

Once OCSP is enabled, the server-side SteelHead adds a status request to every client Hello sent to the origin server. If the origin server is OCSP-enabled, it responds to the status request by appending (or stapling) the time-stamped status (revoked, good, or unknown) to the server Hello. The server-side SteelHead then continues the handshake after inspecting the certificate.

You only need to enable this on the server-side SteelHead.

To verify the current settings, use the **show protocol ssl backend** command.

Example

```
amnesiac (config) # protocol ssl backend server ocsp strict
```

```
amnesiac (config) # show protocol ssl backend
Bypass interval when handshakes fail:                  300 seconds
Bypass interval when no suitable certificate is found: 31536000 seconds
Bypass table maximum size:                             80000
Renegotiation with NULL certificates enabled:          no
Certificate chain caching enabled:                     no
SNI enabled:                                           no
Client TLSv1.2:                                        yes
Server TLSv1.2:                                        yes
Include proxy SAN in certificate selection:            no
Forward ALPN extension:                                yes
OCSP Stapling Level:                                   strict
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl backend”

protocol ssl bulk-export password

Exports the current SSL configuration, keys, and certificates.

Syntax

protocol ssl bulk-export password <password> [include-servers] [incl-scep-crl]

Parameters

<password>	Password used to encrypt exported data.
include-servers	Includes 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 keyword when performing bulk exports of peers.
incl-scep-crl	Includes 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 SteelHeads (including multiple server-side appliances), you can use the bulk import feature to avoid configuring each peering trust relationship between the pairs of SteelHeads.

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 importing the bulk data overwrites its existing peering certificates and keys with that bulk data. If the serial numbers do not match, the SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl,” “show scep service”

---

protocol ssl bulk-import

Imports SSL configuration, keys, and certificates.

Syntax

protocol ssl bulk-import password <password> data <data>

Parameters

password <password>	Specifies a password required to decrypt data.
data <data>	Specifies a file that contains previously exported data. Cut and paste from the output of the corresponding **protocol ssl bulk-export** command.

Usage

You can import multiple files or copy and paste multiple exported data sets. Quotation marks (") 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. The SteelHead 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 importing the bulk data overwrites its existing peering certificates and keys with that bulk data. If the serial numbers do not match, the SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl”

protocol ssl ca cert

Imports CA certificates.

Syntax

[no] protocol ssl ca cert <cert-data> [local-name <name>]

Parameters

<cert-data>	Certificate data in PEM format. You can import multiple certificates.
local-name <name>	Specifies the local name for the certificate (ignored if importing multiple certificates).

Usage

Enable on a client-side SteelHead 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 command is disabled.

Both the client-side and server-side SteelHeads must be configured to optimize SSL traffic.

Enabling this command 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl”

---

protocol ssl client-cer-auth enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl”

---

protocol ssl client-side session-reuse enable

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 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 command is disabled in RiOS v6.5.2 and earlier releases. Enabling this command requires an optimization service restart.

In RiOS 7.0, this command is enabled by default when a new configuration is created or when upgrading from a version prior to RiOS 7.0.

Example

```
amnesiac (config) # protocol ssl client-side session-reuse enable
amnesiac (config) # service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl client-side session-reuse”

protocol ssl client-side session-reuse timeout

Configures the client-side SSL connection-reuse time-out setting.

Syntax

[no] protocol ssl client-side session-reuse timeout <number-of-seconds>

Parameters

<number-of-seconds>	Amount of time, in seconds, the client can reuse a session with an SSL server after the initial connection ends. The range is from 120 to 86400 (2 minutes to 24 hours). The default value is 36000 (10 hours).

Usage

Use this command to 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl client-side session-reuse”

protocol ssl crl ca

Configures Certificate Revocation Lists (CRLs) 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-address or hostname> [crl-attr-name <attr-name>] [port <port>]

Parameters

<ca-name>	Name of an SSL CA certificate.
cdp <integer>	Specifies 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 removes the update.
ldap-server <ip-address>	Specifies the Lightweight Directory Access Protocol (LDAP) server IP address to modify a CDP URI.
ldap-server <ip-address or hostname>	Specifies the LDAP server hostname to modify a CDP URI.
crl-attr-name <attr-name>	Specifies the attribute name of CRL in an LDAP entry.
port <port>	Specifies 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.

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 ldap-server 192.168.172.1
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl crl”

protocol ssl crl cas enable

Enables CRL polling and use of CRL in handshake verifications of CAs certificates. Currently, the SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl crl”

protocol ssl crl handshake fail-if-missing

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl crl”

protocol ssl crl manual

Manually configures a CRL Certificate Distribution Point (CDP) for CRL management.

Syntax

[no] protocol ssl crl manual ca <ca-name> uri <string>

Parameters

ca <ca-name>	Specifies the CA name to manually configure the CDP. The **no protocol ssl crl manual** command removes manually configured CDPs.
uri <string>	Specifies the CDP LDAP URI to manually configure the CDP for the CRL.

Usage

The SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl crl”

protocol ssl crl query-now

Downloads CRLs now.

Syntax

[no] protocol ssl crl query-now ca <string> cdp <integer>

Parameters

ca <string> cdp <integer>	Downloads the 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl crl”

protocol ssl enable

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 SteelHeads 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 6.0 or later, you need to provide an IP address, port, and certificate to enable SSL optimization for a server. In RiOS 6.0 and later, you need only add unique certificates to a Certificate Pool on the server-side SteelHead. When a client initiates an SSL connection with a server, the SteelHead 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 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.

When you configure the back-end server proxy certificate and key on the server-side SteelHead, 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 User 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 User Guide*.

The **no** command option disables SSL module support.

Example

```
amnesiac (config) # protocol ssl enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl”

protocol ssl midsession-ssl enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl midsession-ssl”

protocol ssl protocol-vers

Configures the SSL versions supported in your deployment. The default setting is **SSLv3** or **TLSv1**.

Syntax

[no] protocol ssl protocol-vers <version>

Parameters

<version>	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 command option clears the setting.

Example

```
amnesiac (config) # protocol ssl protocol-vers SSLv3_or_TLSv1
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl”

protocol ssl proxy-support enable

Enables SSL proxy support.

Syntax

[no] protocol ssl proxy-support enable

Parameters

None

Usage

SSL proxy support enables the SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl proxy-support”

protocol ssl server-cert import-cert-key

Imports a certificate and key together.

Syntax

[no] protocol ssl server-cert import-cert-key <cert-key-data> [name <name>] [password <password>] [non-exportable]

Parameters

<cert-key-data>	Certificate and private key data in PEM format.
name <name>	Specifies the server certificate name.
password <password>	Specifies an alphanumeric password associated with the private key.
non-exportable	Makes the private key for server certificates nonexportable.

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-cert name certificate”

protocol ssl server-cert name chain-cert ca

Configures a server certificate chain.

Syntax

[no] protocol ssl server-cert name <server-cert-name> chain-cert ca <ca-name>

Parameters

<server-cert-name>	Server certificate name.
<ca-name>	Existing CA name.

Usage

The **no** command option disables a server certificate chain.

Example

```
amnesiac (config) # protocol ssl server-cert name examplename chain-cert ca Go_Daddy_Class_2
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-cert name chain-certs”

protocol ssl server-cert name chain-cert cert

Configures the server certificate chain.

Syntax

[no] protocol ssl server-cert name <server-cert-name> chain-cert cert <cert-data> [local-name <local-name>]

Parameters

<server-cert-name>	Server certificate name.
cert <cert-data>	Specifies the certificate(s) data in PEM format to import the certificates.
local-name <local-name>	Specifies the local name for the certificate (ignored if importing multiple certificates).

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands-

“show protocol ssl server-cert name chain-certs”

protocol ssl server-cert name change generate-cert

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>	Server certificate name.
rsa	Specifies RSA encryption.
key-size	Specifies the key size: **512**, **1024**, **2048**
common-name <string>	Specifies the certificate common name.
country <string>	Specifies the certificate 2-letter country code.
email <email-address>	Specifies the email address of the contact person.
locality <string>	Specifies the city.
org <string>	Specifies the organization.
org-unit <string>	Specifies the organization name (for example, the company).
state <string>	Specifies the state. You cannot use abbreviations.
valid-days <int>	Specifies how many days the certificate is valid. If you omit **valid-days**, the default is 2 years.
non-exportable	Makes the private key for server certificates non-exportable. If enabled, the SteelHead 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 SCC resync.

Usage

When you configure the back-end server proxy certificate and key on the server-side SteelHead, 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 User 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-cert name chain-certs”

protocol ssl server-cert name change import-cert

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>	Specifies the server certificate name.
import-cert <certificate- data>	Specifies the certificate data in PEM format.
import-key <key-data>	Specifies the private key data in PEM format.
password <password>	Specifies an alphanumeric password associated with the private key.
non-exportable	Makes the private key for server certificates non-exportable. If enabled the SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-cert name chain-certs”

protocol ssl server-cert name change import-cert-key

Imports an SSL certificate and key together.

Syntax

[no] protocol ssl server-cert name <server-cert-name> change import-cert-key <cert-key-data> [password <password>]

Parameters

<server-cert-name>	Server certificate name.
<cert-key-data>	Certificate and private key data in PEM format.
password <password>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-cert name chain-certs”

protocol ssl server-cert name export

Exports certificate (and optional key) in PEM format.

Syntax

[no] protocol ssl server-cert name <server-cert-name> export [include-key password <password>]

Parameters

<server-cert-name>	Server certificate name.
include-key	Includes the private key.
password <password>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-cert name chain-certs”

protocol ssl server-cert name generate-cert

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>	Server certificate name.
rsa	Specifies RSA encryption.
common-name <string>	Specifies the certificate common name.
country <string>	Specifies the certificate 2-letter country code.
email <email address>	Specifies the email address of the contact person.
key-size <512|1024|2048>	Specifies the key size.
locality <string>	Specifies the city.
org-unit <string>	Specifies the organization name (for example, the company).
state <string>	Specifies the state. You cannot use abbreviations.
valid-days <int>	Specifies how many days the certificate is valid. If you omit **valid-days**, the default is 2 years.
non-exportable	Makes the private key for server certificates non-exportable. If enabled, the SteelHead 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, 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 User 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-cert name chain-certs”

protocol ssl server-cert name import-cert

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>] [password <password>] [non-exportable]

Parameters

<server-cert-name>	Server certificate name.
<cert-data>	Certificate data in PEM format.
import-key <key-data>	Specifies the private key data in PEM format to import a private key.
password <password>	Specifies an alphanumeric password associated with the private key.
non-exportable	Makes a private key for server certificates nonexportable. If enabled, the SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-cert name chain-certs”

protocol ssl server-cert name import-cert-key

Imports an SSL certificate and key together.

Syntax

[no] protocol ssl server-cert name <server-cert-name> import-cert-key <cert-key-data> [password <password>] [non-exportable]

Parameters

<server-cert-name>	Server certificate name.
<cert-key-data>	Certificate and private key data in PEM format.
password <password>	Specifies an alphanumeric password associated with the private key.
non-exportable	Makes the private key for server certificates non-exportable. If enabled, the SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-cert name chain-certs”

protocol ssl server-cert name rename

Renames an existing server certificate.

Syntax

[no] protocol ssl server-cert name <server-cert-name> rename <new-name>

Parameters

<server-cert-name>	Server certificate name.
<new-name>	New CA name.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # protocol ssl server-cert name examplecertname rename myexample
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-cert name chain-certs”

protocol ssl server-certs non-exportable enable

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; however, security-conscious organizations might want to make SSL configurations non-exportable.

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, 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 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol ssl bulk-export password," "show protocol ssl"

protocol ssl sfe-mode

Configures safe SSL mode.

Syntax

[no] protocol ssl sfe-mode {advanced_only | mixed}

Parameters

advanced_only	Allows clients capable of Advanced mode SSL.
mixed	Allows both advanced and legacy clients.

Usage

The **no** command option disables safe SSL mode.

Example

```
amnesiac (config) # protocol ssl sfe-mode Advanced_Only
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol ssl"

protocol ssl strm-cipher-cmp enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol ssl"

scep service restart

Restarts Simple Certificate Enrollment Protocol (SCEP) services.

Syntax

scep service restart

Parameters

None

Example

```
amnesiac (config) # scep service restart
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering scep”

secure-vault

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>	Specifies an initial or new password for the secure vault.
reset-password <old-password>	Specifies the old secure vault password to reset it.
unlock <password>	Specifies the current password to unlock the secure vault.

Usage

The *secure vault* is an encrypted file system on the SteelHead where all SteelHead 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 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 is powered on. After rebooting the SteelHead, 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 CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

“show protocol ssl”

ssl-connect

Connects to an SSL server.

Syntax

ssl-connect <hostname>:<port>

Parameters

<hostname>	SSL server hostname.
<port>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl”

web ssl cert generate

Generates a new SSL key and self-signed certificate.

Syntax

web ssl cert generate [key-size {1024|2048|3072|4096}] [country <string>] [email <email-address>] [locality <string>] | [org <string>] [org-unit <string>] [state <string>] [valid-days <int>]

Parameters

key-size	Specifies the key size: **1024**, **2048**, **3072**, **4096** 3072 is the default key size.
country <string>	Specifies 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>	Specifies the email address of the contact person.
locality <string>	Specifies the city.
org <string>	Specifies the organization.
org-unit <string>	Specifies the organization unit (for example, the company).
state <string>	Specifies the state. You cannot use abbreviations.
valid-days <int>	Specifies how many days the certificate is valid. If you omit **valid-days**, the default is 2 years.

Usage

This command generates 3072 bit keys by default.

Example

```
amnesiac (config) # web ssl cert generate
```

Product

Controller, Mobile Controller, SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

web ssl cert generate-csr

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>	Specifies the common name of the certificate authority.
country <string>	Specifies 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>	Specifies the email address of the contact person.
locality <string>	Specifies the city.
org <string>	Specifies the organization.
org-unit <string>	Specifies the organization unit (for example, the company).
state <string>	Specifies the state. You cannot use abbreviations.
valid-days <int>	Specifies how many days the certificate is valid. If you omit **valid-days**, the default is 2 years.

Usage

This command is available on the SteelHead Interceptor starting in version 4.0.

Example

```
amnesiac (config) # web ssl cert generate-csr
```

Product

Controller, Mobile Controller, SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web ssl cert”

web ssl cert import-cert

Imports a certificate, optionally with current private key, in PEM format, and optionally a password.

Syntax

web ssl cert import-cert <cert-data> [import-key <key> [password <password>]]

Parameters

import-cert <cert-data>	Specifies a certificate file in PEM format.
import-key <key>	Specifies a private key in PEM format.
password <password>	Specifies 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

Controller, Mobile Controller, SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web ssl cert”

web ssl cert import-cert-key

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>	Specifies a private key and certificate file in PEM format.
password <password>	Specifies a password.

Example

```
amnesiac (config) # web ssl cert import-cert-key mykey
```

Product

Controller, Mobile Controller, SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show web ssl cert”

web ssl protocol sslv3

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

Controller, Mobile Controller, SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl”

web ssl protocol tlsv1

Sets the SSL v1 protocols for Apache to use.

Syntax

[no] web ssl protocol tlsv1

Parameters

None

Usage

You can also set the SSL protocol to **tlsv1.1** or **tlsv1.2**. The **no** command option disables this setting.

Example

```
amnesiac (config) # web ssl protocol tlsv1
```

Product

Controller, Mobile Controller, SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show protocol ssl"

Secure peering (secure inner channel) commands

This section describes the Secure Inner Channel (SIC) commands.

In RiOS 6.0 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, 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 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 SteelHeads authenticating each other by exchanging certificates and negotiating a separate encryption key for each intercepted connection. Next, the SteelHeads create corresponding inner connections for all outer connections between the client and the client-side SteelHead and between the server and the server-side SteelHead.

Peers are detected the first time a client-side SteelHead 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 SteelHeads, 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 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 trusts the server-side SteelHead, and vice versa.

We recommend 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 User Guide*.

---

secure-peering black-lst-peer

Configures a trusted self-signed black list peer.

Syntax

secure-peering black-lst-peer address <ip-address> trust

Parameters

address <ip-address>	Specifies a password used to encrypt exported data.
trust	Configures a trusted black list peer.

Usage

Lists all untrusted SteelHeads. 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 peer is copied into the local SteelHead untrusted hosts black list.

Example

```
amnesiac (config) # secure-peering black-lst-peer address 10.0.0.1 trust
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering black-lst-peers”

secure-peering cipher-string

Configures a cipher string to use for peering.

Syntax

secure-peering cipher-string <string> [cipher-num <number>]

Parameters

cipher-string <string>	Specifies 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>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering ca”

secure-peering crl ca

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-address or hostname> crl-attr-name <name> port <port>

Parameters

ca <string>	Specifies the name of a secure peering CA certificate.
cdp <integer>	Specifies a Certificate Distribution Point (CDP) in a secure peering CA certificate.
ldap-server <ip-address>	Specifies the IP address of a Lightweight Directory Access Protocol (LDAP) server answering a query to Certificate Revocation List (CRL).
ldap-server <hostname>	Specifies the hostname of an LDAP server answering a query to Certificate Revocation List (CRL).
crl-attr-name <name>	Specifies the attribute name of CRL in an LDAP entry.
port <port>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering crl”

secure-peering crl cas enable

Enables CRL polling and use of CRL in handshake verifications of CAs certificates. Currently, the SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering crl”

secure-peering crl manual ca

Manually configures a CDP for CRL management.

Syntax

[no] secure-peering crl manual ca <ca-name> uri <string>

Parameters

<ca-name>	Specifies the CA name to manually configure the CDP. The **no protocol ssl crl manual** command removes manually configured CDPs.
uri <string>	Specifies the CDP URI to manually configure the CDP for the CR.

Usage

The SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering crl”

secure-peering crl query-now

Downloads CRL now.

Syntax

[no] secure-peering crl query-now ca <string> cdp <integer>

Parameters

ca <string>	Specifies the CA name.
cdp <integer>	Specifies the CDP integer.

Usage

The SteelHead automatically discovers Certificate Distribution Points (CDP) 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering crl”

secure-peering export

Exports a certificate (and optional key) in PEM format.

Syntax

[no] secure-peering export [include-key password <password>]

Parameters

include-key	Includes the private key.
password <password>	Specifies a password used to encrypt exported data.

Usage

The SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering”

secure-peering fallback-no-enc enable

Enables fallback to no encryption on the inner channel.

Syntax

[no] secure-peering fallback-no-enc enable

Parameters

None

Usage

Specifies that the SteelHead 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 SteelHeads, especially in mixed deployments where one SteelHead is running RiOS 6.0 or later and the other SteelHead is running an earlier RiOS version.

This option applies only to non-SSL traffic.

Use this command 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 SteelHeads. Consequently, configurations with this setting disabled risk the possibility of dropped connections. For example, consider a configuration with a client-side SteelHead running RiOS 5.5.x or earlier and a server-side SteelHead running RiOS 6.0 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering”

---

secure-peering generate-cert rsa

Generates a private key and a self-signed certificate using RSA encryption.

Syntax

secure-peering 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 <integer>]

Parameters

key-size	Specifies the key size: **512**, **1024**, **2048**
common-name <string>	Specifies 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 SteelHeads, all three server configurations may use the same certificate name *.nbttech.com.
country <string>	Specifies the certificate two-letter country code.
email <email-address>	Specifies the email address of the contact person.
locality <string>	Specifies the city.
org <string>	Specifies the organization.
org-unit <string>	Specifies the organization unit (for example, the company).
state <string>	Specifies the state. You cannot use abbreviations.
valid-days <integer>	Specifies 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 6.0, you need to provide an IP address, port, and certificate to enable SSL optimization for a server. In RiOS 6.0 and later, you need only add unique certificates to a Certificate Pool on the server-side SteelHead. When a client initiates an SSL connection with a server, the SteelHead 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 supports RSA private keys for peers and SSL servers.

For detailed information about configuring SSL including basic steps, see the *SteelHead User 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-certs”

secure-peering generate-csr

Generates a certificate signing request with current private key.

Syntax

secure-peering generate-csr [common-name <string>] [country <string>] [email <email-address>] [locality <string>] [org <string>] | [org-unit <string>] [state <string>]

Parameters

common-name <string>	Specifies the certificate common name.
country <string>	Specifies the certificate 2-letter country code.
email <email-address>	Specifies the email address of the contact person.
locality <string>	Specifies the city.
org-unit <string>	Specifies the organization name (for example, the company).
state <string>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-certs”

secure-peering gray-lst-peer

Configures a trust relationship for a self-signed gray-list peer.

Syntax

[**no**] **secure-peering gray-lst-peer <ip-address> trust**

Parameters

<ip-address>	IP address for the self-signed gray list peer.
trust	Enables a trust relationship for the specified peer.

Usage

Peers are detected the first time a client-side SteelHead 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 SteelHeads, 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.

Example

```
amnesiac (config) # secure-peering gray-lst-peer 10.0.0.1 trust
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering gray-lst-peer,” “show secure-peering gray-lst-peers”

secure-peering import-cert

Imports a certificate.

Syntax

[no] secure-peering import-cert "<cert-data>" [import-key <key-data>]

Parameters

"<cert-data>"	Existing string to import the certificate. (These are X509 PEM-format field names.) You must enclose the **"<cert-data>"** parameter in quotations.
import-key <key-data>	Specifies 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
dmVyYmVkIFRlY2hub2xvZ3ksIBBBBBBBBFjAUBgNVBAcTDVNhbiBGcmFuY2lzY28x
EzARBgNVBAgTCkNDDDDDDDDDDaWExCzAJBgNVBAYTAi0tggkAhZ8k1kQmIA8wCQYD
VR0TBAIwADANBgkqhkiG9w0BAQUFAAOBgQCwxb8SSSSSSSSSSK48+kytIgpl0SHW
QYe1+YuLU36q12kY19dkpqbqmbKO/+iIIUH9cflpq2QNL7tnK1xPOxpk9AeuhRZq
X7Wk5IHe7zebpYuvHxmFWjYFKjm8oLEswqnaZF9UYmxUf7+g1J7bE7A42EEM0S/B
0w7oWN72V1Yk1Q==
-----END CERTIFICATE-----
"
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering certificate”

secure-peering import-cert-key

Imports a certificate and key together.

Syntax

[no] secure-peering import-cert-key "<cert-key-data>" [password <string>]

Parameters

<cert-key-data>	Certificate and private key data in PEM format in which to import the key. (These are X509 PEM-format field names.) You must enclose the "**<cert-key-data>**" value in quotation marks. **Note:** The private key is required regardless of whether you are adding or updating.
password <string>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering certificate”

secure-peering peer-tls-1.2

Enables support for the transport layer security (TLS) v1.1/1.2 encryption protocol on the secure inner channel between peer SteelHeads.

Syntax

[**no**] **secure-peering peer-tls-1.2**

Parameters

None

Usage

When you enable a secure inner channel, all data between the client-side and the server-side SteelHead appliances is sent over the secure inner channel. You configure the peer SteelHead appliances as SSL peers so that they are trusted entities. The SteelHead appliances authenticate each other by exchanging certificates as part of the encrypted inner-channel setup.

You can restrict the cipher list but you must have a common set of ciphers between peer SteelHeads so that peers can negotiate.

The TLS connection is v1.2 only when the TLS protocol is enabled on both the server-side and client-side SteelHeads. If the TLS version is mismatched between peers, the lower protocol version TLS v1.1 is used.

This command is enabled by default. Use the **show secure-peering** command to determine whether or not it is enabled.

Example

```
amnesiac (config) # secure-peering peer-tls-1.2
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"protocol ssl backend client-tls-1.2," "protocol ssl backend server-tls-1.2," "show secure-peering"

secure-peering scep auto-reenroll

Configures automatic reenrollment settings. The SteelHead uses the Simple Certificate Enrollment Protocol (SCEP) to automatically reenroll certificates.

Syntax

[no] secure-peering scep auto-reenroll {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>	Specifies the amount of time (in days) to schedule reenrollment before the certificate expires.
last-result clear-alarm	Clears the automatic reenrollment last-result alarm. The last result is the last completed enrollment attempt.

Usage

The SteelHead uses SCEP to dynamically reenroll 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show secure-peering scep auto-reenroll last-result"

secure-peering scep max-num-polls

Configures the maximum number of polls.

Syntax

secure-peering scep max-num-polls <max-number-polls>

Parameters

<max-number-polls>	Maximum number of polls before the SteelHead 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. The SteelHead polls only if the server responds with **pending**. If the server responds with **fail**, then the SteelHead does not poll.

The **no** command option disables this configuration.

Example

```
amnesiac (config) # secure-peering scep max-num-polls 12
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering scep”

secure peering scep on-demand cancel

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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering scep on-demand csr”

secure-peering scep on-demand gen-key-and-csr rsa

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-address>] [country <string>] [common-name <string>] [key-size <512 | 1024 | 2048>]

Parameters

state <string>	Specifies the state. No abbreviations are permitted.
org-unit <string>	Specifies the organizational unit (for example, the department).
org <string>	Specifies the organization name (for example, the company).
locality <string>	Specifies the city.
email <email-address>	Specifies an email address of the contact person.
country <string>	Specifies thiee country (2-letter code only).
common-name <string>	Specifies the hostname of the peer.
key-size	Specifies the key size in bits: **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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering scep on-demand csr”

secure-peering scep on-demand start

Starts an on-demand enrollment in the background.

Syntax

[**no**] **secure-peering scep on-demand start** [**foreground**]

Parameters

foreground	Starts 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering scep on-demand csr”

secure-peering scep passphrase

Configures the challenge password phrase.

Syntax

secure-peering scep passphrase <passphrase>

Parameters

<passphrase>	Challenge password phrase.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # secure-peering scep passphrase “2C2016767F7CE7FFC0210EA93998042A”
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering scep”

secure-peering scep poll-frequency

Configures the poll frequency.

Syntax

secure-peering scep poll-frequency <minutes>

Parameters

<minutes>	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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering scep”

secure-peering scep signed-renewal enable

Adds a signed renewal for SCEP.

Syntax

[no] secure-peering scep signed-renewal enable

Parameters

None

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # secure-peering scep signed-renewal enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering scep ca certificate”

secure-peering scep trust

Adds a peering trust for SCEP.

Syntax

[**no**] **secure-peering scep trust peering-ca <name>**

Parameters

peering-ca <name>	Specifies the name of the existing peering CA.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # secure-peering scep trust peering-ca Bank_First
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering scep ca certificate”

secure-peering scep url

Configures the SCEP responder URL.

Syntax

secure-peering scep url <url>

Parameters

<url>	URL of the SCEP responder. Use the following format: http://host:port/path/to/service or https: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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering scep”

secure-peering traffic-type

Controls the type of traffic sent through the secure inner channel.

Syntax

secure-peering traffic-type <type>

Parameters

<type>	Traffic type: ▪ **ssl-only** - The peer client-side SteelHead and the server-side SteelHead 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 and the server-side SteelHead 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 and the server-side SteelHead 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, 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 SteelHeads are sent encrypted over the secure inner channel. You configure the SteelHeads as SSL peers so that they trust one another as WAN optimization peers.

The SteelHeads 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 trusts the server-side SteelHead, and vice versa.

All outer connections between the client and the client-side SteelHead and between the server and the server-side SteelHead create a corresponding secure inner connection between the SteelHeads. 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.

- To enable SMB Signing, see “protocol cifs smb signing enable” on page 561
- To enable SMB2 Signing, see “protocol smb2 signing enable” on page 568
- To enable Lotus Notes Optimization, see “protocol notes enable” on page 624
- To enable Encrypted Optimization, see “protocol mapi encrypted enable” on page 599

For detailed information, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # secure-peering traffic-type all
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering scep”

secure-peering trust ca

Adds peering trust CA.

Syntax

secure-peering trust ca "<cert>"

Parameters

<cert>	CA name for the certificate provided by the peer. (These are X509 PEM-format field names.) You must enclose the **"<cert>"** parameter in quotation marks.

Example

```
amnesiac (config) # secure-peering trust ca ADDTRUST_Public
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show protocol ssl server-certs”

secure-peering trust cert

Adds peering trust CA.

Syntax

secure-peering trust cert <cert-data> local-name [<local-name>]

Parameters

<cert-data>	Certificate in PEM format to import the key. (These are X509 PEM-format field names.)
local-name <local-name>	Specifies the local name for certificate (ignored if importing multiple certificates).

Example

```
amnesiac (config) # secure-peering trust cert ADDTRUST_Public
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show secure-peering”

FIPS commands

This section describes the Federal Information Processing Standard (FIPS) support commands.

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 details the U.S. and Canadian Government requirements for cryptographic modules. Protection of a cryptographic module within a security system is necessary to maintain the confidentiality and integrity of the information protected by the module. For more information on the FIPS implementation, see the *FIPS Administrator's Guide*.

fips enable

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 CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

"show fips status"

show fips status

Displays FIPS status information by feature.

Syntax

show fips status

Parameters

None

Example

```
amnesiac > show fips status
SCC Autoregistration: Should not be configured in FIPS mode.
MAPI Encrypted Optimization: Should not be configured in FIPS mode.
SMB2 Signing: May not comply with FIPS standard.
Web: Web SSL ciphers must include the elements in
```

```
TLSv1.2:kRSA:!eNull:!aNULL and may optionally delete ciphers
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

"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

Generates a new REST API access code for appliance monitoring.

Syntax

[no] papi rest access_code generate desc <description>

Parameters

desc <description>	Describes 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 SteelCentral NetProfiler communicating with a SteelCentral NetShark appliance.
- A SteelCentral NetProfiler retrieving a QoS configuration from a SteelHead.

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 User Guide* for more information about REST API access.

Example

```
amnesiac (config) # papi rest access_code generate desc cascadeflow
```

Product

Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

"papi rest access_code import," "show papi rest access_codes"

---

papi rest access_code import

Imports an existing REST access code.

Syntax

[no] papi rest access_code import desc <description> data <data>

Parameters

desc <description>	Describes how the access code will be used.
data <data>	Copies and enters the raw data output generated by the **papi rest access_code generate** command on a peer SteelHead.

Usage

Use this command to import access codes generated by another SteelHead so that a client can use the same access code to communicate through the REST API to multiple SteelHeads.

Example

```
amnesiac (config) # papi rest access_code import desc cascadeflow data <data>
```

Product

Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

“papi rest access_code generate,” “show papi rest access_codes”

Job commands

This section describes commands for running jobs in the system.

job command

Schedules CLI command execution for a specified time in the future.

Syntax

[no] job <job-id> command <sequence #> "<cli-command>"

Parameters

<job-id>	Job identification number.
<sequence #>	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>"	CLI command. Enclose the command in quotation marks (").

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 rewritten 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 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

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

"show job," "show jobs"

job comment

Adds a comment to the job for display when **show jobs** is run.

Syntax

[no] job <job-id> comment "<description>"

Parameters

<job-id>	Job identification number.
comment "<description>"	Specifies the comment for the job. Enclose the description in qotation marks (").

Usage

The **no** command option deletes the comment.

Example

```
amnesiac (config) # job 10 comment "this is a test"
```

Product

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

"show job," "show jobs"

job date-time

Sets the date and time for the job to execute.

Syntax

[no] job <job-id> date-time <hh>:<mm>:<ss> [<yyyy>/<mm>/<dd>]

Parameters

<job-id>	Job identification number.
<hh>:<mm>:<ss>	Time for the job to execute.
<yyyy>/<mm>/<dd>	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

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

“show job,” “show jobs”

job enable

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>	Job identification number.

Usage

The **no** command option disables jobs.

Example

```
amnesiac (config) # job 10 enable
```

Product

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

“show job,” “show jobs”

job execute

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>	Job identification number.

Usage

You can also access this command from enable mode.

Example

```
amnesiac (config) # job 10 execute
```

Product

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

“show job,” “show jobs”

job fail-continue

Executes all commands in a job even if a command in the sequence fails.

Syntax

[no] job <job-id> fail-continue

Parameters

<job-id>	Job identification number.

Usage

The **no** command option disables this command.

Example

```
amnesiac (config) # job 10 fail-continue
```

Product

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

"show job," "show jobs"

job name

Sets the name for the job.

Syntax

[no] job <job-id> name <friendly-name>

Parameters

<job-id>	Job identification number.
<friendly-name>	Name for the job.

Usage

The **no** command option deletes the job name.

Example

```
amnesiac (config) # job 10 name myjob
```

Product

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

"show job," "show jobs"

job recurring

Sets the frequency with which to recurrently execute this job.

Syntax

[no] job <job-id> recurring <seconds>

Parameters

<job-id>	Job identification number.
<seconds>	Frequency that the recurring job should execute.

Example

```
amnesiac (config) # job 10 recurring 36000
```

Product

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

“show job,” “show jobs”

RAID commands

raid alarm silence

Silences the RAID alarm.

Syntax

raid alarm silence

Parameters

None

Example

```
amnesiac (config) # raid alarm silence
```

Product

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

“show raid info”

raid swraid add-disk

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>	Physical drive number of the drive to be added.

Usage

Use this 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

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

"show raid info"

raid swraid add-disk-force

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>	Physical drive number of the drive to be added.

Usage

Use this 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

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

"show raid info"

raid swraid fail-disk

Configures fail setting on a RAID disk.

Syntax

raid swraid fail-disk <disk>

Parameters

<disk>	Physical drive number of the disk.

Usage

This command 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.

Example

```
amnesiac (config) # raid swraid fail-disk 1
```

Product

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

"show raid info"

raid swraid get-rate

Displays the RAID rebuild rate.

Syntax

raid swraid get-rate

Parameters

None

Example

```
amnesiac (config) # raid swraid get-rate
```

Product

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

“show raid info”

raid swraid mdstat

Displays the contents of /proc/mdstat.

Syntax

raid swraid mdstat

Parameters

None

Usage

Use this command 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

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

“show raid info”

raid swraid set-rate

Sets the RAID rebuild rate.

Syntax

raid swraid set-rate <rate>

Parameters

<rate>	Rebuild rate as a number of megabytes or: **fast_rebuild**, **slow_rebuild**, or **normal**.

Example

```
amnesiac (config) # raid swraid set-rate fast_rebuild
```

Product

Controller, Mobile Controller, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, SteelHead Interceptor

Related Commands

"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

Runs the cable swap test.

Syntax

nettest run cable-swap

Parameters

None

Usage

Ensures that the WAN and LAN cables on the SteelHead 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:

- SteelHeads deployed in virtual in-path mode.
- Server-side SteelHeads that receive significant amounts of traffic from nonoptimized sites.
- SteelHeads 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show nettest"

nettest run duplex

Runs the duplex matching test.

Syntax

nettest run duplex <interface> {ipv6-target <ipv6-address> | target <ipv4-address>}

Parameters

<interface>	Duplex interface.
ipv6-target <ipv6-address>	Specifies the target IPv6 address to reach.
target <ipv4-address>	Specifies 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 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.

Example

```
amnesiac (config) # nettest run duplex
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show nettest”

nettest run ip-port-reach

Runs the IP address and port test.

Syntax

nettest run ip-port-reach source <interface> {addr <ipv4-address> |ipv6-addr <ipv6-address>} [port <port>]

Parameters

source <interface>	Specifies the source interface.
addr <ipv4-address>	Specifies the peer IPv4 address to check.
ipv6-addr <ipv6-address>	Specifies the peer IPv6 address to check.
port <port>	Specifies 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show nettest”

nettest run net-gateway

Runs the network gateway test.

Syntax

nettest run net-gateway [**ipv6**]

Parameters

ipv6	Runs 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 is on the correct network segment. If the gateway is reachable from another source, check the connections between the SteelHead 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show nettest”

nettest run peer-reach

Runs the peer reachability test.

Syntax

nettest run peer-reach addr [ip-address> | port <port>}

Parameters

addr <ip-address>	Specifies the IP address of the peer appliance to test.
port <port>	Specifies the port.

Usage

Use this command to send a test probe to a specified peer and await the probe response. If a response is not received, the test fails.

Note: 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 displayed in the Connected Appliances report (the primary or aux IP to which the SteelHead 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 SteelHeads.

Example

```
amnesiac (config) # nettest run peer-reach addr 10.0.0.1 port 1243
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“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 196.

tcpdump stop-trigger delay

Configures the time to wait before stopping a TCP dump.

Syntax

[no] tcpdump stop-trigger delay <duration>

Parameters

<duration>	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

Mobile Controller, Interceptor, SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcpdump stop-trigger enable,” “tcpdump stop-trigger regex,” “tcpdump stop-trigger restart,” “show tcpdump stop-trigger”

---

tcpdump stop-trigger enable

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** command option 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

Mobile Controller, Interceptor, SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcpdump stop-trigger delay,” “tcpdump stop-trigger regex,” “tcpdump stop-trigger restart,” “show tcpdump stop-trigger”

---

tcpdump stop-trigger regex

Sets the regular expression that triggers the stopping of TCP dumps.

Syntax

tcpdump stop-trigger regex <regex>

Parameters

<regex>	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 this 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

Mobile Controller, Interceptor, SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcpdump stop-trigger delay,” “tcpdump stop-trigger enable,” “tcpdump stop-trigger restart,” “show tcpdump stop-trigger”

tcpdump stop-trigger restart

Restarts the TCP dump stop-trigger process.

Syntax

tcpdump stop-trigger restart

Parameters

None

Usage

If you change the regular expression or delay, use this 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

Mobile Controller, Interceptor, SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcpdump stop-trigger delay,” “tcpdump stop-trigger enable,” “tcpdump stop-trigger regex,” “show tcpdump stop-trigger”

tcpdump-x all-interfaces

Configures a list of all interfaces for a TCP dump capture.

Syntax

[no] tcpdump-x all-interfaces [capture-name <capture-name>] [buffer-size <buffer-size>] duration <seconds>] [schedule-time <hh:mm:ss> [schedule-date <yyyy/mm/dd>]] [rotate-count <number-of-files>] [snaplength <snaplength>] [sip <src-address>] [dip <dst-address>] [sport <src-port>] [dport <dst-port>] [dot1q {tagged | untagged | both}] | [ip6] |[custom <custom-param>] [file-size <megabytes> | continuous [file-size <megabytes>] | duration <seconds> [file-size <megabytes>]]

Parameters

capture-name <capture-name>	Specifies 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, 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	Starts a continuous capture.
buffer-size <buffer-size>	Specifies the size in KB for all packets.
duration <seconds>	Specifies the run time for the capture in seconds. The default is 30 seconds.
schedule-time <hh:mm:ss>	Specifies a time to initiate the trace dump in the following format: hh:mm:ss.
schedule-date <yyyy/mm/dd>	Specifies a date to initiate the trace dump in the following format: YYYY/MM/DD
rotate-count <no-of-files>	Specifies the number of files to rotate.
snaplength <snaplength>	Specifies 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-address>	Specifies a comma-separated list of source IP addresses. The default setting is all IP addresses.
dip <dst-address>	Specifies a comma-separated list of destination IP addresses. The default setting is all IP addresses.
sport <src-port>	Specifies a comma-separated list of source ports. The default setting is all ports.
dport <dst-port>	Specifies a comma-separated list of destination ports. The default setting is all ports.

dot1q	Specifies 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	Specifies IPv6 packets for packet capture.
custom <custom-param>	Specifies 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>	Specifies 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

Mobile Controller, Interceptor, SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show tcpdump-x,” “tcpdump”

tcpdump-x capture-name stop

Stops the specified TCP dump capture.

Syntax

[no] tcpdump-x capture-name <capture-name> stop

Parameters

<capture-name>	Capture name to stop.

Example

```
amnesiac (config) # tcpdump-x capture-name example stop
```

Product

Mobile Controller, Interceptor, SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show tcpdump-x," "tcpdump"

tcpdump-x interfaces

Configures a comma-separated list of interfaces to capture in the background.

Syntax

[no] tcpdump-x interfaces <interface-name> {continuous | duration <seconds>} [schedule-time <hh:mm:ss> [schedule-date <yyyy/mm/dd>]] [rotate-count <# files>] [snaplength <snaplength>] [sip <src-address>] | [dip <dst-address>] [sport <src-port>] [dport <dst-port>] [dot1q {tagged | untagged | both}] [ip6] [custom <custom-param>] [file-size <megabytes>]

Parameters

<interface-name>	Comma-separated list of interfaces: **primary**, **aux**, **lan0_0**, **wan0_0**
continuous	Start a continuous capture.
duration <seconds>	Specifies the run time for the capture in seconds.
schedule-time <hh:mm:ss>	Specifies a time to initiate the trace dump in the following format: hh:mm:ss.
schedule-date <yyyy/mm/dd>	Specifies a date to initiate the trace dump in the following format: yyyy/mm/dd.
rotate-count <#files>	Specifies the number of files to rotate.
snaplength <snaplength>	Specifies 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-address>	Specifies the source IP addresses. The default setting is all IP addresses.
dip <dst-address>	Specifies a comma-separated list of destination IP addresses. The default setting is all IP addresses.
sport <src-port>	Specifies a comma-separated list of source ports. The default setting is all ports.
dport <dst-port>	Specifies a comma-separated list of destination ports. The default setting is all ports.

dot1q	Specifies 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	Specifies IPv6 packets for packet capture.
custom <custom-param>	Specifies custom parameters (flags) for packet capture.
file-size <megabytes>	Specifies 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

Mobile Controller, Interceptor, SCC, SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“tcpdump,” “show tcpdump-x”

Remote management port commands

This section describes the commands for configuring the remote management port.

This remote management port is unique in that it is connected to the Baseboard Management Controller (BMC). 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.

The following appliances support remote management: CX570, CX770, CX3070, CX5070, CX7070, GX10000, EX560, EX760, EX1160, EX1260, EX1360, IC9600, and SteelFusion Core 3500. Remote port management is not supported on other platforms.

The port to access remote management capabilities varies by model.

- EX1160, EX1260, EX1360, and GX10000 models use the dedicated REMOTE port on the back of the appliance.
- CX5070, CX7070, IC9600, and SteelFusion Core 3500 models use the dedicated BMC port.
- EX560 and EX760 models do not have a separate remote port but share it with the Primary port.
- CX570, CX770, and CX3070 models do not have a separate remote port but share it with the Primary and Aux ports.

See the installation guide for your appliance to see the exact location of the port.

For details on configuring the remote management port, see “remote ip address” on page 734.

Important: Access to the SteelHead 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/.

remote channel

Assigns a LAN channel to the remote port.

Syntax

[no] remote channel <channel-number>

Parameters

<channel-number>	LAN channel.

Example

```
amnesiac (config) # remote channel 2
```

Product

SteelHead CX, SteelHead EX, Interceptor

Related Commands

“show remote configured”

remote dhcp

Enables DHCP on the remote management port.

Syntax

[no] remote dhcp

Parameters

None

Usage

The **no** command option disables DHCP and switches to static address assignment.

Example

```
amnesiac (config) # remote dhcp
```

Product

SteelHead CX, SteelHead EX, Interceptor

Related Commands

“show remote ip”

remote ip address

Manually sets the IP address of the remote management port.

Syntax

remote ip address <ip-address>

Parameters

<ip-address>	IP address to assign to the remote management port.

Usage

Access to the SteelHead through the remote port requires the use of the IPMItool utility. You can download a Linux version at http://sourceforge.net/projects/ipmitool/files/.

This utility must to be run on an administrator's system outside of the SteelHead 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 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
```

Note: 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 root
```

- 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 the tilde character (~) 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 the tilde (~).

Example

```
amnesiac (config) # remote ip address 192.168.100.100
```

Product

SteelHead CX, SteelHead EX, Interceptor

Related Commands

“show remote ip”

remote ip default-gateway

Manually sets the default gateway of the remote management port.

Syntax

remote ip default-gateway <ip-address>

Parameters

<ip-address>	IP address of the default gateway to assign to remote management port.

Example

```
amnesiac (config) # remote ip default-gateway 10.0.0.2
```

Product

SteelHead CX, SteelHead EX, Interceptor

Related Commands

“show remote ip”

remote ip netmask

Manually sets the subnet mask of the remote management port.

Syntax

remote ip netmask <netmask>

Parameters

<netmask>	Subnet mask to assign to the remote management port.

Example

```
amnesiac (config) # remote ip netmask 255.255.255.0
```

Product

SteelHead CX, SteelHead EX, Interceptor

Related Commands

“show remote ip”

remote password

Sets the password to remotely connect to the remote management port.

Syntax

[no] remote password <password>

Parameters

<password>	Password to connect to the remote management port.

Usage

To set a remote management port password

- On the SteelHead, assign a password to the remote management port:

```
amnesiac (config) # remote password root
```

- Using the IPMItool on a remote computer, view the power status of the SteelHead. If you are using the Windows version of IPMItool, replace all references to **ipmitool** with ipmitool.exe.

```
ipmitool -H <remote port ip address> -P "root" chassis power status
```

  Output should state **Chassis Power is on**.

Note: You can download a Linux version at http://sourceforge.net/projects/ipmitool/files/. .

Example

```
amnesiac (config) # remote password root
```

Product

SteelHead CX, SteelHead EX, Interceptor

Related Commands

"show remote ip"

Hardware-assist rule commands

The following section describes the hardware-assist rule commands for the SteelHead and SteelHead Interceptor.

in-path hw-assist edit-rule

Provides an optional text description of the specified rule.

Syntax

in-path hw-assist edit-rule rulenum <rule-number> description "<description>"

Parameters

rulenum <rule-number>	Specifies the rule number.
description "<description>"	Specifies the description. The text must be enclosed in quotation marks.

Usage

This feature functions only on a SteelHead or SteelHead Interceptor 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 SteelHeads 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

Interceptor, SteelHead CX, SteelHead EX

Related Commands

"show in-path hw-assist rules"

in-path hw-assist move-rule rulenum

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>	Specifies the rule number.
to <new-rule-number>	Specifies the new position for the rule.

Usage

This feature functions only on a SteelHead or SteelHead Interceptor 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 workload on the local SteelHeads 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 10-G 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

Interceptor, SteelHead CX, SteelHead EX

Related Commands

"show in-path hw-assist rules"

in-path hw-assist passthrough tcp enable

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 or SteelHead Interceptor 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 workload on the local SteelHeads 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 10-G 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.

This command requires a service restart.

Example

```
amnesiac (config) # in-path hw-assist passthrough tcp enable
amnesiac (config) # service restart
```

Product

Interceptor, SteelHead CX, SteelHead EX

Related Commands

“show in-path hw-assist rules”

in-path hw-assist passthrough udp enable

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 or SteelHead Interceptor 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 workload on the local SteelHeads 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 10-G 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.

This command requires a service restart.

Example

```
amnesiac (config) # in-path hw-assist passthrough udp enable
amnesiac (config) # service restart
```

Product

Interceptor, SteelHead CX, SteelHead EX

Related Commands

“show in-path hw-assist rules”

in-path hw-assist rule

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 "<description>"] | [vlan <vlan>] [rulenum <rule-number>]

Parameters

accept	Accepts traffic for this rule.
pass-through	Passes through traffic for this rule.
subnet-a <subnet-a>	Specifies 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>	Specifies 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>"	Specifies a description of the rule. The string must be in enclosed in quotes (").
vlan <vlan>	Specifies 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. ▪ Specify untagged to specify the rule applies to non-tagged connections. **Note:** Pass-through traffic maintains any preexisting 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 SteelHead Interceptor uses to communicate with other SteelHead Interceptor.
rulenum <rule-number>	Specifies the rule number to insert the pass-through load-balancing rule before.

Usage

This feature functions only on a SteelHead or SteelHead Interceptor 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 SteelHeads 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

Interceptor, SteelHead CX, SteelHead EX

Related Commands

"show in-path hw-assist rules"

Hardware security module commands

A hardware security module (HSM) is a cryptographic device that secures and manages cryptographic keys offering accelerated cryptographic operations. Appliances that need the private key (for example, servers, load balancers, and WAN optimization appliances such as the SteelHead) communicate with the HSM and retrieve the required certificate and/or session key. The private keys from the HSM are used for proxy certificates in SSL optimization.

The server-side SteelHead and HSM communicate through a Network Trust Link (NTL) connection. NTLs are secure, authenticated network connections between the HSM server and its clients (for example, a server-side SteelHead), which use two-way digital certificate authentication and SSL data encryption. Initial configuration steps are needed to create the two-way certificate trust between the server-side SteelHead and HSM.

The server-side SteelHead must be accessible from the HSM on either the auxiliary or management interfaces. We recommend that the server-side SteelHead and HSM be on the same LAN because high latency between them will adversely affect the SSL handshake between the SteelHead and the clients.

RiOS supports Luna HSM Client version 5.4.2 that ships preinstalled with RiOS 9.2. SafeNet Network HSM is a product from Gemalto/Safenet. You need a SafeNet support account to log in to the documentation at:

https://kb.safenet-inc.com/kb/link.jsp?id=DOW3161

The following is the workflow of commands to configure HSM support:

- How to set up the initial configuration to create the two-way certificates of trust between the server-side SteelHead and HSM:
  - "protocol ssl hsm safenet generate-cert"
  - "protocol ssl hsm safenet export-cert"
  - "protocol ssl hsm safenet hsm-server import-cert"
- How to configure proxy certificates and private keys (you need to assign a slot on the HSM dedicated to the server-side SteelHead before you run these commands. See the SafeNet knowledge base documentation for instructions on how to configure the HSM server):
  - "protocol ssl hsm server-cert import-cert"
  - "protocol ssl hsm slot"
  - "protocol ssl ca cert"
  - "protocol ssl hsm server-certs flush"
- How to display HSM information:
  - "show protocol ssl hsm safenet"
  - "show protocol ssl hsm server-cert"
  - "show protocol ssl hsm server-certs"

protocol ssl hsm safenet export-cert

Exports the SteelHead client certificate that was generated using the "protocol ssl hsm safenet generate-cert" command.

Syntax

protocol ssl hsm safenet export-cert

Parameters

None

Usage

This command exports the SteelHead client certificate used to create a Network Trust Link (NTL). Use the UNIX **scp** command to send a secure copy to the HSM server. See the SafeNet Network HSM documentation for details:

https://kb.safenet-inc.com/kb/link.jsp?id=DOW3161

You need a SafeNet support account to log in to the SafeNet Network HSM documentation.

Example

```
amnesiac (config) # protocol ssl hsm safenet export-cert
```

Product

SteelHead CX

Related Commands

"show protocol ssl hsm safenet"

protocol ssl hsm safenet generate-cert

Generates the server-side SteelHead client certificate and private key.

Syntax

protocol ssl hsm safenet generate-cert name {<hostname> | <ip-address>}

Parameters

name <hostname>	Specifies the common name of the SteelHead that is accessible from the HSM. Use the unqualified hostname (without the domain name appended). This generates the client certificate with the specified hostname.
name <ip-address>	Specifies the IP address of the SteelHead that is accessible from the HSM.

Usage

This command generates the SteelHead client certificate and private key used to establish an NTL connection to the HSM server.

Copy the raw output of this command and save it as a certificate file, <hostname>.pem, using the same hostname or IP address specified by the command. Use the following command to securely transfer the certificate file to the HSM from any host that can securely use SSH:

```
scp <path-to-pem-file> admin@<hsm-hostname/IP>:
```

Example

```
amnesiac (config) # protocol ssl hsm safenet generate-cert name server-sh1
         Successfully created certificate with common name: "server-sh1"
         "-----BEGIN CERTIFICATE-----
          MIIDKzCCAhOgAwIBAgIBADANBgkqhkiG9w0BAQsFADBZMQswCQYDVQQGEwJDQTEQ
```

```
 MA4GA1UECBMHT250YXJpbzEPMA0GA1UEBxMGT3R0YXdhMRMwEQYDVQQKEwpNeSBj
 b21wYW55MRIwEAYDVQQDEwlvYWstdnNoNzQwHhcNMTUwNzA2MjA0MzQwWhcNMjUw
 NzA0MjA0MzQwWjBZMQswCQYDVQQGEwJDQTEQMA4GA1UECBMHT250YXJpbzEPMA0G
 A1UEBxMGT3R0YXdhMRMwEQYDVQQKEwpNeSBjb21wYW55MRIwEAYDVQQDEwlvYWst
 6tu6ToTKdlxCnN+mAyLI0TkHXiNnqnPXFchzpl2rzh4muTHQkYIk0dFDft8JuW4u
 vqXQAjCPE5ZzgEbEaOuydvBhrKS3L+Kw+N+GNxbhjnYOt4QjPYEH/mdbiGwTB/1W
 CYc1/Ee25Xx2HXgoJWwjo5z+pdKA9gzAtatdVXz65RHDAQBLtSpGJ9hW5qBsemQf
 WyKnZA2DeohiG/ApvAr0gxIftNA+ciwSydYkHD14Wivt9Z+nJmmsD/H7DmZbVtn6
 e1scFyiIsfE9mEYnb8AEN3KzkvgMz+TXZdodXBJzQlFaMJpLnFCEDBd3bEKFeuE=
        -----END CERTIFICATE-----" > server-sh1.pem

# scp server-sh1.pem admin@luna-host1.lab.nbttech.com:
admin@luna-host1.lab.nbttech.com's password:
```

Product

SteelHead CX

Related Commands

"show protocol ssl hsm safenet"

protocol ssl hsm safenet hsm-server import-cert

Imports the HSM server certificate into the server-side SteelHead local directory.

Syntax

[no] protocol ssl hsm safenet hsm-server name <hsm-device-name> import-cert "<cert-data>"

Parameters

name <hsm-device-name>	Specifies the HSM device name.
import-cert "<cert-data>"	Imports certificate data in PEM format to the server-side SteelHead local directory.

Usage

Use this command as part of the configuration process to set up the trusted NTL connection between the server-side SteelHead and the HSM.

To obtain the HSM server certificate file that you import, secure copy the file from the HSM:

```
scp admin@<HSM_hostname>:server.pem <HSM_hostname>.pem
```

Example

```
amnesiac (config) # protocol ssl hsm safenet hsm-server name safenet-host1 import-cert "-----BEGIN
CERTIFICATE-----
> MIIDKzCCAhOgAwIBAgIBADANBgkqhkiG9w0BAQsFADBZMQswCQYDVQQGEwJDQTEQ
> -----END CERTIFICATE-----"
```

Product

SteelHead CX

Related Commands

"show protocol ssl hsm safenet"

protocol ssl hsm server-cert import-cert

Configures a proxy certificate and corresponding private-key object on the HSM.

Syntax

protocol ssl hsm server-cert name <name> import-cert "<proxy-certificate-text>" key-slot <slot-number> [key-label <key-label>] [key-id <key-id>]

Parameters

<name>	Server certificate name.
"<proxy-cert-text>"	Proxy certificate data in PEM format. Copy the text from the proxy certificate file here.
key-slot <slot-number>	Specifies the slot number where the private key is placed on the HSM. You need to assign one slot on the HSM per server-side SteelHead. A slot is analogous to a partition on a disk. You need to assign a slot number on the HSM as part of the HSM configuration. See the SafeNet HSM documentation at: https://kb.safenet-inc.com/kb/link.jsp?id=DOW3161
key-label <key-label>	Specifies the key label. This label helps to identify the private key.
key-id <key-id>	Specifies the key identifier. This identifier helps to identify the private key.

Usage

Proxy certificates are stored on the server-side SteelHead and private keys are stored on the HSM. You configure commands on the server-side SteelHead to specify the location of the private-key objects on the HSM. You need to run these commands for each proxy certificate and key pair. The HSM contains multiple slots (partitions) and each slot can contain multiple objects.

Any SafeNet HSM client needs to know:

- Slot number on the HSM where the object is placed
- Slot pin for the slot
- Label or ID of the object for identification

Example

```
amnesiac (config) # protocol ssl hsm server-cert name rsa1024_cert import-cert "-----BEGIN
CERTIFICATE..... --END CERTIFICATE-----" key-slot 1 key-label rsa1024_key
```

Product

SteelHead CX

Related Commands

“show protocol ssl hsm server-cert”

protocol ssl hsm server-certs flush

Removes all server certificates with a private key on the HSM.

Syntax

protocol ssl hsm server-certs flush [confirm]

Parameters

confirm	Confirms that you want to remove all server certificates with private keys on the HSM.

Example

```
amnesiac (config) # protocol ssl hsm server-certs flush
```

```
Please re-run with "confirm" within 10 seconds to take effect
amnesiac (config) # protocol ssl hsm server-certs flush confirm
```

Product

SteelHead CX

Related Commands

“show protocol ssl hsm server-certs”

protocol ssl hsm slot

Configures the HSM slot settings for the slot from which the server-side SteelHead accesses the private key objects on the HSM.

Syntax

protocol ssl hsm slot <slot-number> slot-pin <password>

Parameters

<slot-number>	Slot number. This number corresponds to the HSM partition assigned to the server-side SteelHead. The **show protocol ssl hsm safenet** command displays the assigned slot number. All slots assigned to the SteelHead should have the same slot pin.
slot-pin <password>	Specifies the password for the HSM partition that corresponds to this slot.

Usage

This command allows the server-side SteelHead to log in to the HSM to allow access to the private key objects.

Example

```
amnesiac (config) # protocol ssl hsm slot 1 slot-pin hsmpass
```

Product

SteelHead CX

Related Commands

“show protocol ssl hsm safenet”

User identity commands

user-identity propagation enable

Enables or disables the propagation of the user identity (UID) across connection from the same client.

Syntax

[no] user-identity propagation enable

Parameters

None

Usage

The SteelHead collects UIDs from SMB, MAPI over HTTP, and Office 365 SaaS (when enabled) connections. The SteelHead can also use pre-existing SMB and MAPI over HTTP connections where the UID has been extracted to propagate and report the UID for new connections coming from the same source IP.

UID reporting per connection helps with debugging, filtering, and usage estimates for your enterprise traffic. It provides better visibility to help tie connections to user information.

Both the server-side and client-side SteelHeads in your network must be running v9.7 or later for this reporting to work. This feature does not work as expected if you use NAT before the SteelHead appliance. In this scenario, the SteelHead will not know the true source IP address of the connection.

For propagation to work, the **user-identity sources enable** or **protocol saas identity o365 enable** command must be enabled.

This command is enabled by default.

Example

```
amnesiac (config) # user-identity propagation enable
```

Product

SteelHead CX

Related Commands

“protocol saas identity o365 enable,” “user-identity sources enable,” “show connections”

---

user-identity sources enable

Extracts the user identity from authoritative sources for MAPI over HTTP and SMB connections.

Syntax

[**no**] **user-identity sources enable**

Parameters

None

Usage

This command is enabled by default. It enables the collection of statistics by user ID, which is displayed in the **show connections optimized full** command and the User Identity field of the Current Connections report in the user interface.

The UID is reported for all concurrent connections for any user who is connected to SSO or through SMB and MAPI over HTTP.

Example

```
amnesiac (config) # user-identity sources enable
```

Product

SteelHead CX

Related Commands

“user-identity propagation enable,” “show connections,” “show protocol saas identity o365 status”

SaaS protocol commands

---

protocol saas identity o365 enable

Configures SaaS user identity settings for Office 365 interoperability.

Syntax

[**no**] **protocol saas identity o365 enable**

Parameters

None

Usage

This command enables collection of statistics by user ID, which is viewable using the **show connections optimized full** command and the Current Connections report in the user interface.

The SteelHead collects User IDs only from Office 365 users that are authenticated with single sign-on (SSO) using Active Directory Federation Services (ADFS).

This feature is disabled by default. You only need to enable this feature on one SteelHead in your network. You must enable HTTP and SSL optimization as a prerequisite for this feature.

In addition to enabling the feature, you must configure proxy certificates for certain hosts on the server-side SteelHead.

Example

```
amnesiac (config) # protocol saas identity o365 enable
amnesiac (config) # service restart
```

Product

SteelHead CX

Related Commands

“show connections,” “show protocol saas identity o365 status”

SaaS Accelerator commands

service saas-accel enable

Enables SaaS acceleration on the appliance.

Syntax

[no] service saas-accel enable

Parameters

None

Usage

Running this command enables SaaS acceleration. You can also enable SaaS acceleration in the appliance’s Management Console. You cannot enable SaaS acceleration without registering the appliance with SCM. You also need to enable SSL optimization on the appliance before you can enable SaaS acceleration.

The **no** command option disables SaaS acceleration.

Example

```
amnesiac (config) # service saas-accel enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“service saas-accel register”

service saas-accel register

Registers the appliance with the SteelConnect Manager using a registration token.

Syntax

[no] service saas-accel register scm <hostname> token <token-number> [port <port-number>]

Parameters

scm <hostname>	Specifies the hostname of the SteelConnect Manager.
token <token-number>	Specifies the registration number you copied from the SteelConnect Manager under WAN Optimization > SaaS Client Appliances.
port <port-number>	The default port is 3900 and we recommend not changing this value.

Usage

A registration token enables the appliance to register and communicate with the SteelConnect Manager set up to manage SaaS Acceleration. To get the token from the SCM, choose WAN Optimization > SaaS Client Appliances and copy the token from the top of the page.

Once registered, the appliance can peer with the SaaS acceleration service hosted by Riverbed.

You can also register the appliance from the SteelHead Management Console.

The **no** command option deregisters the appliance. If you deregister your appliance, you must register it again for it to participate in the cloud acceleration service.

Before deregistering an, ensure that you have deleted all the SaaS acceleration in-path rules (on a Mobile Controller, ensure the SaaS acceleration in-path rules are deleted from all policies). If you run the command without deleting the SaaS acceleration in-path rules, deregistration fails with a warning. To both deregister the appliance from SCM and to delete the SaaS acceleration in-path rules from all the policies, use the **no service saas-accel register force** command.

Example

```
amnesiac (config) # service saas-accel register scm scm-name token ABCDE12345
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“service saas-accel enable”

service saas-accel scm refresh

Update SaaS acceleration information on the appliance.

Syntax

service saas-accel scm refresh

Parameters

None

Usage

By default, the appliance gets data from the SteelConnect Manager every five minutes. Use this command to connect with the SteelConnect Manager and update the SaaS Accelerator configuration and status information.

Example

```
amnesiac (config) # service saas-accel scm refresh
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service saas-accel applications,”

Displaying SaaS Accelerator information

show service saas-accel

Displays the information about the SteelHead/Mobile Controller SaaS Accelerator including whether it is enabled, its status, the associated SCM hostname and port number, the last four digits of the registration token, the last four digits of the organization ID, and which access list (white list, black list, or gray list) it belongs to on SCM.

Syntax

show service saas-accel

Parameters

None

Example

```
amnesiac (config) # show service saas-accel
SaaS-Accel status:
   Enabled:    Yes
   SCM:        saassystem.riverbed.cc:3900
   Registration token: ....2eRO
   OrgID:      ....9083
   Registered: Yes
   Last Contact: 2018/07/16 00:12:35 PDT (28 seconds ago)
   On SCM:     White List
   Status:     OK
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“SaaS Accelerator commands”

show service saas-accel applications

Displays SaaS applications configured for acceleration through SteelConnect.

Syntax

show service saas-accel applications

Parameters

None

Example

```
amnesiac (config) # show service saas-accel applications
Application                  dst-app             SaaS Service Endpoint
-----------                  -------             ---------------------
SharePoint for Business      shrpoint            104.211.159.33:7810
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"SaaS Accelerator commands"

Legacy Cloud Accelerator commands

This section describes the commands unique to the Legacy Cloud Accelerator feature. 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.

Note: In RiOS 9.8, the name for this feature has changed from SteelHead Cloud Accelerator to Legacy Cloud Accelerator. The SaaS Accelerator through SteelConnect replaces the Legacy Cloud Accelerator and provides a Riverbed end-to-end solution with simplified deployment and certificate management.

in-path peering rule cloud-accel

Configures in-path peering rules for the SteelHead SaaS.

Syntax

[no] in-path peering rule cloud-accel {auto | passthru} [peer <peer-ip-address>] [ssl-capability {cap | in-cap | no-check}] [src {<ip-address> | all-ip |all-ipv4 | all-ipv6>}] [dest {<ip-address> | all-ip |all-ipv4 | all-ipv6>}] [dest-port <port>] [rulenum <rule-number>] [description <description>]

Parameters

cloud-accel	Uses cloud acceleration in peering rules on a data center SteelHead in a back-hauled deployment to configure which connections coming from a branch SteelHead (with the SteelHead SaaS enabled but with redirect disabled) should be optimized with the SteelHead SaaS. Specify one of the following rules: ▪ **auto** - The data center SteelHead redirects to the cloud connections when the branch SteelHead tries to optimize with the SteelHead SaaS. ▪ **passthru** - The data center SteelHead does not redirect to the cloud connections when the branch SteelHead tries to optimize with the SteelHead SaaS. If the branch SteelHead does not have the SteelHead SaaS enabled, or if it is not trying to optimize the SteelHead SaaS connection, the value of this field is irrelevant on the data center SteelHead.
peer <peer-ip-address>	Specifies the in-path IP address of the probing SteelHead. If more than one in-path interface is present on the probing SteelHead, apply multiple peering rules, one for each in-path interface.

ssl-capability	Specifies 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 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, and if there is no temporary or short-lived error condition, the SSL-capable check is a success. The SteelHead 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 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 performs both auto-discovery and SSL optimization. ▪ **in-cap (incapable)** - If the destination IP address and port are not an SSL server that is properly configured and enabled on the server-side SteelHead, or if there is a temporary or short-lived error condition, the SSL-capable check fails. The SteelHead 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. ▪ **no-check** - The peering rule does not determine whether the server SteelHead 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 performs auto-discovery and does not optimize SSL. This rule always appears last in the list and you cannot remove it.
src <ip-address>	Specifies 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.
src all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
src all-ipv4	Specifies all IPv4 addresses.
src all-ipv6	Specifies all IPv6 addresses.
dest <ip-address>	Specifies 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.
dest all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
dest all-ipv4	Specifies all IPv4 addresses.
dest all-ipv6	Specifies all IPv6 addresses.
dest-port <port>	Specifies the destination port for this rule. You can specify a port label, or **all** for all ports.
rulenum <rule-number>	Specifies 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 takes on the connection.
description <description>	Specifies a description to facilitate communication about network administration.

Usage

You can provide increased optimization by deploying two or more SteelHeads 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 is reached, that appliance stops intercepting new connections. This allows the next SteelHead 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 in a cluster not to intercept connections between themselves.

You configure peering rules that define what to do when a SteelHead receives an auto-discovery probe from another SteelHead.

You can deploy serial clusters on the client or server-side of the network.

For environments that want to optimize MAPI or FTP traffic which require all connections from a client to be optimized by one SteelHead, 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 SteelHead Interceptor to build multi-appliance clusters. For details, see the *SteelHead Interceptor Deployment Guide* and the *SteelHead Interceptor User Guide*.

To prevent an unknown SteelHead from peering you must add a pass-through peering rule that passes through traffic from the unknown SteelHead in the remote location. For detailed information, see the Management Console online help and the *SteelHead 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 with in-path peering rules to prevent peering with another SteelHead in the cluster, and with in-path rules to not optimize connections originating from other SteelHeads 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 CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show in-path peering rules”

---

service cloud-accel application

Enables cloud accelerator per Software as a Service (SaaS) application.

Syntax

[no] service cloud-accel application <app-id> appgroup <group-name> enable

Parameters

<app-id>	Application ID. The application ID is an alphanumeric string unique to each SaaS application. You can find a complete list of supported SaaS applications and their associated IDs by logging into the Riverbed Cloud Portal and viewing the Cloud Accelerator > Service Summary page.
<group-name>	Application group to which the SaaS application you are configuring belongs. Legacy SaaS applications O365 and SFDC are available under two appgroups for optimization: a-la-carte (legacy offering) and All-SaaS (new offering). All other SaaS applications are only available under the All-SaaS group name. Enter a question mark (?) after the application's group name to show the list of available appgroups: ▪ **O365-a-la-carte** for Office365 under old license. ▪ **SFDC-a-la-carte** for SalesForce under old license. ▪ **All-SaaS** for O365, SalesForce, Box.com, and others under new All SaaS offering.
enable	Enables the optimization for the SaaS application.

Usage

The **no** command option disables cloud acceleration for the SaaS platform specified under the selected group name.

Example

```
amnesiac (config) # [no] service cloud-accel application O365 appgroup All-SaaS enable
amnesiac (config) # service cloud-accel application O365 appgroup O365-a-la-carte enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"show service cloud-accel applications," "show service cloud-accel application"

service cloud-accel enable

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

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service cloud-accel”

service cloud-accel geodns anycast sharepoint enable

Enables GeoDNS optimization on the SteelHead appliance for servers supporting anycast IP lookup for SharePoint.

Syntax

[no] service cloud-accel geodns anycast sharepoint enable

Parameters

None

Usage

GeoDNS is used to locate the best SaaS server to the destination Exchange-online (Office 365) server. Microsoft now returns generic anycast IPs when resolving SharePoint hostnames (for example, rvbdtech.sharepoint.com). The responding server is usually close to the client rather than the data, which results in poor SteelHead optimization.

With this feature, the client-side SteelHead performs DNS resolutions to determine the real backend SharePoint server IP for discovered hostnames. The SteelHead uses this IP address for the next connection going forward, which improves optimization performance.

Single client IPs connecting to multiple SharePoint servers at the same time are not supported (for example, rvbdtech.sharepoint.com and rvbd346.sharepoint.com). When this behavior is detected, the client IP and anycast IP pair are blacklisted for a period of time (1 hour) and redirected to a different server. Traffic is still optimized when the blacklist is in place.

This command is enabled by default in RiOS 9.7 and later and should not be disabled under normal circumstances.

Example

```
amnesiac (config) # service cloud-accel geodns anycast sharepoint enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service cloud-accel geodns”

service cloud-accel geodns enable

Enables GeoDNS optimization on the SteelHead appliance.

Syntax

[no] service cloud-accel geodns enable

Parameters

None

Usage

GeoDNS is used to locate the closest SteelHead to the destination Exchange-online (Office 365) server. The GeoDNS feature is enabled by default in RiOS 8.6.2 and later and should not be disabled under normal circumstances.

The **no** command option disables the GeoDNS service.

Example

```
amnesiac (config) # service cloud-accel geodns enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service cloud-accel geodns”

service cloud-accel geodns portal_update enable

Enables Riverbed Cloud Portal updates for GeoDNS on the SteelHead appliance.

Syntax

[no] service cloud-accel geodns portal update enable

Parameters

None

Usage

GeoDNS is used to locate the closest SteelHead to the destination Exchange-online (Office 365) server.

This command is enabled by default. The **no** command option disables the GeoDNS service.

Example

```
amnesiac (config) # service cloud-accel geodns portal_update enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“service cloud-accel geodns portal_update interval,” “show service cloud-accel geodns”

service cloud-accel geodns portal_update interval

Changes the GeoDNS portal update interval.

Syntax

service cloud-accel geodns portal_update interval <seconds>

Parameters

<seconds>	Update interval in seconds. The default interval is 300.

Usage

GeoDNS is used to locate the closest SteelHead to the destination Exchange-online (Office 365) server.

The **no** command option disables the GeoDNS service.

Example

```
amnesiac (config) # service cloud-accel geodns portal_update interval 400
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“service cloud-accel geodns portal_update enable,” “show service cloud-accel geodns”

service cloud-accel geodns rule

Configures a GeoDNS rule.

Syntax

[no] service cloud-accel geodns rule {opt srcaddr {<ip-address> | all-ipv4 |all-ipv6} geo-dns-ip <address> | pass srcaddr {<ip-address> | all-ipv4 |all-ipv6}}

Parameters

opt	Configures a GeoDNS optimization rule.
pass	Configures a GeoDNS optimization or pass through rule. You can use the **pass** option for debugging purposes to disable certain client subnets if a customer configuration has issues with its Windows client rather than with GeoDNS on the SteelHead.
srcaddr <ip-address>	Specifies 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.
srcaddr all-ip	Specifies all IPv4 and all IPv6 addresses. This is the default.
srcaddr all-ipv4	Specifies all IPv4 addresses.
srcaddr all-ipv6	Specifies all IPv6 addresses.
geo-dns-ip <address>	Redirects Outlook connections from the source IP address to the specified GeoDNS address.

Usage

GeoDNS is used to locate the closest SteelHead to the destination Exchange-online (Office 365) server. This command configures client-subnet specific GeoDNS optimization or pass through rules that take precedence over the mapping from the Riverbed Cloud Portal.

The **no** command removes the rule.

Example

```
amnesiac (config) # service cloud-accel geodns rule opt srcaddr 10.0.0.0/16 geo-dns-ip 1.2.3.4
amnesiac (config) # service cloud-accel geodns rule pass srcaddr 10.1.2.3/32
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service cloud-accel geodns”

service cloud-accel log-level

Specifies the severity of the log message. The log contains all messages with this severity level or higher.

Syntax

service cloud-accel log-level {debug | info | notice | warning | error | critical}

Parameters

log-level debug	Contains messages that help you debug a failure.
log-level info	Contains informational messages that provide general information about system operations.
log-level notice	Contains normal, but significant conditions, such as a configuration change. This is the default setting.
log-level warning	Contains conditions that might affect the functionality of the appliance, such as authentication failures.
log-level error	Contains conditions that probably affect the functionality of the appliance.
log-level critical	Conditions that affect the functionality of the appliance.

Example

```
amnesiac (config) # service cloud-accel log-level info
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service cloud-accel”

service cloud-accel platforms enable

Allows you to enable or disable cloud acceleration for a specific SaaS platform.

Syntax

[**no**] **service cloud-accel platforms <appid> enable**

Parameters

<appid>	Saas application for which you want to enable or disable cloud acceleration. You can find a complete list of supported SaaS applications and their associated IDs by logging into the Riverbed Cloud Portal and viewing the Cloud Accelerator > Service Summary page.

Usage

The **no** command option disables cloud acceleration for the SaaS platform specified.

Example

```
amnesiac (config) # service cloud-accel platforms O365 enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service cloud-accel platforms,” “show service cloud-accel platforms ip”

service cloud-accel portal refresh

Instructs the Enterprise SteelHead 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

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service cloud-accel”

---

service cloud-accel redirect enable

Enables redirection of connections through the SteelHead SaaS.

Syntax

[**no**] **service cloud-accel redirect enable**

Parameters

None

Usage

Use this command to activate traffic redirection from the Enterprise SteelHead to the Akamai network. This feature is enabled by default. There are two modes of proxy redirection:

- Direct mode - The Enterprise SteelHead redirects traffic to the Akamai network.
- Backhauled mode - The Enterprise SteelHead in the data center redirects traffic to the Akamai network. So, you must disable proxy redirection in the branch Enterprise SteelHead 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

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service cloud-accel”

---

service cloud-accel redirect log-level

Sets the redirection logging level.

Syntax

service cloud-accel redirect log-level {debug | info | notice | warning | error | critical}

Parameters

log-level debug	Contains messages that help you debug a failure.
log-level info	Contains informational messages that provide general information about system operations.
log-level notice	Contains normal, but significant conditions, such as a configuration change. This is the default setting.
log-level warning	Contains conditions that might affect the functionality of the appliance, such as authentication failures.
log-level error	Contains conditions that probably affect the functionality of the appliance.
log-level critical	Conditions that affect the functionality of the appliance.

Example

```
amnesiac (config) # service cloud-accel redirect log-level info
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service cloud-accel”

service cloud-accel redirect port

Specifies the destination port used to redirect connections through the SteelHead SaaS.

Syntax

service cloud-accel redirect port <port>

Parameters

port <port>	Specifies 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 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

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service cloud-accel”

service cloud-accel redirect spill-over enable

Specifies whether the Enterprise SteelHead should continue to redirect new SaaS connections through the cloud when it reaches the Enterprise SteelHead 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 SteelHeads 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 reaches admission control, it redirects connections through the cloud, but the connections are not optimized.

You must enable this setting on the first SteelHead in a serial failover or serial cluster configuration.

The **no** command option disables the cloud acceleration redirection when the Enterprise SteelHead reaches its admission control.

Example

```
amnesiac (config) # service cloud-accel redirect spill-over enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service cloud-accel”

service cloud-accel register

Registers the Enterprise SteelHead using the appliance registration key you specify.

Syntax

[no] service cloud-accel register <key>

Parameters

<key>	Appliance registration key.

Usage

The appliance registration key enables the Enterprise SteelHead to register with the Riverbed Cloud Portal.

The **no** command option deregisters the Enterprise SteelHead. Deregistration cannot be reversed. If you deregister your Enterprise SteelHead, you must register it again for it to participate in the cloud acceleration service.

Example

```
amnesiac (config) # service cloud-accel register ABCDEF12345
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“show service cloud-accel”

Displaying Legacy Cloud Accelerator information

This section describes the **show** commands for displaying SteelHead SaaS information.

show service cloud-accel

Displays the following information about the legacy SteelHead SaaS solution: 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

```
amnesiac (config) # show service cloud-accel
  Enabled:            No
  Status:             Unregistered
  Portal:             cloudportal.riverbed.com:443 (HTTPS)
  Redirection:        Enabled
    Port:             9545
    State:            Inactive
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“SaaS protocol commands”

show service cloud-accel applications

Displays the local enable status for all SaaS applications available on the Riverbed Cloud Portal.

Syntax

show service cloud-accel applications

Parameters

None

Usage

This command lists the SaaS applications that are available for optimization based on the company account configuration on the Portal, and it displays the local enable status of each application. Customers that have an existing and valid Office365 or SalesForce offering will see two entries for each of those SaaS applications: one a-la-carte entry and one All-SaaS entry.

Example

```
amnesiac (config) # show service cloud-accel applications
AppID    AppGroup           Enabled
-----    --------           -------
O365     All-SaaS           Yes
O365     O365-a-la-carte    Yes
SFDC     All-SaaS           No
SFDC     SFDC-a-la-carte    Yes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“service cloud-accel application”

show service cloud-accel application

Displays the local enable status of a particular SaaS application. Customers with existing and valid Office365 or SalesForce offerings in addition to the AllSaaS offering will see an entry for each application group.

Syntax

show service cloud-accel application <app-id>

Parameters

<app-id>	Application ID. The application ID is an alphanumeric string unique to each SaaS application. Enter a question mark after the **application** keyword to show the list of available application IDs, which is based on the applications that are available from the Riverbed Cloud Portal. ▪ **O365** for Office365. ▪ **SFDC** for SalesForce. ▪ **BOX** for Box.com.

Usage

This command lists the local enable status for this SaaS application.

You can use this command to troubleshoot issues when connections to the SaaS are not optimized through the cloud. The output of this command displays details about the server IP addresses that the Enterprise SteelHead is optimizing for the SaaS application.

Example

```
amnesiac (config) # show service cloud-accel application O365
ServiceGroup           Enabled
------------           -------
All-SaaS               No
O365-a-la-carte        Yes

IP Address Ranges:
------------------
65.52.45.0/24          0:65535
65.55.93.64/28         0:65535
70.37.144.0/21         0:65535
70.37.188.105/32       0:65535
94.245.113.128/25      0:65535
94.245.126.120/30      0:65535
111.221.17.128/25      0:65535
111.221.20.0/24        0:65535
111.221.22.0/26        0:65535
111.221.22.192/26      0:65535
111.221.64.0/21        0:65535
111.221.112.0/21       0:65535
132.245.1.128/25       0:65535
132.245.2.0/23         0:65535
132.245.4.0/22         0:65535
132.245.8.0/25         0:65535
132.245.8.128/26       0:65535
132.245.9.0/24         0:65535
132.245.10.0/23        0:65535
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"service cloud-accel application"

---

show service cloud-accel geodns

Displays details about GeoDNS settings.

Syntax

show service cloud-accel geodns

Parameters

None

Example

```
amnesiac > show service cloud-accel geodns
---------------- GeoDNS ----------------------
Enabled:                      Yes
GeoDNS Cache Timeout:         300
Enabled protocols:            http, mapi
GeoDNS Anycast Apps:          Sharepoint
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"service cloud-accel geodns enable," "service cloud-accel geodns anycast sharepoint enable"

---

show service cloud-accel platforms

Displays details about the SaaS platforms that the Enterprise SteelHead is optimizing.

Note: This command is deprecated in RiOS 9.1 and only displays SaaS offerings available in releases before RiOS 9.1.

Syntax

show service cloud-accel platforms

Parameters

None

Example

```
amnesiac > show service cloud-accel platforms
SaaS Platform          App ID         Enabled
-------------          ------         ------
Office 365             O365           Yes
Salesforce.com         SFDC           Yes
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SaaS protocol commands"

show service cloud-accel platforms ip

Displays details about the server IP addresses that the Enterprise SteelHead is optimizing. You can use this command to troubleshoot issues when connections to a certain SaaS service are not optimized through the cloud.

Note: This command is deprecated in RiOS 9.1 and only displays SaaS offerings available in releases before RiOS 9.1.

Syntax

show service cloud-accel platforms ip

Parameters

None

Example

```
amnesiac > 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
.
.
.
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

“SaaS protocol commands”

show service cloud-accel statistics connections

Displays details about the optimized SaaS connections.

Syntax

show service cloud-accel statistics connections

Parameters

None

Example

```
amnesiac > 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

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SaaS protocol commands"

---

show service cloud-accel statistics devices

Displays details about the SaaS platforms that the Enterprise SteelHead is optimizing.

Syntax

show service cloud-accel statistics devices

Parameters

None

Example

```
amnesiac >  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

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c

Related Commands

"SaaS protocol commands"

SAML command

aaa saml enable

Enables Security Assertion Markup Language (SAML) 2.0 authentication on an appliance.

Syntax

[no] aaa saml enable

Parameters

None

Usage

You must have IdP configured for the appliance before you enable SAML. Once IdP is configured, you can choose to enable SAML in the SCC or SteelHead Management Console or by running this CLI command on the appliance.

SAML authentications are only available in the Management Console web interface; they are not available through the CLI. Once SAML is enabled on the appliance, users can log in to its Management Console, provided their user accounts have been set up in IdP. Users who have not been mapped to IdP can log in through the CLI but are authenticated using the local, RADIUS, or TACACS+ authentication methods.

By default, SAML is disabled. The **no** command option disables SAML if it has been enabled.

If you cannot log in using SAML (for example, if the IdP server is unavailable), you can log in through the CLI and disable SAML. Once SAML is disabled, you revert to the previously configured (local, RADIUS, or TACACS+) authentication method for the web interface.

For more details on how to configure IdP and enable SAML, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # aaa saml enable
```

Product

SCC, SteelHead CX, SteelHead EX, SteelHead-c, SteelHead-v

Related Commands

“show saml”

SteelConnect compatibility commands

SteelHead CX appliances running RiOS 9.5 and later are compatible with SCM 2.3 and later, integrating the SteelHead WAN optimization capabilities with the SteelConnect software-defined WAN (SD-WAN) capabilities. The combined products provide a smooth transition from WAN optimization to hybrid networking to SD-WAN. See the *SteelConnect Manager User Guide* for more information about the SteelConnect compatibility feature.

steelhead steel-connect compatibility enable

Enables the SteelConnect compatibility feature.

Syntax

[no] steelhead steel-connect compatibility enable

Parameters

None

Usage

Enable this command on the SteelHead CX running 9.5 to allow SteelConnect gateways running SteelConnect Manager 2.3 to recognize optimized flows from the SteelHead CX appliance. When this feature is enabled and the SteelHead CX discovers a compatible SteelConnect gateway in the network path, the appliances connect automatically.

The SteelHead CX optimizes connections, classifies the traffic, and sends application identification information to the gateway. The gateway applies traffic rules to the optimized flows based on the application ID provided by the SteelHead CX and steers the traffic over the selected path.

By default, this command is disabled on the SteelHead CX and disabled globally for an organization in the SteelConnect Manager. SteelConnect compatibility must be enabled on both appliances for auto-discovery.

See the *SteelConnect Manager User Guide* for more information about the SteelConnect compatibility feature.

Example

```
amnesiac (config) # steelhead steel-connect compatibility enable
```

Product

SteelHead CX

Related Commands

“show steelhead steel-connect compatibility config”

---

show steelhead steel-connect compatibility config

Displays whether or not the SteelConnect compatibility feature is enabled.

Syntax

show steelhead steel-connect compatibility config

Parameters

None

Example

```
amnesiac (config) # show steelhead steel-connect compatibility config
Enabled: yes
```

Product

SteelHead CX

Related Commands

“steelhead steel-connect compatibility enable”

SteelHead EX commands

This section describes commands that are unique to the SteelHead EX that you can use to configure SteelHead EX features. It includes the following sections:

■ “VSP commands” on page 800

Alarm commands

This section describes the commands to configure alarm settings for the SteelHead EX.

---

alarm enable (EX)

Enables the specified alarm.

Syntax

[no] alarm <type> enable

Parameters

<type>	▪ **acs** - This alarm indicates that an application-consistent snapshot failed to be committed to the SteelFusion Core, or a snapshot failed to complete. This alarm is enabled by default. ▪ **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 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 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 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 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 moves out of this condition. ▪ **appliance_unlicensed** - This alarm triggers if the SteelHead 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 the system has encountered issues with the SteelFusion Edge blockstore such as the blockstore has run out of space or the blockstore has run out of memory. ▪ **bypass** - This alarm should not be disabled. It indicates that the system is in bypass mode. If the SteelHead 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.

<type>	▪ **cf_keepalive_timeout_aggr -** This alarm indicates that the connection forwarding neighbor has not sent a keepalive message within the time-out period to the neighbor SteelHead(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_neighbor_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, or if path selection is enabled locally and the neighbor does not have path selection enabled. The SteelHead neighbors pass through IPv6 connections when this alarm triggers. ▪ **cf_read_info_timeout_aggr -** This alarm indicates that the SteelHead has timed out while waiting for an initialization message from the connection-forwarding neighbor. ▪ **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 ▪ **critical_temp** - This alarm indicates that the CPU temperature has exceeded the critical threshold. The default value for the rising threshold temperature is 80ºC; the default reset threshold temperature is 70ºC. ▪ **crl_error: SSL_CAs** - Indicates that an SSL peering certificate has failed to re-enroll automatically within the Simple Certificate Enrollment Protocol (SCEP) polling interval. ▪ **crl_error: SSL_Peering_CAs** - Indicates that an SSL peering certificate has failed to reenroll automatically within the Simple Certificate Enrollment Protocol (SCEP) polling interval. ▪ **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:<x>:status** - These alarms indicate 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_ha** - This alarm indicates that the system has encountered a problem with an appliance in a high availability (HA) pair. ▪ **edge_service** - This alarm indicates that only one of the appliances in an HA pair is actively serving storage data.

<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. ▪ **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. ▪ **esxi_initial_config_failed** - This alarm indicates that the ESXi initial configuration failed. Contact Riverbed Support. ▪ **esxi_license** - This alarm is the parent ESXi licensing alarm on the SteelHead EX. It sends an email notification if the ESXi license is removed, about to expire, has expired, or is a trial version. ▪ **esxi_license_expired** - This alarm indicates that the ESXi license has expired on the SteelHead EX. ▪ **esxi_license_expiring** - This alarm indicates that the ESXi license is going to expire within two weeks on the SteelHead EX. ▪ **esxi_license_is_trial** - This alarm indicates that ESXi is using a trial license. ▪ **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. ▪ **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. ▪ **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. ▪ **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. ▪ **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 continues to function normally. When this error triggers you cannot perform a software upgrade, as the SteelHead 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 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). ▪ **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.

<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 pair is actively serving storage data (the active node).
- **inbound_qos_wan_bw_err** - This alarm indicates that the inbound QoS WAN bandwidth for one or more of the interfaces is set incorrectly. You must configure the WAN bandwidth to be less than or equal to the interface bandwidth link rate.
- **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 module has encountered an error.
- **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: <x> -** These alarms indicate 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 SteelFusion 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.

<type>

- **non_443_ssl_servers_detected_on_upgrade** - This alarm indicates that during a RiOS upgrade (for example, from 5.5 to 6.0), 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 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 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
  ```

- **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 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 does not have enough disk, memory, CPU cores, or NIC cards to support the current configuration.
  - The SteelHead 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.
- **outbound_qos_wan_bw_err** - This alarm indicates that the outbound QoS WAN bandwidth for one or more of the interfaces is set incorrectly. You must configure the WAN bandwidth to be less than or equal to the interface bandwidth link rate.
- **paging** - This alarm indicates whether the system has reached the memory paging threshold. If 100 pages are swapped approximately every two hours the SteelHead 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 predefined uplinks for a connection is unavailable because it has exceeded either the timeout value for uplink latency or the threshold for observed packet loss.
- **path_selection_path_probe_err** - This alarm indicates that a path selection monitoring probe for a predefined uplink has received a probe response from an unexpected relay or interface.

<type>	▪ **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 SteelFusion 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+ SteelFusion SteelHead. 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 to 6 hours. ▪ **rhsp** - This alarm indicates that the Riverbed host tools package (RHSP) is incompatible with the Windows Server version. RHSP provides snapshot capabilities by exposing the Edge through iSCSI to the Windows Server as a snapshot provider. RHSP is compatible with 64-bit editions of Microsoft Windows Server 2008 R2 or later and can be downloaded from the Riverbed Support site at https://support.riverbed.com ▪ **secure_transport_controller_unreachable** - This alarm indicates a network connectivity failure to the Controller for the secure transport feature. Issues that might trigger this alarm are Controller services down because of an upgrade or a network connectivity failure to the Controller. ▪ **secure_transport_registration_failed** - This alarm indicates that the registration with the Controller for secure transport was unsuccessful. ▪ **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 connection forwarding neighbor is lost. ▪ **smb_alert** - This alarm indicates that the system has detected an SMB signing error. ▪ **snapshot -** This alarm indicates that a snapshot has failed to commit to the SAN, or a snapshot has failed to complete. This is a SteelHead EX alarm. ▪ **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.

<type>

- **ssd_wear_warning** - This alarm indicates that the specified disk is approaching its write cycle limit. (Appears only on SteelHead 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 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.
- **steelfusion-core** - This alarm indicates that the connection to the SteelFusion Core is lost.
- **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.
- **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 on the SteelHead EX.
- **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 on the SteelHead EX.
- **warning_temp -** This alarm indicates whether the CPU temperature has exceeded the warning threshold. The default value for the rising threshold temperature is 80ºC; the default reset threshold temperature is 70ºC.
- **web_proxy_config_alarm** - This alarm indicates that an error has occurred with the web proxy configuration.
- **web_proxy_service_alarm -** This alarm indicates that an error has occurred with the web proxy service.

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

SCC, Interceptor, Mobile Controller, SteelHead CX, SteelHead EX

Related Commands

"alarm clear," "alarm clear-threshold," "alarm error-threshold," "show alarm," "show alarms"

Storage commands

This section describes the branch storage commands that are unique to the BlockStream-enabled SteelHead EX. SteelFusion is a dual-ended system with SteelFusion Core at the data center and a SteelHead EX appliance at the edge.

The SteelFusion 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 SteelFusion system eliminates the need for dedicated storage at the branch office, including management and related backup resources.

---

device-failover peer clear

Clears the failover peer settings for the current BlockStream-enabled SteelHead EX.

Syntax

device-failover peer clear

Example

```
Edge1 (config) # device-failover peer clear
Edge1 (config) # show device-failover
```

Product

SteelHead EX

Related Commands

"show device-failover"

---

device-failover peer set

Specifies and sets the failover peer settings for the BlockStream-enabled SteelHead EX.

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>	Serial number of the SteelHead EX active peer.
ip <address>	Specifies the IP address of the SteelFusion Edge active peer appliance.
local-if <local-interface-name>	Specifies the local interface for the standby peer to connect to the active peer.
additional-ip <additional-ip>	Specifies the IP address of the SteelFusion Edge active peer, which is different from the first peer IP address specified by the **ip <address>** parameter.
local-if2 <local-interface-name2>	Specifies 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>	Specifies 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**, period (**.**), and hyphen (**-**). 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>	Specifies the local interface for the current appliance to use when connecting with the SteelFusion Core appliance.

Usage

This command configures the failover peer settings to provide high availability between BlockStream-enabled SteelHeads. 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 SteelFusion 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

Related Commands

“show device-failover”

disk-config layout

Switches among five modes of disk-space allocation between SteelHead EX and VSP.

Syntax

disk-config layout {vsp | granite | vsp_granite | vsp_ext | vsp_granite_ext}

Parameters

vsp	Specifies VSP standalone storage mode to allot all the disk space for VSP functionality. If Granite is not licensed, this mode is not available.
granite	Specifies Granite stand-alone 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	Specifies VSP and Granite stand-alone 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	Specifies that this mode is 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	Specifies that this mode is 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

Related Commands

“show disk-config”

storage core add host

Configures the SteelFusion Core connection.

Syntax

storage core add host <hostname> edge-id <id> [port <port>] [local-interface <interface>]

Parameters

<hostname>	Hostname of the SteelFusion Core host device.
edge-id <id>	Specifies the self-identifier of the SteelFusion Core device.
port <port>	Specifies the port the SteelFusion Core device is to listen on.
local-interface <interface>	Specifies the local interface for the connection to the SteelFusion Core device:

Usage

Use this command to specify and configure the connection to the intended SteelFusion Core host.

Example

```
Edge1 (config) # storage core add host CoLo2 edge-id Branch1 local-interface aux
```

Product

SteelHead EX

Related Commands

“show service storage,” “show storage core,” “storage core host local-interface,” “storage core remove”

storage core host interface

Configures SteelFusion Core interface connection settings.

Syntax

storage core host <hostname> interface {add <hostname> [port <port>] | remove <hostname>}

Parameters

<hostname>	Hostname of the SteelFusion Core host device.
add <hostname>	Add additional SteelFusion Core hostnames.
port <port>	Specifies the port the SteelFusion Core device is to listen on.
remove <hostname>	Removes the SteelFusion Core hostnames.

Example

```
Edge1 (config) # storage core host CoLo1 interface add CoLo2
```

Product

SteelHead EX

Related Commands

“show storage core,” “storage core add host,” “storage core remove”

storage core host local-interface

Configures SteelFusion Core local interface connection settings.

Syntax

storage core host <hostname> local-interface {add <local-interface-name> | remove <local-interface-name>}

Parameters

<hostname>	Hostname of the SteelFusion Core host device.
add <local-interface-name>	Adds the local interface used to connect to the SteelFusion Core device.
remove <local-interface-name>	Removes the local interface used to connect to the SteelFusion Core device.

Example

```
Edge1 (config) # storage core host CoLo1 local-interface add primary
```

Product

SteelHead EX

Related Commands

“storage core add host,” “show storage core,” “storage core remove”

storage core host modify

Modifies the existing SteelFusion Core connection settings.

Syntax

storage core host <hostname> modify {port <port> | new-host <host>}

Parameters

<hostname>	Hostname of the SteelFusion Core host device.
port <port>	Specifies the port the SteelFusion Core device is to listen on.
new-host <host>	Specifies the new hostname of the SteelFusion Core host device.

Example

```
Edge1 (config) # storage core host CoLo2 modify new-host Calif2
```

Product

SteelHead EX

Related Commands

“show storage core,” “storage core add host,” “storage core remove”

storage core remove

Removes the connection to the specified SteelFusion Core host device.

Syntax

storage core remove host <hostname> [force]

Parameters

<hostname>	Hostname of the SteelFusion Core host device.
force	Skips the validation check and forces the removal, even if the LUNs are still online. 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 SteelFusion Core host device.

Example

```
Edge1 (config) # storage core remove host CoLo2
```

Product

SteelHead EX

Related Commands

"show service storage," "show storage core"

storage iscsi mpio interface

Adds or removes the specified multi-path I/O (MPIO) interface.

Syntax

storage iscsi mpio interface {add name <mpio-interface> | remove {name <mpio-interface> | all}

Parameters

add name <mpio-interface>	Specifies an MPIO interface to add: **aux**, **inpath0_0**, **primary**, **vmaux**, **vmlocal**, or **vmpri**.
remove name <mpio-interface>	Removes an MPIO interface.
remove all	Removes all MPIO interfaces.

Usage

MPIO interfaces connect the SteelFusion 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

Related Commands

"show storage iscsi"

storage lun activate

Activates the specified LUN.

Syntax

storage lun activate {alias <lun-alias> | serial <lun-serial>}

Parameters

alias <lun-alias>	Activates the LUN specified by the alias value number.
serial <lun-serial>	Activates the LUN specified by the serial number.

Usage

Use this command to activate a LUN that was previously deactivated because of low space in the SteelFusion Edge blockstore.

Example

```
Edge1 (config) # storage lun activate alias LUN2
```

Product

SteelHead EX

Related Commands

"show storage lun"

storage lun snapshot create

Creates a storage snapshot on the specified LUN.

Syntax

storage lun {alias <alias> | serial <serial>} snapshot create [proxy-backup]

Parameters

alias <alias>	Specifies the alias of the LUN.
serial <serial>	Specifies the serial value of the LUN.
proxy-backup	Enables proxy backup for this private snapshot.

Usage

You configure the proxy backup for the specified LUN on the SteelFusion Core appliance. See the *SteelFusion Deployment Guide* and the *SteelFusion Core Management Console User's Guide* for information about the types of snapshots supported.

Example

```
Edge1 (config) # storage lun alias LUN2 snapshot create
```

Product

SteelHead EX

Related Commands

"show storage lun"

storage lun snapshot remove

Removes a storage snapshot on the specified LUN.

Syntax

storage lun {alias <alias> | serial <serial>} snapshot remove id <snapshot-id> [rm-proxy-backup]

Parameters

alias <alias>	Specifies the alias of the LUN.
serial <serial>	Specifies the serial value of the LUN.
id <snapshot-id>	Removes the private storage snapshot for the LUN as specified by the ID value.
rm-proxy-backup	Removes the proxy-backup for this private snapshot if it exists.

Usage

You configure the proxy backup for the specified LUN on the SteelFusion Core appliance. See the *SteelFusion Deployment Guide* and the *SteelFusion Core Management Console User's Guide* for information about the types of snapshots supported.

Example

```
Edge1 (config) # storage lun alias LUN2 snapshot remove id 2
```

Product

SteelHead EX

Related Commands

"show storage lun"

storage lun snapshot remove non-replicated

Removes all non-replicated snapshots for the LUN.

Syntax

storage lun {alias <alias> | serial <serial>} snapshot remove non-replicated

Parameters

alias <alias>	Specifies the alias of the LUN. This is the alias of the parent LUN.
serial <serial>	Specifies the serial value of the LUN. This is the serial value of the parent LUN.

Usage

This command removes all non-replicated snapshots on the SteelFusion Edge.

Example

```
Edge1 (config) # storage lun alias LUN2 snapshot remove non-replicated
```

Product

SteelHead EX

Related Commands

"show storage lun"

Displaying storage information

The following commands display information about storage configuration on the SteelHead EX appliance.

show device-failover

Displays the failover settings for the current SteelFusion Edge device or BlockStream-enabled SteelHead EX.

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

Related Commands

“device-failover peer set”

show disk-config

Displays the specified 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

Related Commands

"disk-config layout"

show service storage

Displays the status of the SteelFusion Edge service.

Syntax

show service storage

Parameters

None

Example

```
Edge1 # show service storage
SteelFusion-Edge Service: Running
```

Product

SteelHead EX

Related Commands

"show storage core"

show stats storage core-io-bytes

Displays the number of bytes of data read from and written to the SteelFusion Core appliance.

Syntax

show stats storage core-io-bytes {interval <time-interval> | start-time <start> end-time <end>}

Parameters

interval <time-interval>	Returns 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 hour. ▪ **day** - Returns statistics for the last day. ▪ **week** - Returns statistics for the last week. ▪ **month** - Returns statistics for the last 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.

Example

```
Edge1 # show stats storage core-io-bytes interval month
```

```
Total Bytes Read: 333 Bytes
Total Bytes Prefetched: 250
Total Bytes Written: 333
```

Product

SteelHead EX

Related Commands

"storage core add host"

show stats storage initiator-bytes

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 hour. ▪ **day** - Returns statistics for the last day. ▪ **week** - Returns statistics for the last week. ▪ **month** - Returns statistics for the last 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>	Specifies 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

Related Commands

"show stats storage initiator-iops," "show stats storage initiator-ltncy"

show stats storage initiator-iops

Displays the standard I/O operations per second written to and read from the blockstore 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 hour. ▪ **day** - Returns statistics for the last day. ▪ **week** - Returns statistics for the last week. ▪ **month** - Returns statistics for the last 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>	Specifies 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

Related Commands

“show stats storage initiator-bytes,” “show stats storage initiator-ltncy”

show stats storage initiator-ltncy

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 hour. ▪ **day** - Returns statistics for the last day. ▪ **week** - Returns statistics for the last week. ▪ **month** - Returns statistics for the last 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>	Specifies 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

Related Commands

“show stats storage initiator-bytes,” “show stats storage initiator-iops”

show stats storage lun-bytes

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 hour. ▪ **day** - Returns statistics for the last day. ▪ **week** - Returns statistics for the last week. ▪ **month** - Returns statistics for the last 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>	Specifies 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

SteelHead EX

Related Commands

“show stats storage lun-commit-rate”

show stats storage lun-commit-rate

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 hour. ▪ **day** - Returns statistics for the last day. ▪ **week** - Returns statistics for the last week. ▪ **month** - Returns statistics for the last 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.
lun <lun-id>	Specifies 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

SteelHead EX

Related Commands

“show stats storage lun-latency,” “show stats storage lun-bytes”

show stats storage lun-iops

Displays the LUN I/O report 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>	Specifies 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

Related Commands

“show stats storage lun-latency,” “show stats storage lun-bytes”

show stats storage lun-latency

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 hour. ▪ **day** - Returns statistics for the last day. ▪ **week** - Returns statistics for the last week. ▪ **month** - Returns statistics for the last 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>	Specifies 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

Related Commands

“show stats storage lun-bytes”

show storage blockstore

Displays blockstore information.

Syntax

show storage blockstore [**rdc-policy**]

Parameters

rdc-policy	Returns statistics for the current SSD read cache population policy.

Usage

This command is available on the SteelHead EX and SteelFusion Core appliance.

Example

```
Edge1 > show storage blockstore
Blockstore usable bytes : 167.32 GB

Edge1 > show storage blockstore rdc-policy
    Blockstore Read Cache not present
```

Product

SteelHead EX

Related Commands

“show storage core”

---

show storage core

Displays detailed status and information about the configured SteelFusion Core.

Syntax

show storage core

Parameters

None

Example

```
Edge1 # show storage core
SteelFusion-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

Related Commands

“storage core add host,” “storage core host local-interface,” “storage core remove”

---

show storage iscsi

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	Displays information specific to iSCSI initiator credentials.
name <initiator>	Specifies the name of a specific initiator to limit the output to information about that initiator.
initiator-group	Displays the details of iSCSI initiator groups, including configuration status and the initiators in the group.
name <initiator-group>	Specifies the name of a specific initiator group to limit the output to information about that initiator group.
lun-alias <lun-alias>	Specifies 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>	Specifies 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	Displays the details of all configured LUNs, including configuration status, size, type, vendor, serial number, and so on.
mpio interfaces	Displays the details of multipath I/O interfaces.
targets	Displays 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
  Report iSCSI NAA serials:          Enabled
```

Product

SteelHead EX

Related Commands

“show stats storage initiator-bytes,” “show stats storage initiator-iops,” “show storage core,” “show service storage,” “storage iscsi mpio interface”

show storage lun

Displays the details of the storage LUN settings.

Syntax

show storage lun {alias <alias> | serial <serial>} [snapshot {all | id} | snapshot-config | snapshot-log]

Parameters

alias <alias>	Specifies the alias of the LUN to be displayed.
serial <serial>	Specifies the serial value of the LUN to be displayed.
snapshot all	Displays all snapshots associated with a LUN.
snapshot id	Displays snapshots associated an ID.
snapshot-config	Displays snapshot configuration details.
snapshot-log	Displays snapshot log information.

Example

```
Edge_01 > show storage lun alias va-ntfs

Locally Assigned Serial: 80a98000433468734b4a676949794569
  Alias                    : va-ntfs
  LUN Size                 : 900.126 GB
  LUN Type                 : blkdev
  Parent VlunID            : Unknown
  Snapshot Status          : Unknown
  Scheduled snapshots      : Enabled
  Originating Granite-Core : 10.12.200.100
  LUN ID                   : 2
  Online                   : Yes
  Offline percentage       : Not applicable
  IOPs acceleration        : Disabled
  iSCSI Target             : iqn.2003-10.com.company:testbed-edge.000
  Granite-Core Session     : Not Connected
  Origin LUN serial        : 80a98000433468734b4a676949794569
  Pinned                   : no

Mapped igroups:
         all

Mapped initiators:

Snapshot Policy : default_policy
  Max Hourly snaps         : 2
  Max Daily snaps          : 2
  Max Weekly snaps         : 1
  Schedule  :
             daily      : everyday  @  00
             hourly     : everyday  @  04,08,12,16,20
             weekly     : sun  @  23
```

Product

SteelHead EX

Related Commands

“show storage luns”

show storage luns

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 storage luns [block-disk | deactivated | edge-local | iscsi]

Parameters

block-disk	Limits the output to block-disk LUNs.
deactivated	Limits the output to deactivated LUNs.
edge-local	Limits the output to local edge LUNs.
iscsi	Limits the output to iSCSI LUNs.

Example

```
Edge_01 > 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

SteelHead EX

Related Commands

“show storage lun”

Data interface commands

ip data route

Adds an IPv4 data interface static route.

Syntax

[no] ip data route <interface> <network-prefix> <network-mask> <next-hop-ip-address>

Parameters

<interface>	Interface.
<network-prefix>	Network prefix.
<network-mask>	Netmask.
<next-hop-ip-address>	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

Related Commands

“hardware nic slot,” “ip data-gateway,” “ipv6 data route,” “ipv6 data-gateway”

ipv6 data route

Adds an IPv6 data interface route.

Syntax

[no] ipv6 data route <interface> <ipv6-network-prefix> <next-hop-ipv6addr>

Parameters

<interface>	Interface.
<ipv6-network-prefix>	Network prefix. Use the format X:X:X::X/<0-128>.
<next-hop-ipv6addr>	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

Related Commands

“hardware nic slot,” “ip data-gateway,” “ipv6 data-gateway,” “hardware nic slot”

ip data-gateway

Configures an IPv4 default gateway for a data interface.

Syntax

[no] ip data-gateway <interface> <destination>

Parameters

<interface>	Data interface.
<destination>	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

Related Commands

“storage core add host,” “ipv6 data route,” “ipv6 data-gateway,” “hardware nic slot”

ipv6 data-gateway

Configures the IPv6 default gateway for a data interface.

Syntax

[no] ipv6 data-gateway <interface> <destination>

Parameters

<interface>	Data interface.
<destination>	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

Related Commands

“hardware nic slot,”“ipv6 data route,” “ip data-gateway”

Traffic-mode commands

interface traffic-mode

Configures the traffic-mode settings on the specified interface.

Syntax

interface <interface> traffic-mode <traffic-mode>

Parameters

<interface>	Primary or auxiliary interface: **aux** or **primary**.
<traffic-mode>	Traffic mode: ▪ **default** - Default interface setting ▪ **span** - Interface setting for SPAN traffic

Usage

Use this command if you are running a virtual machine (VM) in ESXi that is monitoring network traffic by connecting to a Switched Port Analyzer (SPAN) port. All traffic is mirrored from the SPAN port and received by the VM. This command is a per-interface setting that is limited to the primary or auxiliary interface.

Example

```
Edge1 (config) # interface primary traffic-mode span
```

Product

SteelHead EX

Related Commands

“show interface traffic-mode”

show interface traffic-mode

Displays the traffic mode for the specified interface.

Syntax

show interface <interface> traffic-mode

Parameters

<interface>	Interface type: **aux** or **primary**.

Example

```
Edge1 # show interface aux traffic-mode
Traffic mode: default
```

Product

SteelHead EX

Related Commands

“interface traffic-mode”

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. VSP offers a VM-based virtualization platform with the most commonly deployed and advanced virtualization tool set.

VSP is included in the SteelHead EX functionality and does not require a separate download or license. In SteelHead EX 4.2, ESXi and RiOS software versions are bundled—a new installation of SteelHead EX 4.5 software uses ESXi 6.0 Express Patch 4 as the virtualization platform. The VSP features do not change for this release.

For detailed information on installing and upgrading the SteelHead EX appliance, see the *SteelHead EX Installation and Configuration Guide*. For detailed information about configuring VSP, see the *SteelHead EX Management Console User's Guide*.

Note: VSP is supported on SteelHead 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

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

Related Commands

"Displaying VSP information"

vsp esxi password

Specifies the VSP ESXi password.

Syntax

vsp esxi password <password-string>

Parameters

<password-string>	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 hypervisor password complexity has changed in ESXi 6.0. Passwords that were valid for 5.x may not be permitted in 6.0. However, if you upgrade from ESXi 5.x to 6.x, your password will be saved. For details on this password policy change, see:
https://pubs.vmware.com/vsphere-60/index.jsp?topic=%2Fcom.vmware.vsphere.security.doc%2FGUID-DC96FFDB-F5F2-43EC-8C73-05ACDAE6BE43.html.

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

Related Commands

“Displaying VSP information”

vsp esxi push-config license key

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>	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-western-branch
```

Product

SteelHead EX

Related Commands

“show vsp esxi push-config network”

vsp esxi push-config network ip default-gw

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>	Default ESXi IPv4 gateway address for the ESXi configuration.

Usage

The **no** command option deletes the ESXi default gateway.

Example

```
Edge1 (config) # vsp esxi push-config network ip default-gw 10.5.16.233
```

Product

SteelHead EX

Related Commands

“show vsp esxi push-config network”

vsp esxi push-config network ip interface enable

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>	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

Related Commands

“show vsp esxi push-config network”

vsp esxi push-config network ip interface ipv4

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>	Interface name. Choose either **vmk1** for the ESXi primary interface or **vmk2** for the ESXi auxiliary interface.
ipv4 dhcp enable	Automatically obtains 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	Dynamically obtains IPv4 network settings from a DNS server using dynamic DNS.
ipv4 static address <ipv4-address> netmask <netmask>	Specifies 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

Related Commands

“show vsp esxi push-config network”

vsp esxi push-config network vsphere interface

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>	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

Related Commands

“show vsp esxi push-config network”

vsp esxi push-config ntp enable

Configures the RiOS software to push the 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** command option resets the NTP server settings to the default.

Example

```
Edge1 (config) # vsp esxi push-config ntp enable
```

Product

SteelHead EX

Related Commands

“show vsp esxi push-config ntp”

vsp esxi rios-mgmt-ip

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>	IPv4 address of the local ESXi configuration.

Usage

The **no** command option resets the IPv4 address to the default value.

Example

```
Edge1 (config) # vsp esxi rios-mgmt-ip 10.22.12.3
```

Product

SteelHead EX

Related Commands

“show vsp esxi rios-mgmt-ip”

vsp esxi vnc enable

Enables the use of a Virtual Network Computing (VNC) client to connect directly to an ESXi host that is running on a SteelHead EX.

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. The **no** version of the command disables the VNC capability.

Example

```
Edge1 (config) # vsp esxi vnc enable
```

Product

SteelHead EX

Related Commands

“vsp esxi vnc password,” “vsp esxi vnc port”

vsp esxi vnc password

Configures the VNC password.

Syntax

[no] vsp esxi vnc password <password>

Parameters

<password>	VNC 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

Related Commands

“vsp esxi vnc enable,” “vsp esxi vnc port”

vsp esxi vnc port

Configures the VNC port number of the virtual machine.

Syntax

[no] vsp esxi vnc port <vnc-port>

Parameters

<vnc-port>	VNC port number. By default, a VNC client uses port 5900.

Usage

The **no** command option returns the VNC port to the default port.

Example

```
Edge1 (config) # vsp esxi vnc port 5800
```

Product

SteelHead EX

Related Commands

"vsp esxi vnc enable," "vsp esxi vnc password"

vsp install

Runs the VSP service wizard and installs ESXi.

Syntax

vsp install esxi-password <password>

Parameters

esxi-password <password>	Specifies 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

Related Commands

"disk-config layout," "vsp reinstall esxi-password"

vsp reinstall esxi-password

Reinstalls ESXi configurations and restarts VSP.

Syntax

vsp reinstall esxi-password <password> [wipe-datastore]

Parameters

<password>	New ESXi root password set during reinstallation.
wipe-datastore	Reinstalls ESXi with ESXi configurations in RiOS software, re-create the local data store, and restarts 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

Related Commands

"vsp install"

---

vsp restart

Restarts VSP.

Syntax

vsp restart [**force**]

Parameters

force	Forces 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

Related Commands

"Displaying VSP information"

Displaying VSP information

This section describes the **show** commands for displaying VSP information.

---

show vsp

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

Related Commands

“VSP commands”

---

show vsp configured

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

Related Commands

“VSP commands”

---

show vsp esxi push-config network

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 default-gw	Displays ESXi IPv4 default gateway settings 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

Related Commands

“vsp esxi push-config network ip interface ipv4”

show vsp esxi push-config ntp

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

Related Commands

"vsp esxi push-config ntp enable"

show vsp esxi rios-mgmt-ip

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

Related Commands

"vsp esxi rios-mgmt-ip"

show vsp esxi runtime network

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

Related Commands

"VSP commands"

---

show vsp esxi version

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

Related Commands

"VSP commands"

---

show vsp esxi version-history

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

Related Commands

"VSP commands"

SteelHead Interceptor commands

This chapter describes commands you use to configure SteelHead Interceptor features. It includes the following sections:

Note: Riverbed recommends that you use the Interceptor Management Console to configure the SteelHead Interceptor. For details, see the *SteelHead Interceptor User Guide* and the *SteelHead Interceptor Deployment Guide*.

Note: You must also set up the host and networking configuration, configure in-path interfaces, and configure in-path rules for deployments that use the SteelHead Interceptor for load balancing. These commands are common to the SteelHead and SteelHead Interceptor. 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 737.

---

xbridge enable

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 10-G interfaces on an Interceptor appliance.

Example

```
amnesiac (config) # xbridge enable
```

Product

Interceptor

Related Commands

“show xbridge”

Interceptor failover support commands

failover steelhead interceptor name

Configures the hostname for the failover SteelHead Interceptor.

Syntax

[no] failover steelhead interceptor name <hostname> {additional-ip <ip-address> | main-ip <ip-address>}

Parameters

<hostname>	Hostname of the failover SteelHead Interceptor appliance.
additional-ip <ip-address>	Specifies one or more additional IP addresses (separated by commas) of the failover SteelHead Interceptor appliance. ▪ For IPv4 addresses, use this format: XXX.XXX.XXX.XXX/XX ▪ For IPv6 addresses, use this format: X:X:X::X/XXX
main-ip <ip-address>	Specifies the main IP address of the failover SteelHead Interceptor appliance. ▪ For IPv4 addresses, use this format: XXX.XXX.XXX.XXX/XX ▪ For IPv6 addresses, use this format: X:X:X::X/XXX

Usage

There can be only one failover SteelHead Interceptor.

You must restart the service for your changes to take effect.

Important: You can enter either IPv4 or IPv6 addresses. However, if you have enabled IPv6 connection forwarding, you must enter an IPv6 address. For more information about enabling IPv6 connection forwarding, see the *SteelHead Interceptor User Guide*

The **no** command option removes the failover SteelHead Interceptor from the configuration and removes the hostname.

For detailed information about configuring the failover SteelHead Interceptor process, see the *SteelHead Interceptor Deployment Guide*.

Note: This command replaces the **failover buddy name** command.

Example

```
amnesiac (config) # failover steelhead interceptor name test additional-ip 10.0.0.2
```

Product

Interceptor

Related Commands

"show failover interceptor"

Interceptor operating mode commands

appliance operating-mode 9350

Changes the operating mode of the 9600 appliance to one compatible with the 9350 appliance.

Syntax

[**no**] **appliance operating-mode 9350**

Parameters

None

Usage

This command is intended for use in topologies with a mixture of appliances (for example, both the 9600 appliance and the 9350 appliance).

The **no** command option returns the 9600 appliance to the original operating mode.

Note: For the **no** command option, the **9350** keyword is not applicable and is not included in the command syntax.

Note: This command is supported only on the 9600 appliance.

After using this command, you must restart the service for the change to take effect.

Example

```
amnesiac (config) # appliance operating-mode 9350
amnesiac (config) # no appliance operating-mode
```

Product

Interceptor

Related Commands

"show appliance operating-mode"

Load-balancing commands

clear load balance rule

Clears load-balancing rule statistics.

Syntax

clear load balance rule [<rule-number> | default | all]

Parameters

<rule-number>	Clears the statistics for the load-balancing rule number you specify. Valid values are from 1 to 65534.
default	Clears the statistics for the system-generated default load-balancing rule.
all	Clears the statistics for all load-balancing rules.

Usage

This command clears the load-balancing rule statistics for the rules displayed by the **show load balance rules** command.

You can choose to clear the statistics for a specific load-balancing rule, the system-generated default load-balancing rule, or all load-balancing rules.

To specify more than one load-balancing rule, enter the rule numbers separated by commas (no spaces); for example, 5,7,9.

If you don't specify a rule number, by default the statistics for all load-balancing rules are cleared.

Example

```
amnesiac (config) # clear load balance rule  2,3
```

Product

SteelHead Interceptor

Related Commands

"show load balance rules"

load balance default-rule fair-peering

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

Related Commands

"show load balance rules"

load balance fair-peer-v2 enable

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

Related Commands

“show load balance rules”

load balance fair-peer-v2 threshold

Configures the peer threshold percentage.

Syntax

load balance fair-peer-v2 threshold <percentage>

Parameters

<percentage>	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

Related Commands

“show load balance rules”

load balance move-rule

Moves the order of the rule in the rule list to the specified number.

Syntax

load balance move-rule rulenum <rule-number> to <rule-number>

Parameters

rulenum <rule-number> to <rule-number>	Specifies the rule number to be moved and where to move it.

Example

```
amnesiac (config) # load balance move-rule rulenum 9 to 5
```

Product

Interceptor

Related Commands

"show load balance rules"

load balance rule edit rulenum

Edits a hardware assist rule and, optionally, enables or disables receiving email reminders about load-balancing pass-through rules in use.

Syntax

load balance rule edit rulenum <rule-number> description "<description>" [email-notify {yes | no}]

Parameters

<rule-number>	Rule number to edit.
description "<description>"	Description for the rule. The description must be enclosed in double-quotes.
email-notify	Enables or disables reminders about load-balancing pass-through rules. ▪ **yes** - Sends email reminders every 15 days (the default). ▪ **no** - Does not send email reminders.

Usage

Email reminders apply only to pass-through rules. You can't use them for other types of rules.

If you use the **email-notify** keyword, you'll receive an email message reminding you that you have pass-through rules in use on your network, and asking you to check periodically whether you still need to use them. The reminders help to identify any obsolete rules that you might want to delete to improve traffic optimization.

To receive email reminders, you must also use the **email notify passthrough rule enable** command.

By default, you'll receive email reminders every 15 days. To change the frequency, use the **notify-timer <frequency>** options of the **email notify passthrough rule enable** command.

The email reminders are sent to the addresses shown in the event email recipients field of the **show email** command.

Example

```
amnesiac (config) # load balance rule edit rulenum 9 description "this is a test"
```

Product

Interceptor

Related Commands

"email notify passthrough rule enable," "show email," "show load balance rules"

load balance rule pass

Creates load-balancing pass-through rule.

Syntax

load balance rule pass [src <subnet>/<mask>] [dest <subnet>/<mask> dest-port <port>] [description <string>] [peer {<ip-address> |any | probe-only| non-probe}] [rulenum <rule-number>] [vlan <vlan number>]

Parameters

src <subnet>/<mask>	Specifies the IP address for the source network. Use the following format: XXX.XXX.XXX.XXX/XX
dest <subnet>/<mask>	Specifies the IP address for the destination subnet. Use the following format: XXX.XXX.XXX.XXX/XX
dest-port <port>	Specifies the destination port number or port label.
description <string>	Specifies a description of the rule.
peer <ip-address>	Specifies the peer IP address to apply pass-through load-balancing rules to this IP address only.
peer any	Applies the pass-through rule to any SYN packet and probe.
peer probe-only	Applies the pass-through rule to any probes from any router.
peer non-probe	Applies the pass-through rule to any SYN packet without a probe.
rulenum <rule-number>	Specifies the rule number to insert the pass-through load-balancing rule before.
vlan <vlan-number>	Specifies 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 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 SteelHeads you have configured as neighbor peers to be targets of redirect rules or reserved for the automatic load-balancing rule.
- If a neighbor SteelHead 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 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 SteelHead Interceptor processes load-balancing rules as follows:

1. Redirect rule matches and the target SteelHead is available: Redirect to a target appliance according to the load-balancing algorithm.
2. Redirect rule matches but none of the target SteelHeads for the rules are available: Consults the next rule in the 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 SteelHeads not reserved by other rules.
5. No rules match or no rules specified. Target SteelHeads are chosen based on the following rules:
   - **Peer Affinity** - Prefers a target SteelHead that has had a previous connection with the source SteelHead.
   - **Least Connections** - If more than one target SteelHead has peer affinity, the connection is redirected to one that has the least current connections.
   - **No Peer Affinity** - If no SteelHead has peer affinity, the connection is redirected to the SteelHead 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

Related Commands

"show load balance rules"

load balance rule pass email-notify

Specify whether an email reminder is needed for a load-balancing pass-through rule.

Syntax

load balance rule pass email-notify {yes | no}

Parameters.

yes	Sends email reminders every 15 days (the default).
no	Does not send email reminders.

Usage

Pass-through rules are often created as a solution for a temporary network issue. When the issue is resolved, it's easy to forget that the rule is in use, which results in traffic not being optimized. Email reminders help you remember that these rules are in use on your network, and they help to identify any obsolete rules that you might want to delete to improve traffic optimization.

With this command enabled, you'll receive an email message reminding you that you have pass-through rules in use on your network, and asking you to check periodically whether you still need to use them. The reminders help to identify any obsolete rules that you might want to delete to improve traffic optimization.

This command is enabled by default and it applies to load-balancing pass-through rules only.

To receive email reminders, you must also use the **email notify passthrough rule enable** command.

By default, you'll receive email reminders every 15 days. To change the frequency, use the **notify-timer <frequency>** options of the **email notify passthrough rule enable** command.

The email reminders are sent to the addresses shown in the event email recipients field of the **show email** command.

Important: To turn off email reminders for all pass-through rules (both in-path rules and load-balancing), use the **no email notify passthrough rule enable** command.

Example

```
amnesiac (config) # load balance rule pass email-notify yes
```

Product

Interceptor

Related Commands

"email notify passthrough rule enable," "show email," "show load balance rules"

load balance rule redirect

Creates load-balancing redirect rules.

Syntax

load balance rule redirect addrs <ip-address> [src <subnet>/<mask>] [dest <subnet>/<mask> dest-port <port>] [peer {<ip-address> | any | probe-only | non-probe}] [rulenum <rule-number>] [description "<description>"] [vlan <vlan-number>] [fair-peering {yes | no}]

Parameters

addrs <ip-address>	Specifies a comma-separated list of SteelHead IP addresses to which traffic can be redirected. (Specify the IP address for the SteelHead inpath0_0 interface.) ▪ For IPv4 addresses, use this format: XXX.XXX.XXX.XXX/XX ▪ For IPv6 addresses, use this format: X:X:X::X/XXX If a rule matches, connections are redirected to a SteelHead 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 communication and SteelHead-to-Interceptor communication for peering between appliances. For detailed information, see “steelhead communication interface” on page 828.
src <subnet>/<mask>	Specifies the IP address for the source network. ▪ For IPv4 addresses, use this format: XXX.XXX.XXX.XXX/XX ▪ For IPv6 addresses, use this format: X:X:X::X/XXX
dest <subnet>/<mask>	Specifies the IP address for the destination network. ▪ For IPv4 addresses, use this format: XXX.XXX.XXX.XXX/XX ▪ For IPv6 addresses, use this format: X:X:X::X/XXX
dest-port <port>	Specifies a port number or port label.
peer <ip-address>	Specifies the peer IP address to apply pass-through load-balancing rules to this IP address only.
peer any	Applies the pass-through rule to any SYN packet and probe.
peer probe-only	Applies the pass-through rule to any probes from any router.
peer non-probe	Applies the pass-through rule to any SYN packet without a probe.
rulenum <rule-number>	Specifies the rule number. The rule is inserted before the existing pass-through load-balancing rule.
description "<description>"	Specifies a description of the rule.
vlan <vlan-number>	Specifies the VLAN tag identification number (ID).
fair-peering {yes | no}	Adds (**yes**) or removes (**no**) fair peering for the load-balancing rule.

Usage

Load-balancing rules define the characteristics by which traffic is selected for load balancing and the availability of the LAN-side SteelHead 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 SteelHeads you have configured as neighbor peers to be targets of redirect rules or reserved for the automatic load-balancing rule.
- manage neighbor SteelHeads in one of these ways:
  - If a neighbor SteelHead 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 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 SteelHead Interceptor processes load-balancing rules as follows:

1. The redirect rule matches and the target SteelHead is available: Redirects to a target appliance according to the load-balancing algorithm.
2. The redirect rule matches but none of the target SteelHeads for the rules are available: Consults the next rule in list.
3. The pass-through rule matches: Traffic traverses Riverbed routes but is unoptimized.
4. The redirect rule matches but there's no capacity and it does not match a pass-through rule: Automatically balances load among neighbor SteelHeads not reserved by other rules.
5. No rules match or no rules are specified. Target SteelHeads are chosen based on the following rules:
   - **Peer affinity** - Prefers a target SteelHead that has had a previous connection with the source SteelHead. If no SteelHead has peer affinity, the connection is redirected to the SteelHead with the least current connections.
   - **Least connections** - If more than one target SteelHead has peer affinity, the connection is redirected to one that has the least current connections.
   - **No peer affinity** - If no SteelHead has peer affinity, the connection is redirected to the SteelHead with the least current connections.

Important: You can enter either IPv4 or IPv6 addresses. However, if you have enabled IPv6 connection forwarding, you must enter an IPv6 address. For more information about enabling IPv6 connection forwarding, see the *SteelHead Interceptor User Guide*

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

Related Commands

"show load balance rules"

Interceptor peering and redirect commands

conn-trace rule

Configures connection tracing rules.

Syntax

[no] conn-trace rule [protocol {tcp | udp | any}] srcnet {<subnet> | all-ip | all-ipv4 | all-ipv6} srcport-start <start-port> srcport-end <end-port> dstnet {<ip-address> | all-ip | all-ipv4 | all-ipv6} dstport-start <start-port> dstport-end <end-port> vlan <vlan-id>

Parameters

protocol	Specifies the protocol type. ▪ **tcp** - Specifies Transmission Control Protocol (TCP). This is the default. ▪ **udp** - Specifies User Datagram Protocol (UDP). ▪ **any** - Specifies both TCP and UDP.
srcnet	Specifies the IP address and mask for the traffic source. ▪ **<subnet>** - IPv4 or IPv6 address and mask. ▪ For IPv4 addresses, use this format: xxx.xxx.xxx.xxx/xx ▪ For IPv6 addresses, use this format: x:x:x::x/xxx ▪ **all-ip** - Specifies all IPv4 and IPv6 addresses. ▪ **all-ipv4** - Specifies all IPv4 addresses. ▪ **all-ipv6** - Specifies all IPv6 addresses.
srcport-start <start-port>	Specifies the starting port number for the traffic source.
srcport-end <end-port>	Specifies the ending port number for the traffic source.
dstnet	Specifies the IP address and mask for the traffic destination. ▪ **<subnet>** - IPv4 or IPv6 address and mask: ▪ For IPv4 addresses, use this format: xxx.xxx.xxx.xxx/xx ▪ For IPv6 addresses, use this format: x:x:x::x/xxx ▪ **all-ip** - Specifies all IPv4 and IPv6 addresses. ▪ **all-ipv4** - Specifies all IPv4 addresses. ▪ **all-ipv6** - Specifies all IPv6 addresses.
dstport-start <start-port>	Specifies the starting port number for the traffic destination.
dstport-end <end-port>	Specifies the ending port number for the traffic destination.
vlan <vlan-id>	Specifies the VLAN ID. ▪ **all** for all VLANs. ▪ **0** (zero) for untagged VLANs. ▪ VLAN numbers from 1 to 4094 for tagged VLANs.

Usage

Connection tracing rules let you determine to which SteelHeads the SteelHead Interceptor has redirected specific connections. Connection traces can be used as a debugging tool for troubleshooting issues with failing or unoptimized connections or connections requiring path selection.

Note: If you manually restart the SteelHead Interceptor, the connection traces are lost. Prior to restarting, perform a system dump.

The **no** command option disables connection tracing.

Example

```
amnesiac (config) # conn-trace rule protocol tcp srcnet 10.0.0.1/32 srcport-start 1234 srcport-end
4567 dstnet 10.0.0.2/32 dstport-start 7890 dstport-end 8890 vlan 20
```

Product

Interceptor

Related Commands

“show conn-trace”

interceptor communication allow-failure enable

Allows failure in active-passive SteelHead Interceptor deployments.

Syntax

[**no**] **interceptor communication allow-failure enable**

Parameters

None

Usage

Run this command on all SteelHead Interceptors on the active and passive links. You must also run the **steelhead communication allow-failure** command on all SteelHeads that point to the SteelHead Interceptors on which you ran this command.

This command replaces the **redirect allow-failure** command.

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

Example

```
amnesiac (config) # interceptor communication allow-failure enable
```

Product

Interceptor

Related Commands

“show interceptor communication”

interceptor communication interface

Configures the Interceptor interface.

Syntax

interceptor communication interface <interface>

Parameters

<interface>	Name of the interface the appliance uses to communicate with peer SteelHead Interceptors.

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 SteelHead Interceptor in your deployment.

This 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

Related Commands

“show steelhead name all”

interceptor communication multi-interface enable

Enables the neighbor multiple interface support.

Syntax

interceptor communication multi-interface enable

Parameters

None

Usage

This command replaces the **redirect multi-interface enable** command.

Example

```
amnesiac (config) # interceptor communication multi-interface enable
```

Product

Interceptor

Related Commands

“show interceptor communication,” “show steelhead name all”

interceptor name

Configures an Interceptor peer.

Syntax

interceptor name <host> {additional-ip <ip-address> | main-ip <ip-address> [port <port>] | port <port>}

Parameters

<host>	Hostname for a peer SteelHead Interceptor in-path interface. This is the interface you set when you run the **interceptor communication interface** command on the peer SteelHead Interceptor.
additional-ip <ip-address>	Specifies an additional IP address for the peer SteelHead Interceptor.
main-ip <ip-address>	Specifies the main IP address of the peer SteelHead Interceptor.
port <port>	Specifies the corresponding port for the peer SteelHead Interceptor. The default port is 7860.

Usage

This command replaces the **redirect peer name** command.

The **no** command option disables the connection to the peer SteelHead Interceptor.

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 in to 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. Log in to 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`

This command replaces the **redirect peer name** command.

Example

```
amnesiac (config) # interceptor name mypeer main-ip 10.10.10.1
```

Product

Interceptor

Related Commands

"show interceptor communication," "show steelhead name all"

---

steelhead communication ack-timer-cnt

Sets the number of intervals to wait for an acknowledgment (ACK).

Syntax

[no] steelhead communication ack-timer-cnt <integer>

Parameters

<integer>	Number of intervals.

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # steelhead communication ack-timer-cnt 5
```

Product

Interceptor

Related Commands

"show steelhead communication"

---

steelhead communication ack-timer-intvl

Sets the length of time to wait for an acknowledgment (ACK).

Syntax

[no] steelhead communication ack-timer-intvl <milliseconds>

Parameters

<milliseconds>	Length of the interval in milliseconds. The default value is 1000 milliseconds.

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # steelhead communication ack-timer-intvl 1500
```

Product

Interceptor

Related Commands

“show steelhead communication”

steelhead communication heartbeat enable

Configures SteelHead communication heartbeat settings.

Syntax

[no] steelhead communication heartbeat enable

Parameters

None

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # steelhead communication heartbeat enable
```

Product

Interceptor

Related Commands

“show steelhead communication”

steelhead communication interface

Sets the interface to use for Interceptor-to-SteelHead communication.

Syntax

steelhead communication interface <interface-name>

Parameters

<interface-name>	Interface name.

Usage

This command replaces the **in-path neighbor interface** command.

Note: Make sure you configure the SteelHead to communicate with this SteelHead Interceptor 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 in to 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

Related Commands

“show steelhead communication”

---

steelhead communication multi-interface enable

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, you must enable multiple interface support. If you enable multiple interface support, the following constraints apply:

- 5.0x SteelHeads must be running RiOS 5.0.7 or later.
- 5.5.x SteelHeads must be running RiOS 5.5.2 or later.
- Load-balancing rules apply only to the main IP address.

The **no** command option disables multiple interface support.

This command replaces the **in-path neighbor multi-interface enable** command.

Example

```
amnesiac (config) # steelhead communication multi-interface enable
```

Product

Interceptor

Related Commands

“show steelhead communication”

steelhead communication multi-interface load balance enable

Enables communication and load balancing across multiple SteelHead interfaces in an appliance cluster.

Syntax

[no] steelhead communication multi-interface load balance enable

Parameters

None

Usage

The **no** command option disables communication and load balancing across multiple SteelHead interfaces in an appliance cluster.

Example

```
amnesiac (config) # steelhead communication multi-interface load balance enable
```

Product

Interceptor, SteelHead

Related Commands

“Interceptor peering and redirect commands”

steelhead communication read-timeout

Sets the response wait time.

Syntax

[no] steelhead communication read-timeout <milliseconds>

Parameters

<milliseconds>	Length of the interval in milliseconds. The default value is 10000 milliseconds.

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # steelhead communication read-timeout 5000
```

Product

Interceptor

Related Commands

“show steelhead communication”

steelhead communication recon-timeout

Sets the time period to wait for a reconnect response.

Syntax

[no] steelhead communication recon-timeout <milliseconds>

Parameters

<milliseconds>	Length of the interval in milliseconds. The default value is 10000 milliseconds.

Usage

The **no** command option disables this setting.

Example

```
amnesiac (config) # steelhead communication recon-timeout 5000
```

Product

Interceptor

Related Commands

“show steelhead communication”

steelhead interceptor communication allow-failure enable

Enables the SteelHead Interceptor to continue to optimize connections when one or more of the peer Interceptors are unreachable.

Syntax

[no] steelhead interceptor communication allow-failure enable

Parameters

None

Usage

The **no** command option disables the allow-failure feature.

Note the following points:

- For parallel physical in-path deployments, where multiple paths to the WAN are covered by different SteelHead Interceptors, 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 Interceptors 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.
- By default, if a SteelHead Interceptor loses connectivity to a peer Interceptor, the SteelHead Interceptor stops attempting to optimize new connections. By using this command, the SteelHead Interceptor continues to optimize new connections, regardless of the state of its peer Interceptor.
- If the allow-failure feature is used in a parallel physical in-path deployment, SteelHead Interceptors only optimize those connections that are routed through the paths with operating SteelHead Interceptors. TCP connections that are routed across paths without SteelHead Interceptors (or with a failed SteelHead Interceptor) are detected by the asymmetric routing detection feature on the SteelHead.
- For physical in-path deployments, the allow-failure feature is commonly used with the fail-to-block feature (on supported hardware). When the fail-to-block feature is enabled, a failed SteelHead Interceptor blocks traffic along its path, forcing traffic to be rerouted onto other paths (where the remaining SteelHead Interceptors are

deployed). For details about configuring the allow-failure feature and the fail-to-block feature, see the *SteelHead Deployment Guide*.

- For virtual in-path deployments with multiple SteelHead Interceptors, including WCCP clusters, the connection forwarding and the allow-failure features must always be used. This is because certain events, such as network failures, and router or cluster changes, can cause routers to change the destination SteelHead Interceptor for TCP connection packets. When the destination changes, the SteelHead Interceptors must be able to redirect traffic to the SteelHead appliance to ensure that optimization continues.

Note: You must restart the service for your changes to take effect.

Example

```
amnesiac (config) # steelhead interceptor communication allow-failure enable
```

Product

SteelHead Interceptor

Related Commands

“show steelhead interceptor communication”

steelhead interceptor communication heartbeat enable

Configures the SteelHead Interceptor appliance communication heartbeat settings.

Syntax

[no] steelhead interceptor communication heartbeat enable

Parameters

None

Usage

When this command is enabled, the connection forwarding peer Interceptors 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 interceptor communication heartbeat enable
```

Product

SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-c

Related Commands

“show steelhead interceptor communication”

steelhead interceptor communication interface

Sets the interface to use for Interceptor-to-SteelHead communication.

Syntax

steelhead interceptor communication interface <interface-name>

Parameters

<interface-name>	Interface name.

Usage

This command replaces the **in-path neighbor interface** command.

Caution: Make sure you configure the SteelHead to communicate with this SteelHead Interceptor 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 in to the CLI for Interceptor A.
2. Specify which in-path interface on Interceptor A to use for Interceptor-to-SteelHead peering:
   ```
   steelhead interceptor 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 interceptor 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.

Note: Disable multiple interface support for the SteelHead Interceptor before changing the communication interface. To disable multiple interface support, use the **no steelhead interceptor communication multi-interface** command.

Example

```
amnesiac (config) # steelhead interceptor communication interface inpath0_0
```

Product

SteelHead Interceptor

Related Commands

“show steelhead interceptor communication”

steelhead interceptor communication mode-ipv6

Enables IPv6 connection forwarding between SteelHead Interceptors in an appliance cluster.

Syntax

[no] steelhead interceptor communication mode-ipv6

Parameters

None

Usage

Before using this command, these tasks are required:

- Path selection must be disabled. To disable path selection, use the **no path-selection enable** command.
- Remove all appliances from the connection forwarding appliance list and the failover appliance list. To remove an appliance from these lists, use the **no** command option with the appropriate CLI command (for example, **no interceptor name**, **no steelhead interceptor name** or **no failover steelhead interceptor name**).

The **no** option of this command disables IPv6 connection forwarding between SteelHead Interceptors in an appliance cluster.

Use this command on each SteelHead Interceptor in the cluster.

You must restart the service for your changes to take effect.

Example

```
amnesiac (config) # steelhead interceptor communication mode-ipv6
```

Product

Interceptor

Related Commands

“show steelhead interceptor communication”

steelhead interceptor communication multi-interface enable

Enables SteelHead Interceptor communication on multiple interfaces.

Syntax

[no] steelhead interceptor communication multi-interface enable

Parameters

None

Usage

When using more than one data connection on the SteelHead Interceptor, use this command to enable SteelHead Interceptor communication on multiple interfaces.

Note: If you enable SteelHead Interceptor communication on multiple interfaces, load-balancing and service rules apply only to the main IP address.

The **no** command option disables SteelHead Interceptor communication on multiple interfaces.

This command replaces the **in-path neighbor multi-interface enable** command.

Example

```
amnesiac (config) # steelhead interceptor communication multi-interface enable
```

Product

SteelHead Interceptor

Related Commands

“show steelhead interceptor communication”

steelhead interceptor name

Configures the SteelHead Interceptor hostname, IP address, and port number.

Syntax

[no] steelhead interceptor name <name> {main-ip <ip-address> | port <port> | additional-ip <ip-address>}

Parameters

<name>	Hostname of the SteelHead Interceptor.
main-ip <ip-address>	Specifies the main IP address of the SteelHead Interceptor. ▪ For IPv4 addresses, use this format: XXX.XXX.XXX.XXX/XX ▪ For IPv6 addresses, use this format: X:X:X::X/XXX
port <port>	Specifies the port of the SteelHead Interceptor.
additional-ip <ip-address>	Specifies an additional IP address for the SteelHead Interceptor. ▪ For IPv4 addresses, use this format: XXX.XXX.XXX.XXX/XX ▪ For IPv6 addresses, use this format: X:X:X::X/XXX

Usage

The **no** command option removes the SteelHead Interceptor hostname, IP address, or port number, if specified.

Important: You can enter either IPv4 or IPv6 addresses. However, if you have enabled IPv6 connection forwarding, you must enter an IPv6 address. For more information about enabling IPv6 connection forwarding, see the *SteelHead Interceptor User Guide*

Example

```
amnesiac (config) # steelhead interceptor name test main-ip 10.0.0.1 port 1234
```

Product

SteelHead Interceptor, SteelHead CX, SteelHead EX, SteelHead-c

Related Commands

“show steelhead interceptor name all”

steelhead name (Interceptor)

Configures Interceptor-to-SteelHead peering communication.

Syntax

[no] steelhead name <hostname> {additional-ip <ip-address> | main-ip <ip-address> [port <port> | paused] | paused | reset cap-adjustment {all | perm}}

Parameters

<hostname>	Hostname of the SteelHead neighbor peer.
additional-ip <ip-address>	Specifies an additional IP address for the neighbors. ▪ For IPv4 addresses, use this format: XXX.XXX.XXX.XXX/XX ▪ For IPv6 addresses, use this format: X:X:X::X/XXX
main-ip <ip-address>	Specifies the main IP address of the neighbor in-path X_X interface. ▪ For IPv4 addresses, use this format: XXX.XXX.XXX.XXX/XX ▪ For IPv6 addresses, use this format: X:X:X::X/XXX
port <port>	Specifies a port number for communication with the neighbor.
paused	Puts the SteelHead neighbor receiving the main connection forwarding into pause mode.
reset cap-adjustment	Resets capacity adjustment. ▪ **all** - Resets all capacity adjustments until the SteelHead returns to a normal pressure value. ▪ **perm** - Resets permanent capacity adjustment.

Usage

Important: You can enter either IPv4 or IPv6 addresses. However, if you have enabled IPv6 connection forwarding, you must enter an IPv6 address. For more information about enabling IPv6 connection forwarding, see the *SteelHead Interceptor User Guide*

This 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 adjustment is a SteelHead Interceptor strategy for relieving or avoiding pressure.

For detailed information about configuring connection forwarding, see the *SteelHead Deployment Guide*.

The **no** command option disables Interceptor-to-SteelHead peering communication and also removes the hostname.

Example

```
amnesiac (config) # steelhead name test main-ip 10.0.0.1 port 1234
```

Product

Interceptor

Related Commands

“show steelhead communication,” “show steelhead name all”

steelhead pressure-mon enable

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.

Example

```
amnesiac (config) # steelhead pressure-mon enable
```

Product

Interceptor

Related Commands

"show steelhead communication"

---

steelhead pressure-mon cap-reduction enable

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.

Example

```
amnesiac (config) # steelhead pressure-mon cap-reduction enable
```

Product

Interceptor

Related Commands

"show steelhead communication," "steelhead pressure-mon enable"

---

steelhead pressure-mon perm cap-reduction enable

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.

Example

```
amnesiac (config) # steelhead pressure-mon perm cap-reduction enable
```

Product

Interceptor

Related Commands

“show steelhead communication,” “steelhead pressure-mon enable”

steelhead pressure-mon perm cap-reduction events

Configures the 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>	Number of events.
time <seconds>	Specifies the number of seconds

Usage

You must first enable pressure monitoring with the **steelhead pressure-mon enable** command. Capacity reduction does not apply to a paused SteelHead.

Example

```
amnesiac (config) # steelhead pressure-mon perm cap-reduction events 3 time 10
```

Product

Interceptor

Related Commands

“show steelhead communication,” “steelhead pressure-mon enable”

Load-balancing in-path pass-through rules commands

This section describes the commands for configuring in-path pass-through rules for load balancing.

in-path passthrough move-rule

Moves an in-path pass-through rule.

Syntax

in-path passthrough move-rule rulenum <rule-number> to <rule-number>

Parameters

rulenum <rule-number>	Specifies the start of the rule-number range.
to <rule-number>	Specifies the end of the rule-number range.

Usage

Moves pass-through connection rules so that they can be optimized.

Example

```
amnesiac (config) # in-path passthrough move-rule rulenum 2 to 4
```

Product

Interceptor

Related Commands

"show in-path passthrough rules"

in-path passthrough rule allow

Configures an in-path load-balancing rule that allows pass-through traffic.

Syntax

in-path passthrough rule allow addr {<subnet> | all-ip | all-ipv4 | all-ipv6} port start <port> end <port> [description "<description>"] [rulenum <rule-number>] [vlan <vlan-id>]

Parameters

addr	Specifies the subnet IP address.
	▪ **<subnet>** - IPv4 or IPv6 address and mask:
	  ▪ For IPv4 addresses, use this format: xxx.xxx.xxx.xxx/xx
	  ▪ For IPv6 addresses, use this format: x:x:x::x/xxx
	▪ **all-ip** - Specifies all IPv4 and IPv6 addresses.
	▪ **all-ipv4** - Specifies all IPv4 addresses.
	▪ **all-ipv6** - Specifies all IPv6 addresses.

port start <port>	Specifies the starting port number of the port range.
end <port>	Specifies the ending port number of the port range.
description "<description>"	Specifies a description of the rule. Enclose the description in quotation marks.
rulenum <rule-number>	Specifies a rule number from 1 to N. The system evaluates 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>	Specifies the VLAN ID. ▪ **all** for all VLANs. ▪ **0** (zero) for untagged VLANs. ▪ VLAN numbers from 1 to 4094 for tagged VLANs.

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. Reseting connection rules 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.

You cannot use the GUI to configure the in-path load-balancing rules. You can only use the CLI to configure these rules.

Example

```
amnesiac (config) # in-path passthrough rule allow addr 10.0.0.1 port start 1 end 3 rulenum 1
```

Product

Interceptor

Related Commands

“show in-path passthrough rules”

in-path passthrough rule block

Configures an in-path load-balancing rule that blocks pass-through traffic.

Syntax

in-path passthrough rule block addr {<subnet> | all-ip | all-ipv4 | all-ipv6} port start <port> end <port> [description "<description>"] [rulenum <rule-number>] [vlan <vlan-id>]

Parameters

addr	Specifies the subnet IP address.
	▪ **<subnet>** - IPv4 or IPv6 address and mask:
	  ▪ For IPv4 addresses, use this format: xxx.xxx.xxx.xxx/xx
	  ▪ For IPv6 addresses, use this format: x:x:x::x/xxx
	▪ **all-ip** - Specifies all IPv4 and IPv6 addresses.
	▪ **all-ipv4** - Specifies all IPv4 addresses.
	▪ **all-ipv6** - Specifies all IPv6 addresses.

port start <port>	Specifies the starting port number of the port range.
end <port>	Specifies the ending port number of the port range.
description "<description>"	Specifies a description of the rule. Enclose the description in quotation marks.
rulenum <rule-number>	Specifies a rule number from 1 to N. The system evaluates 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>	Specifies the VLAN ID. ▪ **all** for all VLANs. ▪ **0** (zero) for untagged VLANs. ▪ VLAN numbers from 1 to 4094 for tagged VLANs.

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.

You cannot use the GUI to configure the in-path load-balancing rules. You can only use the CLI to configure these rules.

Example

```
amnesiac (config) # in-path passthrough rule block addr 10.0.0.1 port start 6509 end 6509 vlan 12
```

Product

Interceptor

Related Commands

“show in-path passthrough rules”

in-path passthrough rule edit

Edit an in-path pass-through rule description.

Syntax

in-path passthrough rule edit rulenum <rule-number> description "<description>"

Parameters

rulenum <rule-number>	Specifies the rule number to modify.
description "<description>"	Specifies a description of the rule. The description must be enclosed in quotation marks.

Usage

You cannot use the GUI to edit the in-path pass-through rule description. You can only use the CLI to edit the rule description.

Example

```
amnesiac (config) # in-path passthrough rule edit rulenum 2 description “blocks traffic to port 6509”
```

Product

Interceptor

Related Commands

“show in-path passthrough rules”

in-path rule edit

Edits an in-path pass-through rule and, optionally, enables or disables email reminders about in-path pass-through rules in use.

Syntax

in-path rule edit rulenum <rule-number> description "<description>" [email-notify {yes | no}]

Parameters

rulenum <rule-number>	Specifies the rule number to edit.
description "<description>"	Specifies the description for the rule. Enclose the description in quotation marks.
email-notify	Enables or disables reminders about in-path pass-through rules. ▪ **yes** - Sends email reminders every 15 days (the default). ▪ **no** - Does not send email reminders.

Usage

Email reminders apply only to pass-through rules. You can't use them for other types of rules.

If you use the **email-notify** keyword, you'll receive an email message reminding you that you have pass-through rules in use on your network, and asking you to check periodically whether you still need to use them. The email reminders help to identify any obsolete rules that you might want to delete to improve traffic optimization.

To receive email reminders, you must also use the **email notify passthrough rule enable** command.

By default, you'll receive email reminders every 15 days. To change the frequency, use the **notify-timer <frequency>** options of the **email notify passthrough rule enable** command.

The email reminders are sent to the addresses shown in the event email recipients field of the **show email** command.

Example

```
amnesiac (config) # in-path rule edit rulenum 9 description "this is a test"
```

Product

Interceptor

Related Commands

"email notify passthrough rule enable," "show email"

in-path rule pass-through email-notify

Specify whether an email reminder is needed for an in-path pass-through rule in use on your network.

Syntax

[no] in-path rule pass-through email-notify {yes | no}

Parameters

yes	Sends email reminders every 15 days (the default).
no	Does not send email reminders.

Usage

Pass-through rules are often created as a solution for a temporary network issue. When the issue is resolved, it's easy to forget that the rule is in use, which results in traffic not being optimized. With this command enabled, you'll receive an email message reminding you that you have pass-through rules in use on your network, and asking you to check periodically whether you still need to use them. The email reminders help to identify any obsolete rules that you might want to delete to improve traffic optimization.

This command is enabled by default and applies to in-path pass-through rules only.

To receive email reminders, you must also use the **email notify passthrough rule enable** command.

By default, you'll receive email reminders every 15 days. To change the frequency, use the **notify-timer <frequency>** options of the **email notify passthrough rule enable** command.

The email reminders are sent to the addresses shown in the event email recipients field of the **show email** command.

Important: To turn off email reminders for all pass-through rules (both in-path rules and load-balancing), use the **no email notify passthrough rule enable** command.

Example

```
amnesiac (config) # in-path rule pass-through email-notify yes
```

Product

Interceptor

Related Commands

email notify passthrough rule enable, in-path rule pass-through, no email notify passthrough rule enable, show email

in-path rule redirect

Creates rules for redirecting traffic along in-path routes.

Syntax

in-path rule redirect [description "<description>"] [dest {<**subnet>** | **all-ip** | **all-ipv4** | **all-ipv6 | ipv4 | ipv6**}] **[dest-port** {<**port>** | **Interactive | RBT-Protocol | Secure**}] **[rulenum <rule-number>] [src** {<**subnet>** | **all-ip** | **all-ipv4** | **all-ipv6**}] **[vlan <vlan-id>]**

Parameters

description "<description>"	Specifies a description of the rule. Enclose the description in quotation marks.

dest	Specifies the IP address and mask for the traffic destination.
	▪ **<subnet>** - IPv4 or IPv6 address and mask:
	  ▪ For IPv4 addresses, use this format: xxx.xxx.xxx.xxx/xx
	  ▪ For IPv6 addresses, use this format: x:x:x::x/xxx
	▪ **all-ip** - Specifies all IPv4 and IPv6 addresses.
	▪ **all-ipv4** - Specifies all IPv4 addresses.
	▪ **all-ipv6** - Specifies all IPv6 addresses.

dest-port	Specifies a destination port or port label for this rule.
	▪ **<port>** - a single port number or a comma-separated list of ports with or without ranges (for example, 1, 2, 4 -10,12).
	▪ A user-defined port label.
	  ▪ **Interactive** - Ports that belong to the system label for interactive ports.
	  ▪ **RBT-Proto** - Ports that belong to the label for system processes.
	  ▪ **Secure** - Ports that belong to the system label for secure ports.

rulenum <rule-number>	Specifies the rule number.

src	Specifies the IP address and mask for the traffic source.
	▪ **<subnet>** - IPv4 or IPv6 address and mask:
	  ▪ For IPv4 addresses, use this format: xxx.xxx.xxx.xxx/xx
	  ▪ For IPv6 addresses, use this format: x:x:x::x/xxx
	▪ **all-ip** - Specifies all IPv4 and IPv6 addresses.
	▪ **all-ipv4** - Specifies all IPv4 addresses.
	▪ **all-ipv6** - Specifies all IPv6 addresses.

vlan <vlan-id>	Specifies the VLAN ID. ▪ **-1** for all VLANs. ▪ **0** (zero) for untagged VLANs. ▪ VLAN numbers from 1 to 4094 for tagged VLANs.

Usage

This command lets you create rules for redirecting traffic to an in-path SteelHead.

You also have the option of entering a description for the rule and specifying the settings used for redirecting the traffic, such as the following:

- destination subnet
- port or port label
- rule number
- source subnet
- VLAN identification number

Example

```
amnesiac (config) # in-path rule redirect description “test” dest 10.0.0.0/16 dest-port 1240 src
10.0.0.0/16 vlan 12
```

Product

Interceptor

Related Commands

“load balance rule redirect”

Path selection support commands

RiOS 9.1 and later extends path selection to operate in SteelHead Interceptor cluster deployments, providing high scale and high availability deployment options. A SteelHead Interceptor cluster is one or more SteelHead Interceptors collaborating with one or more SteelHead appliances to select paths dynamically.

---

path-selection enable (Interceptor)

Enables path selection.

Syntax

[**no**] **path-selection enable**

Parameters

None

Usage

Path selection allows you to more accurately control traffic flow across multiple WAN circuits. Path selection is a transparent operation to the client, server, and any networking devices such as routers or switches.

This command enables path selection support in an Interceptor cluster. When path selection is enabled in a SteelHead Interceptor cluster, the cluster can transparently alter the next hop gateway for the client traffic.

Path selection must also be enabled on the SteelHeads in the cluster.

Path selection is disabled by default.

Use the **no** command option to disable path selection if it has been enabled.

Path selection does require a service restart.

For details about the path selection feature, see the *SteelHead User Guide*, the *SteelHead Deployment Guide*, and the *SteelHead Interceptor User Guide*.

Example

```
amnesiac (config) # path-selection enable
```

Product

SteelHead Interceptor

Related Commands

"show path-selection status"

service rule edit

Edits a service rule.

Syntax

service rule edit rulenum <rule-number> description <description>

Parameters

rulenum <rule-number>	Specifies the rule number to edit.
description <description>	Specifies the description for this rule.

Usage

Service rules are used with path selection. The service rules control which traffic flows are redirected for path selection and how the traffic flows are distributed to the SteelHead appliance clusters. The SteelHead chosen then matches its path selection rules to direct traffic to the appropriate uplink.

Path selection must be enabled for your changes to take effect. For details about path selection, see the *SteelHead User Guide*, the *SteelHead Deployment Guide*, and the *SteelHead Interceptor User Guide*.

Note: When specifying the description, use underscores (_) instead of spaces between words or enclose the entire description in quotation marks (").

Example

```
amnesiac (config) # service rule edit rulenum 2 description UDP_traffic_redirected
```

Product

SteelHead Interceptor

Related Commands

"show service rules"

service rule move

Moves a service rule.

Syntax

service rule move rulenum <rule-number> to <rule-number>

Parameters

rulenum <rule-number> to <rule-number>	Specifies the rule number to move and the destination to which the rule should be moved.

Usage

Path selection must be enabled for your changes to take effect. For details about path selection, see the *SteelHead User Guide*, the *SteelHead Deployment Guide*, and the *SteelHead Interceptor User Guide*.

Example

```
amnesiac (config) # service rule move rulenum 2 to 3
```

Product

Interceptor

Related Commands

“show service rules”

---

service rule passthrough

Configures a service pass-through rule.

Syntax

service rule passthrough [description <description>] [port1 {<port> | <port-label>}] [port2 {<port> | <port-label>}] [protocol {tcp | udp | any}] [rulenum <rule-number>] [subnet1 {<network> | all}] [subnet2 {<network> | all}] [vlan <vlan>]

Parameters

description <description>	Specifies the description for this rule.
port1 <port>	Specifies the first port number.
port1 <port-label>	Specifies the first port label. Valid values correspond to port labels defined previously.
port2 <port>	Specifies the second port.
port2 <port-label>	Specifies the second port label. Valid values correspond to port labels defined previously.
protocol	Specifies the protocol name or protocol type. Valid values are: ▪ **tcp** ▪ **udp** ▪ **any** (This is the default.)
rulenum <rule-number>	Specifies the rule number.
subnet1	Specifies the first subnet. Valid values are: ▪ **<network>** - IP address and mask for the service rule. Use the following format: XXX.XXX.XXX.XXX/XX ▪ **all** - Specifies all IPv4 addresses.
subnet2	Specifies the second subnet. Valid values are: ▪ **<network>** - IP address and mask for the service rule. Use the following format: XXX.XXX.XXX.XXX/XX ▪ **all** - Specifies all IPv4 addresses.
vlan <vlan>	Specifies the VLAN number. Valid values are: ▪ **all** for all VLANs. ▪ Zero (**0**) for untagged VLANs. ▪ VLAN numbers from 1 to 4094 for tagged VLANs.

Usage

You must enable the path selection feature for your changes to take effect. For details about the path selection feature, see the *SteelHead User Guide*, the *SteelHead Deployment Guide*, and the *SteelHead Interceptor User Guide*.

To delete a service rule, use the **no service rule rulenum <rule-number>** command.

Note: When specifying the description, use underscores (_) instead of spaces between words or enclose the entire description in quotation marks (“).

Example

```
amnesiac (config) # service rule passthrough description traffic_on_server_side_of_WAN port1
interactive port2 secure protocol any rulenum 10 subnet1 all subnet2 all vlan 4
```

Product

Interceptor

Related Commands

“show service rules”

service rule redirect

Configures a redirect service rule.

Syntax

service rule redirect addrs <addresses> [description <description>] [port1 {<port> | <port-label>}] [port2 {<port> | <port-label>}] [protocol {tcp | udp | any}] [rulenum <rule-number>] [subnet1 {<network> | all}] [subnet2 {<network> | all}] [vlan <vlan>]

Parameters

addrs <addresses>	Specifies one or more local SteelHead IP addresses (separated by commas) for redirection.
description <description>	Specifies the description for this rule.
port1 <port>	Specifies the first port number.
port1 <port-label>	Specifies the first port label. Valid values correspond to port labels defined previously.
port2 <port>	Specifies the second port number.
port2 <port-label>	Specifies the second port label. Valid values correspond to port labels defined previously.
protocol	Specifies the protocol name or protocol type. Valid values are: ▪ **tcp** ▪ **udp** ▪ **any** (This is the default.)
rulenum <rule-number>	Specifies the rule number.
subnet1	Specifies the first subnet. Valid values are: ▪ **<network>** - IP address and mask for the service rule. Use the following format: XXX.XXX.XXX.XXX/XX ▪ **all** - Specifies all IPv4 addresses.
subnet2	Specifies the second subnet. Valid values are: ▪ **<network>** - IP address and mask for the service rule. Use the following format: XXX.XXX.XXX.XXX/XX ▪ **all** - Specifies all IPv4 addresses.
vlan <vlan>	Specifies the VLAN number. Valid values are: ▪ **all** for all VLANs. ▪ Zero (**0**) for untagged VLANs. ▪ VLAN numbers from 1 to 4094 for tagged VLANs.

Usage

When entering the IP address of the local SteelHead, only the main IP address of the local SteelHead may be specified.

You must enable the path selection feature for your changes to take effect. For details about the path selection feature, see the *SteelHead User Guide*, the *SteelHead Deployment Guide*, and the *SteelHead Interceptor User Guide*.

Note: When specifying the description, use underscores (_) instead of spaces between words or enclose the entire description in quotation marks (“).

Example

```
amnesiac (config) # service rule redirect addrs 10.10.10.1 description redirect_remote_site1_to_SH1
subnet1 12.12.0.0/16
```

Product

Interceptor

Related Commands

“show service 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 (VLAN instance)” listed in the Product field.

---

vlan-seg enable

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

Related Commands

“instance,” “instance-config create,” “show detail,” “vlan add”

instance-config create

Creates a VLAN instance for VLAN segregation. An instance represents a logical Interceptor VLAN.

Syntax

[no] instance-config create <instance-name>

Parameters

<instance-name>	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

```
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

Related Commands

“instance,” “vlan-seg enable,” “show detail,” “vlan add”

instance-config rename

Renames a VLAN instance for VLAN segregation.

Syntax

instance-config rename <instance-name> to <new-instance-name>

Parameters

<instance-name>	Name of the VLAN instance.
to <new-instance-name>	New name of the VLAN instance.

Usage

The instance name must be a unique alphanumeric string, fewer than 24 characters.

Example

```
amnesiac (config) # instance-config rename foo to foobar
```

Product

Interceptor

Related Commands

"instance," "vlan-seg enable," "instance-config create," "vlan add," "show detail"

---

instance

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>	Name of the VLAN instance.

Usage

After entering instance configuration 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 steelhead interceptor name".
- **in-path passthrough {move-rule | rule}** - For details, see "in-path passthrough move-rule," "in-path passthrough rule allow," "in-path passthrough rule block,"and "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," and "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," and "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,"and "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," and "steelhead communication recon-timeout".
- **steelhead name** - For details, see "steelhead name (Interceptor)," and "steelhead pressure-mon enable".
- **vlan <id> add** - For details, see "vlan add".

Example

```
amnesiac (config)# instance foo
(instance-config)#
```

Product

Interceptor

Related Commands

"instance-config create," "show detail," "vlan add," "vlan-seg enable"

Instance configuration mode commands

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

Enables the instance for VLAN segregation.

Syntax

[no] enable

Parameters

None

Usage

The **no** command option disables the instance for VLAN segregation.

Example

```
amnesiac (config)# instance foo
(instance-config)# enable
```

Product

Interceptor (VLAN instance)

Related Commands

"instance-config create," "show detail," "vlan add," "vlan-seg enable"

---

restart

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 (VLAN instance)

Related Commands

“instance-config create,” “show detail,” “vlan add,” “vlan-seg enable”

vlan add

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>	VLAN identifier.

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 from 0 to 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 (VLAN instance)

Related Commands

“instance,” “instance-config create,” “show detail,” “vlan add,” “vlan-seg enable”

in-path move-rule

Moves an in-path pass-through rule.

Syntax

in-path move-rule rulenum <rule-number> to <rule-number>

Parameters

<rule-number> to <rule-number>	Specifies the rule number to move and the destination to which the rule should be moved.

Usage

Moves an in-path rule so that it can be optimized.

Example

```
(instance-config)# in-path move-rule 2 to 4
```

Product

Interceptor (VLAN instance)

Related Commands

“instance,” “instance-config create,” “show detail,” “vlan add,” “vlan-seg enable”

---

exit

Exit instance configuration mode.

Syntax

exit

Parameters

None

Usage

Exit instance configuration mode return to configuration mode for the appliance.

Example

```
(instance-config)# exit
amnesiac (config)#
```

Product

Interceptor (VLAN instance)

Related Commands

“instance,” “instance-config create,” “vlan add,” “vlan-seg enable,” “show detail”

Displaying Interceptor information

This section describes the commands for displaying SteelHead Interceptor settings. Most of the SteelHead **show** commands are also available in the SteelHead Interceptor. For detailed information, see Chapter 2, “User Mode Commands.”

---

show appliance operating-mode

Displays the operating mode in use on the appliance.

Syntax

show appliance operating-mode

Parameters

None

Usage

This command allows you to see the mode in use on a specific appliance and allows you to troubleshoot compatibility issues.

With this command, you can verify that a given appliance is using the correct operating mode. In a topology with a mixture of appliances (for example, a combination of 9350 and 9600 appliances), the 9600 appliance must be in 9350 operating mode for compatibility.

An alarm is generated if the correct operating mode is not enabled.

Example

In this example, the 9600 appliance is shown as being in 9350 operating mode.

```
amnesiac # show appliance operating-mode
Operating Mode: 9350
Model Number: 9600
```

Product

Interceptor

Related Commands

“appliance operating-mode 9350”

show conn-trace

Displays connection tracing details, connection tracing rules, or connection tracing summary information.

Syntax

show conn-trace {connection {protocol {tcp | udp | any} | srcaddr <ip-address> srcport <port> dstaddr <ip-address> dstport <port> vlan <vlan> | rule | summary}

Parameters

connection	Displays tracing details for one connection.
protocol	Specifies the protocol name or protocol type. Valid values are: ▪ **tcp** (This is the default.) ▪ **udp** ▪ **any**
srcaddr <ip-address>	Specifies the source IP address.
srcport <port>	Specifies the source port number for this connection.
dstaddr <ip-address>	Specifies the destination IP address for this connection.
dstport <port>	Specifies the destination port number for this connection.
vlan <vlan>	Specifies the VLAN number. Valid choices are: ▪ **all** for all VLANs. ▪ Zero (**0**) for untagged VLANs. ▪ VLAN numbers from 1 to 4094 for tagged VLANs.
rule	Displays connection tracing rules used for all connections.
summary	Displays connection tracing summary information.

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

Related Commands

“appliance operating-mode 9350”

---

show detail

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 (VLAN instance)

Related Commands

“instance,” “instance-config create,” “vlan add,” “vlan-seg enable”

---

show failover interceptor

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

Related Commands

“Interceptor failover support commands”

show in-path interfaces

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, SteelHead-c, Interceptor

Related Commands

“Load-balancing in-path pass-through rules commands”

show in-path oop

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

Related Commands

“Interceptor peering and redirect commands”

show in-path passthrough rules

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

Related Commands

“Load-balancing in-path pass-through rules commands”

---

show instances

Shows all instances configured for the appliance.

Syntax

show instances

Parameters

None

Usage

The instance name must be a unique alphanumeric string, fewer than 24 characters.

Example

```
amnesiac (config) # show instances
Name    State
====    =====
foo     Disabled
foobar  Enabled
```

Product

Interceptor

Related Commands

“instance,” “instance-config create,” “show detail”

---

show interceptor communication

Displays the interface the appliance uses to communicate with peers.

Syntax

show interceptor communication

Parameters

None

Usage

This 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

Related Commands

"Interceptor peering and redirect commands"

show interceptor name all

Displays status of redirect peers. Redirect peers include SteelHead Interceptors deployed in parallel to cover asymmetric routing, as well as a SteelHead Interceptor that functions as a failover interceptor.

Syntax

show interceptor name all [configured]

Parameters

configured	Displays only a list of configured peers.

Usage

This 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

Related Commands

"Interceptor peering and redirect commands"

show load balance fair-peer-v2

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

Related Commands

"Load-balancing commands"

show load balance rules

Displays information about one or more load-balancing rules.

Syntax

show load balance rules <rule-number> | all | default>

Parameters

detail	Displays detailed information about the load-balancing rule.
<rule-number>	Rule number to display. Valid values are from 1 to 65534.
all	Displays detailed information for all load-balancing rules.
default	Displays detailed information for the system-generated default load-balancing rule.

Example

```
amnesiac (config) # show load balance rules detail all
Rule Number: default (auto-created at start-up)
Creation date: n/a
Created by: n/a, logged in from: n/a
        Type                : auto
        Send periodic email : yes
        Source ip           : all-ip
        Destination ip      : all-ip
        Destination port    : all
        Vlan                : all
        Target              : auto
        Peer                : Any
        Fair Peering        : no
        Hit count           : 0
        Last hit time       : Never
        Counter clear time  : Never
0 user added rule(s)
```

Product

Interceptor

Related Commands

"Load-balancing commands"

show service rules

Displays service rule information.

Syntax

show service rules

Parameters

None

Example

```
amnesiac (config) # show service rules
#   T  Pro Subnet1           Port1      Subnet2           Port2      VLAN Local SteelHead(s)
--- -- --- ----------------- ---------- ----------------- ---------- ---- ------------------
1   P  ANY all               all        all               all        all  n/a
2   P  TCP all               all        all               Secure     all  n/a
3   P  ANY all               all        all               all        all  n/a
4   P  ANY all               all        all               all        all  n/a
5   P  ANY all               all        all               all        all  n/a
6   P  ANY all               all        all               all        all  n/a
7   P  ANY all               all        all               all        2    n/a
def P  ANY all               all        all               all        all  n/a
-------------------------------------------------------------------------------------------
7 user added rule(s)

 Type: R = redirect    P = passthrough
```

Product

SteelHead Interceptor

Related Commands

"show path-selection status," "Path selection support commands"

show steelhead communication

Displays SteelHead communication settings.

Syntax

show steelhead communication [**cf-timer**]

Parameter

cf-timer	Displays connection forwarding (CF) timer settings.

Usage

This command replaces the **show in-path neighbor** command.

Example

Example

```
amnesiac (config) # show steelhead communication
SteelHead Pressure Monitoring:            false
    Capacity Adjustment Enable:           true
    Permanent Capacity Adjustment Enable: false
```

```
SteelHead Interface:                      inpath0_0
Multiple Interface Support:               yes
Multiple Interface Load Balance Support:  no
Use IPv6 Neighbor Connections: yes
```

Product

Interceptor

Related Commands

"Interceptor peering and redirect commands"

show steelhead interceptor communication

Displays SteelHead Interceptor communication settings.

Syntax

show steelhead interceptor communication

Parameters

None

Example

```
amnesiac (config) # show steelhead interceptor communication
SteelHead Interceptor Interface: inpath0_0

Multiple Interface Support: yes
Optimize Connections When Peer SteelHead Interceptor Not Connected: no
Use IPv6 Neighbor Connections: yes
```

Product

Interceptor

Related Commands

"Interceptor peering and redirect commands"

show steelhead interceptor name all

Displays SteelHead Interceptor name settings.

Syntax

show steelhead interceptor name all [configured]

Parameters

configured	Displays name settings for the configured SteelHead Interceptors.

Example

```
amnesiac (config) # show steelhead interceptor name all
Peer                    Type Version       Backup               Last Reconnect
----------------------- ---- ------------- -------------------- ---------------
testname                I                  255.255.255.255:0    Never
                             Peer Status :  Connecting
                             Interface(s):  1.1.0.1:7860         Connecting

Type: 'I' = SteelHead Interceptor
      'F' = Failover
```

Product

Interceptor

Related Commands

“Interceptor peering and redirect commands”

show steelhead name all

Displays SteelHead name settings.

Syntax

show steelhead name all [brief | configured]

Parameters

brief	Displays limited information about the SteelHead.
configured	Displays name settings for the configured SteelHead.

Example

```
amnesiac (config) # show steelhead name all

SteelHead 1: Name: oak-vsh117
Version: Last Reconnect: Never
Optimized Connections: 0
Service Connections: 0
Status: Connecting
```

Product

SteelHead Interceptor

Related Commands

“Interceptor peering and redirect commands”

show xbridge

Displays the Xbridge settings.

Syntax

show xbridge

Parameters

None

Example

```
amnesiac > show xbridge
Xbridge currently enabled: false
Xbridge enabled after next boot: false
```

Product

SteelHead Interceptor

Related Commands

“xbridge enable”

SteelCentral Controller for SteelHead commands

This section describes the SteelCentral Controller for SteelHead (SCC) commands that are unique to the SCC.

Some of the SteelHead CLI commands are also available in the SCC; however, Riverbed strongly recommends that you do not use the CLI to configure the SCC, SCC features, or remote SteelHeads that you are monitoring and configuring using the SCC.

Riverbed strongly recommends that you use the SCC GUI to configure the Controller and remote SteelHeads that you are monitoring and configuring using the SCC.

See the "Product Overview" chapter in the *SteelCentral Controller for SteelHead User Guide* for information about compatibility between RiOS system versions and Controller versions.

SCC system administration commands

This section describes the Controller system administration commands.

---

alarm enable (SCC)

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.
- **cmc_daily_config_backup** - This alarm triggers when an SCC appliance configuration backup occurs.
- **cmc_external_config_backup_restore** - This alarm indicates that an SCC external configuration backup and restore failure occurred.
- **cmc_license_app_insufficient** - This alarm triggers if the Controller has insufficient licenses(s).
- **cmc_license_invalid** - This alarm triggers if one or more SCC licenses are invalid.
- **cmc_license_missing** - This alarm triggers if one or more SCC 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 SCC.
- **critical_temp** - Specifies whether 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.
- **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** - 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 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.
- **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 to 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 Controller 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 70ºC.

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

SCC

Related Commands

“alarm clear,” “alarm clear-threshold,” “alarm error-threshold,” “show alarm,” “show alarms”

SCC export commands

This section describes the export commands for the Controller.

export app_details

Exports appliance information for SCC 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>	Specifies 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>	Specifies 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>	An SCP/FTP URL. The exported file is always a compressed zip folder ending with a .zip extension. If you are scheduling a recurring job to export reports to a URL, it is recommended that you 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

SCC

Related Commands

“Displaying SCC information”

export statistics

Exports statistical information for SCC managed appliances to a remote email address or SCP/FTP location.

Syntax

export statistics [appliance <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>] [inboundids {all | default}] [outboundids {all | default}] [symmid <id>] [rdfgroup <group>] [filer <name>] [lun <lun>] [lid <id>] [iid <id>] [lunReportName <name>] [initReportName <name>] [blockReportName <name>] {to-email <email-address> | to-file {<scp://username:password@hostname/path/filename> | <ftp://username:password@hostname/path/filename>}}

Parameters

appliance <serial number>	Specifies 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>	Specifies 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>	Specifies 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>	Specifies the granularity of the specified report. Each granularity format has the following options: ▪ **300** - Exports 5-minute samples. ▪ **3600** - Exports 1-hour samples. ▪ **86400** - Exports 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>	Specifies the period for which to generate a report. Each period format has the following options: ▪ **month** - Exports last month's statistics. ▪ **week** - Exports last week's statistics. ▪ **day** - Specifies the day for the export. ▪ **hour** - Specifies the hour for the export. ▪ **last_calendar_month** - Specifies the last calendar month. ▪ **last_calendar_week** - Specifies the last calendar week. ▪ **last_calendar_day** - Specifies the last calendar day (yesterday).
start-time <start-time>	Specifies the start time for reporting statistics in the format 'YYYY/MM/DD HH:MM:SS'.
end-time <end- time>	Specifies the end time for reporting statistics in the following 'YYYY/MM/DD HH:MM:SS'.
report <report- name>	Specifies 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>	Specifies 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	Specifies one graph per appliance. This option creates a report graph for each specified appliance in the **appliance** parameter and for each appliance that is part of the group specified by the **group** parameter.
port <port-number>	Specifies 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>	Specifies response types for NFS. The response-type options are: **all**, **local**, **remote**, and **delayed**.
type <options>	Specifies 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>	Specifies 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**.
inboundids	Specifies a comma separated list of inbound QoS classes. The class options are: ▪ **all** - all classes ▪ **default** - default class
outboundids	Specifies a comma separated list of outbound QoS classes. The class options are: ▪ **all** - all classes ▪ **default** - default class
symmId <number>	Specifies the SRDF Symmetrix ID number.
rdfGroup <number>	Specifies the SRDF ID group number. This option is only available if **symmId** is specified.
filer <name>	Specifies the filer name used for SnapMirror optimization. A filer is a NetApp storage device.
lun <lun>	Specifies the LUN.
lid <id>	Specifies the LUN ID.
iid <id>	Specifies the initiator ID.
lunReportName <name>	Specifies the LUN I/O report name.
initReportName <name>	Specifies the initiator I/O report name.
blockReportName <name>	Specifies the block store report name.

to-email <email-address>	Exports the report to the specified email address.

to-file < scp:// username:password@hostname/path/filename>	Specifies 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

SCC

Related Commands

“Displaying SCC information”

export steelhead access_codes

Exports access codes for SteelHeads.

Syntax

export steelhead access_codes to-email <email-address>

Parameters

to-email <email-address>	Emails a CSV file with a list of configured SteelHeads and their authorization codes.

Usage

This command emails a CSV file with a list of configured SteelHeads and their authorization codes that enable the SCC to collect SteelFlow Web Transaction Analysis (WTA) data that can be sent to a SteelCentral AppResponse appliance. On the SteelCentral AppResponse appliance, import the authorization codes. You must have enabled REST API access and generated the codes before you run this command.

For detailed information about enabling REST API and configuring HTTP for SteelFlow WTA, see the *SteelCentral Controller for SteelHead User Guide*.

Example

```
amnesiac # export steelhead access_codes to-email jdoe@email.com
```

Product

SCC

Related Commands

"Displaying SCC information"

Displaying SCC information

This section describes the **show** commands that are unique to the SCC.

show cmc appliance

Displays settings for the specified appliance.

Syntax

show cmc appliance {common auth | <appliance> <serial-number>}

Parameters

common auth	Displays common managed appliance authentication settings.
<appliance>	Displays information about the specified appliance: **steelfusion-core**, **interceptor**, **shm-controller**, **steelhead**, **steelhead-ex**
<serial-number >	Serial number for the appliance.

Example

```
amnesiac (config) # show cmc appliance steelhead V78XW00067821F6
SteelHead V78XW00067821F6 (release-239-102-csh1)

   Connected:                 false
   Version:                   8.6.0-mainline#141
   Model:
   Parent Group:              CSH-QA
   Status:                    Disconnected: missing or invalid base license
   Reduction:                 Unavailable
   Comment:                   CCX-255 Model

   Optimization Policy:
   Networking Policy:
   Security Policy:
```

```
System Policy:
Branch Services Policy:

Auto-configuration:         false
Branch Managed:             false
User-specified Address:     release-239-103-csh1
Auto-registration Address:

Disable Auto-Upgrade:       false
```

Product

SCC

Related Commands

“CLI terminal configuration commands”

show cmc appliances

Displays settings for all Controllers.

Syntax

show cmc appliances [detail]

Parameters

detail	Displays detailed information for all appliances.

Example

```
amnesiac (config) # show cmc appliances
```

Product

SCC

Related Commands

“CLI terminal configuration commands”

show cmc autolicense status

Displays the status of the SCC 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

SCC

Related Commands

"CLI terminal configuration commands"

show cmc backup appsnaps status

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

SCC

Related Commands

"SteelCentral Controller for SteelHead commands"

show cmc backup config

Displays a list of backup files on the disk.

Syntax

show cmc backup config {local | status}

Parameters

local	Displays a list of backup files on disk.
status	Displays status of the configuration backup operation.

Example

```
amnesiac > show cmc backup config local
amnesiac > show cmc backup config status
idle
```

Product

SCC

Related Commands

"SteelCentral Controller for SteelHead commands"

show cmc backup server space

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

SCC

Related Commands

"SteelCentral Controller for SteelHead commands"

---

show cmc backup stats status

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

Controller

Related Commands

"SteelCentral Controller for SteelHead commands"

---

show cmc email notify appliance

Displays the SCC email notifications for appliances.

Syntax

show cmc email notify appliance

Parameters

None

Usage

None

Example

```
amnesiac >  show cmc email notify appliance
CMC Email Appliance Notification
Appliance State Notification:            no
Appliance Aggregate State Notification: no
        Aggregate Duration(seconds):    60
```

Product

SCC

Related Commands

"SteelCentral Controller for SteelHead commands"

show cmc group

Displays the specified Controller group settings.

Syntax

show cmc group <group-name>

Parameters

<group-name>	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

SCC

Related Commands

"CLI terminal configuration commands"

show cmc groups

Displays the specified Controller 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

SCC

Related Commands

"CLI terminal configuration commands"

show cmc monitored-port

Displays the information on a monitored port.

Syntax

show cmc monitored-port <port-number>

Parameters

<port-number>	Port number to monitor.

Example

```
amnesiac >  show cmc monitored-port 80
Port Number     Description
80              HTTP
```

Product

CMC

Related Commands

“SteelCentral Controller for SteelHead commands”

show cmc monitored-ports

Displays information on all monitored ports.

Syntax

show cmc monitored-ports

Parameters

None

Example

```
amnesiac >  show cmc monitored-ports
Port Number     Description
21              FTP
80              HTTP
139             CIFS:NetBIOS
443             SSL
445             CIFS:TCP
1352            Lotus Notes
1433            SQL:TDS
7830            MAPI
8777            RCU
8779            SMB2
8780            SMB2 Signed
10566           SnapMirror
```

Product

CMC

Related Commands

“SteelCentral Controller for SteelHead commands”

show cmc op-history

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

SCC

Related Commands

“SteelCentral Controller for SteelHead commands”

---

show cmc restore appsnaps status

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

SCC

Related Commands

Related Commands

“SteelCentral Controller for SteelHead commands”

---

show cmc restore config status

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

SCC

Related Commands

“SteelCentral Controller for SteelHead commands”

show cmc restore stats status

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

SCC

Related Commands

“SteelCentral Controller for SteelHead commands”

show cmc stats_api logging

Displays the SCC statistics service logging configuration.

Syntax

show cmc stats_api logging

Parameters

None

Example

```
amnesiac >  show cmc stats_api logging
Logging level: info
```

Product

SCC

Related Commands

“SteelCentral Controller for SteelHead commands”

show cmc upgrades_api logging

Displays the SCC upgrades service logging configuration.

Syntax

show cmc upgrades_api logging

Parameters

None

Example

```
amnesiac >  show cmc upgrades_api logging
Logging level: info
```

Product

SCC

Related Commands

“SteelCentral Controller for SteelHead commands”

SteelCentral Controller for SteelHead Mobile commands

This section describes the SteelCentral Controller for SteelHead Mobile (Mobile Controller) commands that are unique to the Mobile Controller 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 features.

Cluster commands

---

cluster detach

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

Mobile Controller

Related Commands

"aaa authentication login default," "**cluster join,**" "cluster remove"

cluster join

Adds a Mobile Controller to a cluster.

Syntax

cluster join <hostname> [<port>]

Parameters

<hostname>	Hostname of the Mobile Controller.
<port>	Port number. The default port is 7870.

Example

```
amnesiac (config) # cluster join mobilecontroller1234
Sending cluster join action to host:mobilecontroller1234:7870
```

Product

Mobile Controller

Related Commands

"aaa authentication login default," "cluster detach," "cluster remove"

cluster license checkout-count

Configures the global count of cluster licenses that can be checked out.

Syntax

[no] cluster license checkout-count <number>

Parameters

<number>	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

Mobile Controller

Related Commands

"show cluster licenses," "show cluster license settings"

cluster license high-threshold

Configures the threshold percentage to check out more licenses.

Syntax

[no] cluster license high-threshold <percentage>

Parameters

<percentage>	Numerical value representing percentage.

Usage

The **no** command option resets cluster license settings.

Example

```
amnesiac (config) # cluster license high-threshold 90
```

Product

Mobile Controller

Related Commands

“show cluster licenses,” “show cluster license settings”

cluster license initial-count

Configures cluster-wide setting of initial number of licenses that can be checked out.

Syntax

[no] cluster license initial-count <number>

Parameters

<number>	Number of licenses to check out.

Usage

The **no** command option resets cluster license settings.

Example

```
amnesiac (config) # cluster license initial-count 100
```

Product

Mobile Controller

Related Commands

“show cluster licenses,” “show cluster license settings”

cluster license low-threshold

Configures the threshold percentage to check in unused licenses.

Syntax

[no] cluster license low-threshold <percentage>

Parameters

<percentage>	Numerical value representing percentage.

Usage

The **no** command option resets cluster license settings.

Example

```
amnesiac (config) # cluster license low-threshold 70
```

Product

Mobile Controller

Related Commands

"show cluster licenses," "show cluster license settings"

cluster remove

Removes the Mobile Controller from the cluster.

Syntax

cluster remove <hostname> [port <port>]

Parameters

<hostname>	Hostname of the Mobile Controller.
port <port>	Specifies the port number. The default port is 7870.

Usage

Removes a remote host from the cluster.

Example

```
amnesiac (config) # cluster remove mobilecontroller1234
```

Product

Mobile Controller

Related Commands

"aaa authentication login default," "**cluster join,**" "cluster detach"

Policy commands

delete policy id

Deletes the specified policy from the Mobile Controller.

Syntax

delete policy id <id>

Parameters

<id>	Policy ID number.

Example

```
amnesiac (config) # delete policy id 1
```

Product

Mobile Controller

Related Commands

"show policy list"

policy assignment adpath

Configures policy assignment by Active Directory path.

Syntax

[no] policy assignment adpath <ad-path> policy_id <policy-id>

Parameters

<ad-path>	Active Directory path.
policy_id <policy-id>	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

Mobile Controller

Related Commands

“show policy assignments adpath”

policy assignment depid

Configures policy assignment by deployment ID.

Syntax

[no] policy assignment depid <deploy-id> policy_id <policy-id>

Parameters

<deploy-id>	Deployment ID.
policy_id <policy-id>	Specifies the policy ID number.

Usage

The **no** command option removes the policy assignment.

Example

```
amnesiac (config) # policy assignment depid 2566 policy_id 1
```

Product

Mobile Controller

Related Commands

“show policy assignments depid”

policy assignment removeall-adpth

Removes all the Active Directory path assignments.

Syntax

policy assignment removeall-adpath

Parameters

None

Example

```
amnesiac (config) # policy assignment removeall-adpth
```

Product

Mobile Controller

Related Commands

“show policy assignments adpath”

policy assignment removeall-depid

Removes all the deployment ID assignments.

Syntax

policy assignment removeall-depid

Parameters

None

Example

```
amnesiac (config) # policy assignment removeall-depid
```

Product

Mobile Controller

Related Commands

“show policy assignments depid”

policy id advanced

Configures advanced policy assignment settings.

Syntax

[no] policy id <id> advanced {nat-port <port-number> | service-port <port-number>}

Parameters

<id>	Policy ID number.
nat-port <port-number>	Specifies the in-path NAT port number.
service-port <port-number>	Specifies 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

Mobile Controller

Related Commands

“show policy id”

policy id branch-warming enable

Enables branch warming for a specified policy.

Syntax

[no] policy id <id> branch-warming enable

Parameters

<id>	Policy ID number.

Usage

Branch warming requires SteelHead Mobile product family v3.0 or later.

You must also enable branch warming on the SteelHead. For detailed information, see the Management Console online help or the *SteelHead User Guide*.

The **no** command option disables branch warming.

Example

```
amnesiac (config) # policy id 1 branch-warming enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id cifs enable

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>	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 suboptimal conditions on the server-side SteelHead Mobile product family 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 User Guide*.

Example

```
amnesiac (config) # policy id 1 cifs dw-throttling enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id citrix enable

Enables Citrix optimization support on the specified policy.

Syntax

[no] policy id <id> citrix enable

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables Citrix optimization support.

For detailed information about CIFS, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 citrix enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id citrix ica

Configures Citrix ICA settings on the specified policy.

Syntax

[no] policy id <id> citrix ica port <port-number>

Parameters

<id>	Policy ID number.
port <port>	Specifies the ICA optimization port number.

Usage

The **no** command option disables Citrix ICA support.

For detailed information about CIFS, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 citrix ica port 1494
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id citrix secure-ica enable

Enables Citrix secure ICA support on the specified policy.

Syntax

[no] policy id <id> citrix secure-ica enable

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables Citrix secure ICA support.

For detailed information about CIFS, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 citrix secure-ica enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id citrix session reliability port

Configures the Citrix session reliability port on the specified policy.

Syntax

[no] policy id <id> citrix session reliability port <port>

Parameters

<id>	Policy ID number.
<port>	Port number.

Usage

The **no** command option disables Citrix session reliability support.

For detailed information about CIFS, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 citrix session reliability port 2598
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id citrix smallpkts enable

Enables Citrix small packet optimization.

Syntax

[no] policy id <id> citrix smallpkts enable

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables Citrix small packet optimization.

For detailed information about Citrix optimization, see the *SteelHead Management Console User Guide*.

Example

```
amnesiac (config) # policy id 1 citrix smallpkts enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id citrix smallpkts threshold

Specifies the threshold used for small packet optimization.

Syntax

[no] policy id <id> citrix smallpkts threshold <threshold>

Parameters

<id>	Policy ID number.
<threshold>	Maximum packet length in bytes. The default is 64. **Note:** For the **no** command option, this variable is not applicable and is not included in the command syntax.

Usage

This command does not limit the threshold value to a specific range.

The **no** command option resets the threshold to 64 (the default).

For more information about Citrix optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 citrix smallpkts threshold 15
```

The following is an example of the **no** command option. Notice that the **<threshold>** variable is not used in the command syntax.

```
amnesiac (config) # no policy id 1 citrix smallpkts threshold
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id connection lan receive buf-size

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>	Policy ID number.
<bytes>	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 User Guide*.

Example

```
amnesiac (config) # policy id 1 connection lan receive buf-size 1000000
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id connection lan send buf-size

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>	Policy ID number.
<bytes>	LAN send buffer size. The default value is 81920.

Usage

For detailed information about high-speed TCP, see the *SteelHead User Guide*.

Example

```
amnesiac (config) #policy id 1 connection lan send buf-size 1000000
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id connection wan receive def-buf-size

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>	Policy ID number.
<bytes>	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 User Guide*.

Example

```
amnesiac (config) # policy id 1 connection wan receive def-buf-size 3875000
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id connection wan send def-buf-size

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>	Policy ID number.
<bytes>	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 User Guide*.

Example

```
amnesiac (config) # policy id 1 connection wan send def-buf-size 3875000
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id endpoint controller add

Adds the Mobile Controller to the policy.

Syntax

policy id <id> endpoint controller add <controller-name> port <port>

Parameters

<id>	Policy ID number.
<controller-name>	Mobile Controller name.
port <port>	Specifies 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

Mobile Controller

Related Commands

“show policy id”

policy id endpoint controller auto-update

Automatically updates the list of Mobile Controllers for the specified policy in a Mobile Controller cluster.

Syntax

policy id <id> endpoint controller auto-update

Parameters

<id>	Policy ID number.

Usage

The **no** command option stops automatically updating the list of Mobile Controllers in a Mobile Controller cluster.

Example

```
amnesiac (config) # policy id 1 endpoint controller auto-update
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id endpoint controller randomize

Configures random ordering of Mobile Controllers when connecting.

Syntax

policy id <id> endpoint controller randomize

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables the randomize feature.

Example

```
amnesiac (config) # policy id 1 endpoint controller randomize
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id endpoint controller remove

Removes the Mobile Controller from the policy.

Syntax

policy id <id> endpoint controller remove <controller-name>

Parameters

<id>	Policy ID number.
<controller-name>	Mobile Controller name.

Example

```
amnesiac (config) # policy id 1 endpoint controller remove smc.example.com
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id endpoint controller remove-all

Removes all Mobile Controllers from the policy.

Syntax

policy id <id> endpoint controller remove-all

Parameters

<id>	Policy ID number.

Example

```
amnesiac (config) # policy id 1 endpoint controller remove-all
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id endpoint datastore-size

Configures the data store size on the endpoint client.

Syntax

policy id <id> endpoint datastore-size <datastore-size>

Parameters

<id>	Policy ID number.
<datastore-size>	Data store size. Valid range is from 256 MB to 20 GB.

Usage

The **no** command option disables the data store size.

Example

```
amnesiac (config) # policy id 1 endpoint datastore-size 400
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id endpoint dis-chksum-offl

Disables checksum off-loading for TCP/IP operations.

Syntax

[no] policy id <id> endpoint dis-chksum-offl

Parameters

<id>	Policy ID number or name.

Usage

Requires a client reboot.

Example

```
amnesiac (config) # policy id 1 endpoint dis-chksum-offl
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id endpoint kickoff

Configures the service to kick off the connections of the specified process.

Syntax

[no] policy id <id> endpoint kickoff <process-name>

Parameters

<id>	Policy name or number.
<process-name>	Kickoff process name.

Usage

The **no** command option disables the kickoff process.

For detailed information about the kickoff feature, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 endpoint kickoff testkickoff
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id endpoint max-log-files

Sets the maximum number of log files.

Syntax

[no] policy id <id> endpoint max-log-files <value>

Parameters

<id>	Policy name or number.
<value>	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

Mobile Controller

Related Commands

"show policy id"

policy id endpoint max-log-size

Sets the maximum size of the log files.

Syntax

[no] policy id <id> endpoint max-log-size <number-of-kilobytes>

Parameters

<id>	Policy name or number.
<number-of-kilobytes>	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

Mobile Controller

Related Commands

"show policy id"

policy id endpoint override-opt

Allows the user to modify optimization settings on the endpoint client.

Syntax

[no] policy id <id> endpoint override-opt

Parameters

<id>	Policy name or number.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # policy id 1 endpoint override-opt
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id endpoint show-tray-icon

Displays the client in the system tray.

Syntax

[no] policy id <id> show-tray-icon

Parameters

<id>	Policy name or number.

Usage

The **no** command option disables this feature.

Example

```
amnesiac (config) # policy id 1 endpoint show-tray-icon
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id eos moh enable

Enables bandwidth and latency optimization for the MAPI over HTTP transport protocol for the specified policy.

Syntax

[no] policy id <policy-id> eos moh enable

Parameters

<policy-id>	Policy identification number.

Usage

Microsoft implemented the MAPI over HTTP transport protocol in Exchange Server 2013 SP1 and Outlook 2013 SP1, and added support to Outlook 2010 update (see Knowledge Base article 2878264). MAPI over HTTP improves reliability and stability of connections by moving the transport layer to the HTTP model.

This command enables bandwidth and latency optimization to support this protocol for the specified policy. This command is disabled by default.

Note: For SteelHeads, enter this command on the client-side SteelHead to enable bandwidth and latency optimization for the MAPI over HTTP transport protocol. For the Mobile Controller, enter this command on the server-side SteelHead.

You must also create an in-path rule using the Exchange Autodetect latency optimization policy to differentiate and optimize this traffic.

For MAPI transport protocol optimization, enable SSL optimization and install the SSL server certificate for the Exchange Server on the server-side SteelHead.

Note: For SteelHeads, both the client-side and server-side SteelHeads must be running RiOS 9.2 for MAPI over HTTP latency optimization. For the Mobile Controller, only the server-side SteelHeads must be running RiOS 9.2 for MAPI over HTTP latency optimization.

If you pair a SteelHead running RiOS 9.2 with a SteelHead running 9.1, only HTTP bandwidth optimization is supported.

Example

```
amnesiac (config) # policy id 1 eos moh enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

"in-path rule auto-discover," "in-path rule pass-through"

policy id eos moh down-negotiate enable

Enables the system to down negotiate from MAPI over HTTP optimization to Outlook Anywhere optimization for the specified policy.

Syntax

[no] policy id <policy-id> eos moh down-negotiate enable

Parameters

<policy-id>	Policy identification number.

Usage

This command allows the system to negotiate down from the MAPI over HTTP protocol optimization to the existing Outlook Anywhere optimization for the specified policy.

You must also create an in-path rule using the Exchange Autodetect latency optimization policy to differentiate and optimize this traffic.

You can use this command on either a SteelHead or a Mobile Controller.

For SteelHead, this command is used only for the client-side SteelHead. To negotiate down, the client-side SteelHead must be running RiOS 9.1 or later, and the server-side SteelHead must be running RiOS 6.5 or later.

For the Mobile Controller, the server-side SteelHeads must be running RiOS 9.2 or later for MAPI over HTTP latency optimization.

Example

```
amnesiac (config) # policy id 1 eos moh down-negotiate enable
```

Product

SteelHead CX, SteelHead EX, SteelHead-v, SteelHead-c, Mobile Controller

Related Commands

“in-path rule auto-discover,”“in-path rule fixed-target,” “policy id eos moh enable”

policy id ftp port

Configures FTP settings on the specified policy.

Syntax

[no] policy id <id> ftp port <port>

Parameters

<id>	Policy ID number.
<port>	Port number.

Usage

The **no** command option removes the FTP port from the list.

Example

```
amnesiac (config) # policy id 1 ftp port 259
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id http add-cookie

Enables cookies in the HTTP optimization process on the specified policy.

Syntax

[no] policy id <id> http add-cookie

Parameters

<id>	Policy ID number.

Usage

The **no** command option disallows cookies.

For detailed information about HTTP optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 http add-cookie
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id http enable

Enables HTTP protocol optimization support on the specified policy.

Syntax

[no] policy id <id> http enable

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables HTTP protocol optimization support.

For detailed information about HTTP optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 http enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id http insrt-keep-aliv

Adds the keepalive option to the HTTP optimization on the specified policy.

Syntax

[no] policy id <id> http insrt-keep-aliv

Parameters

<id>	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 User Guide*.

Example

```
amnesiac (config) # policy id 1 http insrt-keep-aliv
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id http metadata-resp max-time

Configures the maximum time metadata response settings on the specified policy.

Syntax

[no] policy id <id> http metadata-resp max-time <seconds>

Parameters

<id>	Policy ID number.
<seconds>	Number of seconds.

Usage

The **no** command option disables the maximum response time settings.

For detailed information about HTTP optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 http metadata-resp max-time 120
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id http metadata-resp min-time

Configures the minimum time for metadata response settings on the specified policy.

Syntax

[no] policy id http metadata-resp min-time <seconds>

Parameters

<id>	Policy ID number.
<seconds>	Number of seconds.

Usage

The **no** command option disables the minimum response time settings.

For detailed information about HTTP optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 http metadata-resp min-time 20
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id http metadata-resp mode

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>	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 User Guide*.

Example

```
amnesiac (config) # policy id 1 http metadata-resp mode all
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id http prefetch extension

Configures prefetch extensions on the specified policy.

Syntax

[no] policy id <id> http prefetch extension <extension>

Parameters

<id>	Policy ID number.
<extension>	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 User Guide*.

Example

```
amnesiac (config) # policy id 1 http prefetch extension png
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id http prefetch tag attribute

Configures the tag attributes to prefetch on the specified policy.

Syntax

[no] policy id <id> http prefetch tag <tag> attribute <attribute>

Parameters

<id>	Policy ID number.
<tag >	Tag to add or modify.
<attribute>	Tag attribute.

Usage

The **no** command option disables the HTTP prefetch option.

For detailed information about HTTP optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 http prefetch tag body attribute background
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id http server-table

Configures the HTTP protocol settings in the server table for the specified policy.

Syntax

[no] policy id <id> http server-table [default | hostname {<name> | all} | subnet {<subnet> | all-ipv4 | all-ipv6}] [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	Specifies one of the following networks for the HTTP server subnet: ▪ **<subnet>** - Subnet address. For an IPv4 subnet, use the format X.X.X.X/<0-32>. For an IPv6 subnet, use the format X:X:X::X/<0-128>. **Note:** IPv6 is not currently supported on the Mobile Controller. ▪ **all-ipv4 -** Specifies all IPv4 networks. ▪ **all-ipv6 -** Specifies all IPv6 networks.
hostname <name>	Specifies a specific hostname.
hostname all	Specifies all hostnames.
obj-pref-table	Enables (**yes**) or disables (**no**) 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 responds to these IMS checks and HTTP requests, reducing round trips across the WAN. The Object Prefetch Table is disabled by default.
parse-prefetch	Enables (**yes**) or disables (**no**) the Parse-and-Prefetch option, which parses the base HTML page received from the server and prefetches any embedded objects to the client-side SteelHead. 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 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. Parse-and-Prefetch is enabled by default.
url-learning	Enables (**yes**) or disables (**no**) URL Learning, which learns associations between a base URL request and a follow-on request. This option 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 your system is using HTTP v1.0 (with no keepalives), you can force the use of cookies by using the **insert-cookie** option and force the use of persistent connections using the **insrt-keep-aliv** option.

reuse-auth	Allows (**yes**) or disallows (**no**) 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	Adds (**yes**) credentials to the request on an already authenticated connection or removes (**no**) 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. **Caution:** If the web server is configured to use per-request NTLM authentication, enabling this option might cause authentication failure.
gratuitous-401	Enables (**yes**) or disables (**no**) gratuitous-401 settings. When set to **Yes**, the system prevents a WAN round trip by issuing the first 401 containing the realm choices from the client-side SteelHead. 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. **Caution:** 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, requires (**yes**) NTLM or does not (**no**) require NTLM. Allows use of Kerberos. However, 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 option is disabled by default.
strip-compress	Enables (**yes**) strip compression or disables (**no**) strip compression. Strip compression 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 data-reduction algorithms. This option is enabled by default.

insert-cookie	Enables (**yes**) the ability to add cookies to HTTP applications if needed or disables (**no**) this ability. HTTP applications frequently use cookies to monitor sessions. The SteelHead uses cookies to distinguish one user session from another. If an HTTP application does not use cookies, the client SteelHead inserts one so that it can track requests from the same client. This option is disabled by default.
insrt-keep-aliv	Enables (**yes**) the keep alive function or disables (**no**) this function. When this function enabled, the system uses 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 option is disabled by default.
FPSE	Enables (**yes**) or disables (**no**) SharePoint Front Page Server Extensions Protocol (FPSE) on a subnet or hostname. This option is case sensitive and is disabled by default. **Caution:** FPSE requests can introduce significant delays in retrieving a target document from the SharePoint site.
WebDAV	Enables (**yes**) or disables (**no**) 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 option is case sensitive and is disabled by default.
FSSHTTP	Enables (**yes**) or disables (**no**) SharePoint File Synchronization via SOAP over HTTP (FSSHTTP) on a subnet or hostname. This option is case sensitive and is enabled 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)# policy id 73128452008 http server-table subnet 10.10.10.10/32 FPSE yes WebDAV yes
```

Product

Mobile Controller

Related Commands

"show policy id," "show policy id http server-table"

policy id http strip-compress

Configures HTTP strip compression options.

Syntax

[no] policy id <id> http strip-compress

Parameters

<id>	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 User Guide*.

Example

```
amnesiac (config) # policy id 1 http strip-compress
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id in-path rule auto-discover

Adds an auto-discovery rule to a policy.

Syntax

policy id <id> in-path rule auto-discover [srcaddr <subnet>] [dstaddr <subnet>] [dstport <port>] [dst-host <host-label>][optimization <policy>] [preoptimization <policy>] [latency-opt <policy>][cloud-accel <mode>] [neural-mode <mode>] [wan-visibility <mode>] [description <description>] [rulenum <rule-number>]

Parameters

<id>	Policy ID number.
srcaddr <subnet>	Specifies the source subnet, in the format xxx.xxx.xxx.xxx/xx.
dstaddr <subnet> **dstport <port>**	Specifies 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.
dst-host <host-label>	Specifies a destination host label for this rule. You configure the host label settings using the **host-label** command. A destination IP address and host label cannot be specified in the same rule. A host label can be used instead of a destination IP address. Enter an empty string, represented by two quotation marks (""), to remove a host label.
optimization <policy>	Specifies 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 Mobile 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 <policy>	Specifies a preoptimization policy: ▪ **ssl** - Enables SSL preoptimization processing for traffic via SSL secure ports. ▪ **oracle-forms** - Enables preoptimization processing for the Oracle Forms browser plug-in. ▪ **oracle-forms+ssl** - Enables preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side SteelHead Mobile. ▪ **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 <policy>	Specifies 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** - Performs HTTP optimization on connections matching this rule. ▪ **normal** - Performs 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.

cloud-accel <mode>	Applies only if you have subscribed to a Software as a Service (SaaS) platform. Specifies a cloud-acceleration 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 SteelHead SaaS. You do not need to add an in-path rule unless you want to optimize specific users and not others. Specify one of these modes: ▪ **auto** - If the in-path rule matches, the connection is optimized by the Riverbed SteelHead Cloud Accelerator (SCA) connection. ▪ **passthru** - If the in-path rule matches, the connection is not optimized by the SteelHead SaaS, but it follows the rule's other parameters so that the connection might be optimized by this SteelHead with other SteelHeads in the network, or it might be passed through. Domain labels and cloud acceleration are mutually exclusive except when the **_cloud-accel-saas** host label is used. To use cloud acceleration with domain labels, we recommend placing the domain label rules lower than cloud acceleration rules in your rule list so the cloud rules match before the domain label rules.
neural-mode <mode>	Enables neural framing in the SteelHead Mobile. 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 SteelHead Mobile 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** - Bases the 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 SteelHead Mobile (where the connection is initiated). The server-side SteelHead must also support WAN visibility. ▪ **correct** - Turns off WAN visibility. Correct addressing uses SteelHead Mobile 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** - Enables port address transparency, which 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 Mobiles 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 SteelHead Mobiles. **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 SteelHead Mobiles 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 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>	Specifies a description of the rule.
rulenum <rule-number>	Specifies 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 User 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

Mobile Controller

Related Commands

"show policy id"

policy id in-path rule edit rulenum auto-discover

Edits an auto-discovery rule on the specified policy.

Use the auto-discovery process to determine if a remote SteelHead Mobile 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 <rule-number> auto-discover [srcaddr <subnet>] [dstaddr <subnet>] [dstport <port>] [dst-host <host-label>] [preoptimization <policy>] [optimization <policy>] [latency-opt <policy>] [cloud-accel <mode>] [neural-mode <mode>] [wan-visibility <mode>] [description <description>] [rule-enable {true | false}]

Parameters

<id>	Policy ID number.
<rule-number>	Rule number to edit: **1- <n>**, **start**, or **end**.
srcaddr <subnet>	Specifies the source subnet in the format xxx.xxx.xxx.xxx/xx.
dstaddr <subnet> **dstport <port>**	Specifies 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.
dst-host <host-label>	Specifies a destination host label for this rule. You configure the host label settings using the **host-label** command. A destination IP address and host label cannot be specified in the same rule. A host label can be used instead of a destination IP address. Enter an empty string, represented by two quotation marks (""), to remove a host label.

preoptimization <policy>	Specifies 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 SteelHead Mobile. ▪ **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**.
optimization <policy>	Specifies an optimization policy: ▪ **normal** - The **normal** optimization policy is the default. The normal process performs LZ compression and SDR. ▪ **sdr-only** - Turns off LZ compression. ▪ **sdr-m** - Performs data reduction entirely in memory, which prevents the SteelHead Mobile 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** - Turns off SDR but performs LZ compression. ▪ **none** - Turns off LZ compression and SDR.
latency-opt <policy>	Specifies 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** - Performs HTTP optimization on connections matching this rule. ▪ **normal** - Performs 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.

cloud-accel <mode>	Applies only if you have subscribed to a Software as a Service (SaaS) platform. Specifies a cloud-acceleration 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 SteelHead SaaS. You do not need to add an in-path rule unless you want to optimize specific users and not others. Specify one of these modes: ▪ **auto** - If the in-path rule matches, the connection is optimized by the Riverbed SteelHead Cloud Accelerator (SCA) connection. ▪ **passthru** - If the in-path rule matches, the connection is not optimized by the SteelHead SaaS, but it follows the rule's other parameters so that the connection might be optimized by this SteelHead with other SteelHeads in the network, or it might be passed through. Domain labels and cloud acceleration are mutually exclusive except when the **_cloud-accel-saas** host label is used. To use cloud acceleration with domain labels, we recommend placing the domain label rules lower than cloud acceleration rules in your rule list so the cloud rules match before the domain label rules.
neural-mode <mode>	Enables neural framing in the SteelHead Mobile. 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 SteelHead Mobile 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 <mode>

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 SteelHead Mobile (where the connection is initiated). The server-side SteelHead must also support WAN visibility.

- **correct** - Turns WAN visibility off. Correct addressing uses SteelHead Mobile 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 SteelHead Mobiles 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 SteelHead Mobiles.

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 SteelHead Mobiles 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 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-visibility <mode>	▪ **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.
description <description>	Specifies 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 and how to configure WAN visibility, see the *SteelHead User Guide* and the *SteelHead Deployment 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

Mobile Controller

Related Commands

“show policy id”

policy id in-path rule deny

Adds an in-path rule that rejects connection requests on the specified policy.

Syntax

[no] policy id <id> in-path rule deny [srcaddr <subnet>] [dstaddr <subnet>] [dstport <port>] [rulenum <rule-number>] [description <description>]

Parameters

<id>	Policy ID number.
srcaddr <subnet>	Specifies the source subnet for this rule: for example, 1.2.3.4/32
dstaddr <subnet> dstport <port>	Specifies 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 <rule-number>	Specifies 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>	Specifies a description of the rule.

Usage

The SteelHead Mobile 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 User 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

Mobile Controller

Related Commands

“show policy id”

policy id in-path rule discard

Adds an in-path rule that drops connections on the specified policy.

Syntax

[no] policy id <id> in-path rule discard [srcaddr <subnet>] [dstaddr <subnet>] [dstport <port>] [rulenum <rule-number>] [description <description>]

Parameters

<id>	Policy ID number.
srcaddr <subnet>	Specifies the source subnet for this rule, in the format XXX.XXX.XXX.XXX/XX.
dstaddr <subnet> dstport <port>	Specifies 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 <rule-number>	Specifies 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>	Specifies a description of the rule.

Usage

The SteelHead Mobile 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 User 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

Mobile Controller

Related Commands

“show policy id”

policy id in-path rule edit rulenum deny

Edits an in-path rule that rejects connection requests on the specified policy.

Syntax

policy id <id> in-path rule edit rulenum <rule-number> deny [srcaddr <subnet>] [dstaddr <subnet>] [dstport <port>] | [description <description>] [rule-enable {true | false}]

Parameters

<id>	Policy ID number.
rulenum <rule-number>	Specifies the rule number to edit: **1-N** or **start** or **end**.
srcaddr <subnet>	Specifies the source subnet for this rule: for example, **1.2.3.4/32**
dstaddr <subnet> dstport <port>	Specifies 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>	Specifies 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 User 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

Mobile Controller

Related Commands

“show policy id”

policy id in-path rule edit rulenum discard

Edits an in-path rule that drops connections on the specified policy.

Syntax

[no] policy id <id> in-path rule edit rulenum <rulenum> discard [srcaddr <subnet>] [dstaddr <subnet>] [dstport <port>] | [description <description>] [rule-enable {true | false}]

Parameters

<id>	Policy ID number.
rulenum <rulenum>	Rule number to edit: **1-N** or **start** or **end**.
srcaddr <subnet>	Specifies the source subnet, for this rule in the format XXX.XXX.XXX.XXX/XX.
dstaddr <subnet> dstport <port>	Specifies 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>	Specifies a description of the rule.
rule-enable	Enables (**true**) or disables (**false**) an in-path 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 User 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

Mobile Controller

Related Commands

“show policy id”

policy id in-path rule edit rulenum enable

Enables a single in-path rule on the specified policy.

Syntax

policy id <id> in-path rule edit rulenum <rule-number> enable

Parameters

<id>	Policy ID number.
rulenum <rule-number>	Specifies 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 User Guide*.

Example

```
amnesiac (config) # policy id 1 in-path rule edit rulenum 3 enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id in-path rule edit rulenum fixed-target

Edits a fixed-target in-path rule on the specified policy.

Syntax

Syntax

policy id <id> in-path rule edit rulenum <rule-number> fixed-target [target-addr <address>] [target-port <port>] [dstaddr <subnet>] [dstport <port>] [dst-host <host-label>] [srcaddr <subnet>] [backup-addr <address>] [backup-port <port>] [optimization <policy>] [preoptimization <policy>] | [latency-opt {<policy>] [neural-mode <mode>] [description <description>] rule-enable [true | false]

Parameters

<id>	Existing policy number on the local Mobile Controller.
rulenum <rule-number>	Specifies the rule number to edit: 1-N or start or end.
target-addr <address> **target-port <port>**	Specifies 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.
dstaddr <subnet> **dstport <port>**	Specifies 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.
dst-host <host-label>	Specifies a destination host label for this rule. You configure the host label settings using the **host-label** command. A destination IP address and host label cannot be specified in the same rule. A host label can be used instead of a destination IP address. Enter an empty string, represented by two quotation marks (""), to remove a host label.
srcaddr <subnet>	Specifies the source subnet,: for example, 1.2.3.4/32
backup-addr <address>	Specifies a backup appliance for this rule (if any).
optimization <policy>	Specifies an optimization policy: ▪ **normal** - The **normal** optimization policy is the default. The normal process performs LZ compression and SDR. ▪ **sdr-only -** Turns off LZ compression. ▪ **sdr-m -** Performs data reduction entirely in memory, which prevents the SteelHead Mobile 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** - Turns off SDR but perform LZ compression. ▪ **none -** Turns off LZ compression and SDR.
preoptimization <policy>	Specifies a preoptimization policy: ▪ **ssl** - Enables SSL preoptimization processing for traffic via SSL secure ports. ▪ **oracle-forms** - Enables preoptimization processing for the Oracle Forms browser plug-in. ▪ **oracle-forms+ssl** - Enables preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side SteelHead Mobile. ▪ **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 <policy>	Specifies 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** - Performs HTTP optimization on connections matching this rule. ▪ **normal** - Performs 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** - Performs latency optimization on connections matching this rule.
neural-mode <mode>	Enables neural framing in the SteelHead Mobile. 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 SteelHead Mobile 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>	Specifies a description of the rule.
rule-enable [true | false]	Enables (**true**) or disables (**false**) 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).

For detailed information about in-path rules, see the *SteelHead User 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

Mobile Controller

Related Commands

“show policy id”

---

policy id in-path rule edit pass-through

Edits a pass-through in-path rule on the specified policy.

Syntax

[no] policy id <id> in-path rule edit rulenum <rule-number> pass-through [srcaddr <subnet>] [dstaddr <subnet>] [dstport <port>] [dst-host <host-label>] [cloud-accel <mode>] [description <description>]

Parameters

<id>	Policy ID number.
rulenum <rule-number>	Specifies the rule number to edit: 1-N or start or end.
srcaddr <subnet>	Specifies the source subnet, for this rule, for example, 1.2.3.4/32.
dstaddr <subnet> dstport <port>	Specifies 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.
dst-host <host-label>	Specifies a destination host label for this rule. You configure the host label settings using the **host-label** command. A destination IP address and host label cannot be specified in the same rule. A host label can be used instead of a destination IP address. Enter an empty string, represented by two quotation marks (""), to remove a host label.
cloud-accel <mode>	Applies only if you have subscribed to a Software as a Service (SaaS) platform. Specifies a cloud-acceleration 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 SteelHead SaaS. You do not need to add an in-path rule unless you want to optimize specific users and not others. Specify one of these modes: ▪ **auto** - If the in-path rule matches, the connection is optimized by the Riverbed SteelHead Cloud Accelerator (SCA) connection. ▪ **passthru** - If the in-path rule matches, the connection is not optimized by the SteelHead SaaS, but it follows the rule's other parameters so that the connection might be optimized by this SteelHead with other SteelHeads in the network, or it might be passed through. Domain labels and cloud acceleration are mutually exclusive except when the **_cloud-accel-saas** host label is used. To use cloud acceleration with domain labels, we recommend placing the domain label rules lower than cloud acceleration rules in your rule list so the cloud rules match before the domain label rules.
description <description>	Specifies 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 User Guide*.

Example

```
amnesiac (config) # policy id 1 in-path rule edit rulenum 25 pass-through srcaddr 10.10.10.1/24
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id in-path rule fixed-target

Adds a fixed-target in-path rule on the specified policy.

Syntax

Syntax

[no] policy id <id> in-path rule fixed-target [target-addr <address>] [target-port <port>] [dstaddr <subnet>] [dstport <port>] [srcaddr <subnet>] [dst-host <host-label>] [backup-addr <address>] [backup-port <port>] [optimization <policy>] [preoptimization <policy>] [latency-opt <mode>] [neural-mode <mode>] [description <description>] rule-enable [true | false] [rulenum <rule-number>]

Parameters

<id>	Policy ID number.
target-addr <address> target-port <port>	Specifies 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.
dstaddr <subnet> dstport <port>	Specifies 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>	Specifies the source subnet, for example, 1.2.3.4/32.
dst-host <host-label>	Specifies a destination host label for this rule. You configure the host label settings using the **host-label** command. A destination IP address and host label cannot be specified in the same rule. A host label can be used instead of a destination IP address. Enter an empty string, represented by two quotation marks (""), to remove a host label.
backup-addr <address> backup-port <port>	Specifies 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.
optimization <policy>	Specifies an optimization policy: ▪ **normal** - The **normal** optimization policy is the default. The normal process performs LZ compression and SDR. ▪ **sdr-only –** Turns off LZ compression. ▪ **sdr-m –** Performs data reduction entirely in memory, which prevents the SteelHead Mobile 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** - Turns off SDR but performs LZ compression. ▪ **none –** Turns off LZ compression and SDR.
preoptimization <policy>	Specifies a preoptimization policy: ▪ **ssl** - Enables SSL preoptimization processing for traffic via SSL secure ports. ▪ **oracle-forms** - Enables preoptimization processing for the Oracle Forms browser plug-in. ▪ **oracle-forms+ssl** - Enables preoptimization processing for both the Oracle Forms browser plug-in and SSL encrypted traffic through SSL secure ports on the client-side SteelHead Mobile. ▪ **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 <mode>	Specifies 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** - Performs HTTP optimization on connections matching this rule. ▪ **normal** - Performs 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** - Does not perform latency optimization on connections matching this rule.
neural-mode <modes>	Enables neural framing in the SteelHead Mobile. 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 adjusts the Nagle parameters. The SteelHead Mobile picks the best algorithm to use by learning, which algorithm is best and adapting if the traffic characteristic changes. ▪ **never -** Never uses 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 -** Bases 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>	Specifies a description of the rule.
rule-enable	Enables (**true**) or disables (**false**) an in-path rule.
rulenum <rule-number>	Specifies 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 as an optimization peer.

You must specify at least one remote target SteelHead to optimize (and, optionally, which ports and backup SteelHeads), and add rules to specify the network of servers, ports, port labels, and out-of-path SteelHeads to use.

The SteelHead Mobile 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 Mobiles near the target server that you want to optimize.

For detailed information about in-path rules, see the *SteelHead User 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

Mobile Controller

Related Commands

“show policy id”

policy id in-path rule move

Moves an in-path rule in the rule list on the specified policy.

Syntax

policy id <id> in-path rule move rulenum <rule-number> to <rule-number>

Parameters

<id>	Policy ID number.
<rule-number>	Rule number or **start** or **end**.

Usage

For detailed information about in-path rules, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 in-path rule move rulenum 2 to 1
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id in-path rule pass-through

Adds a pass-through in-path rule on the specified policy. Allows the SYN packet to pass through the SteelHead Mobile unoptimized.

Syntax

[no] policy id <id> in-path rule pass-through [srcaddr <subnet>] [dstaddr <subnet> dstport <port>] [dst-host <host-label>] [cloud-accel <mode>] [rulenum <rule-number>] [description <description>]

Parameters

<id>	Policy ID number.
srcaddr <subnet>	Specifies the source subnet for this rule: for example, **1.2.3.4/32**
dstaddr <subnet> dstport <port>	Specifies 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.
dst-host <host-label>	Specifies a destination host label for this rule. You configure the host label settings using the **host-label** command. A destination IP address and host label cannot be specified in the same rule. A host label can be used instead of a destination IP address. Enter an empty string, represented by two quotation marks (""), to remove a host label.
cloud-accel <mode>	Applies only if you have subscribed to a Software as a Service (SaaS) platform. Specifies a cloud-acceleration 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 SteelHead SaaS. You do not need to add an in-path rule unless you want to optimize specific users and not others. Specify one of these modes: ▪ **auto** - If the in-path rule matches, the connection is optimized by the Riverbed SteelHead Cloud Accelerator (SCA) connection. ▪ **passthru** - If the in-path rule matches, the connection is not optimized by the SteelHead SaaS, but it follows the rule's other parameters so that the connection might be optimized by this SteelHead with other SteelHeads in the network, or it might be passed through. Domain labels and cloud acceleration are mutually exclusive except when the **_cloud-accel-saas** host label is used. To use cloud acceleration with domain labels, we recommend placing the domain label rules lower than cloud acceleration rules in your rule list so the cloud rules match before the domain label rules.
rulenum <rule-number>	Specifies 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>	Specifies a description of the rule.

Usage

The SteelHead Mobile 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.

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 Mobile is in bypass mode. (Pass through of traffic might occur because of in-path rules or because the connection was established before the SteelHead Mobile was put in place or before the SteelHead Mobile service was enabled.)

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 User Guide*.

Example

```
amnesiac (config) # in-path rule pass-through srcaddr 10.10.10.1 rulenum 25
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id mapi enable

Enables MAPI optimization and features on the specified policy.

Syntax

[no] policy id <id> mapi enable

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables MAPI optimization settings.

For detailed information about MAPI optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 mapi enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id mapi encrypted enable

Enables MAPI Exchange encrypted optimization settings on the specified policy.

Syntax

[no] policy id <id> mapi encrypted enable

Parameters

<id>	ID number.

Usage

The **no** command option disables MAPI optimization settings.

For detailed information about MAPI optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # no policy id 1 mapi encrypted enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id mapi encrypted only

Enables only MAPI-encrypted optimization settings on the specified policy.

Syntax

[no] policy id <id> mapi encrypted only

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables MAPI-encrypted optimization settings.

For detailed information about MAPI-encrypted optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # no policy id 1 mapi encrypted only
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id mapi encrypted multi-auth enable

Enables multiple authentication MAPI Exchange encrypted optimization for the specified policy.

Syntax

[no] policy id <id> mapi encrypted multi-auth enable

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables the multiple authentication MAPI optimization.

For more information about MAPI optimization, see the *SteelHead Management Console User’s Guide*.

Example

```
amnesiac (config) # policy id 1 mapi encrypted multi-auth enable
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id mapi multi-context enable

Enables multiple context MAPI Exchange encrypted optimization for the specified policy.

Syntax

[no] policy id <id> mapi multi-context enable

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables the multiple context MAPI optimization.

For more information about MAPI optimization, see the *SteelHead Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 mapi multi-context enable
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id mapi outlook-anywhr multi-context enable

Enables multiple context Outlook Anywhere optimization for the specified policy.

Syntax

[no] policy id <id> mapi outlook-anywhr multi-context enable

Parameters

<id>	Policy ID number.

Usage

Enables multiple context Outlook Anywhere 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.

The **no** command option disables the multiple context Outlook Anywhere optimization.

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 SteelHead Mobile product family.

For more information about Outlook Anywhere optimization, see the *SteelHead Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 mapi outlook-anywhr multi-context enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id mapi mac enable

Enables MAPI Exchange MAC settings on the specified policy.

Syntax

[no] policy id <id> mapi mac enable

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables MAPI optimization settings.

For detailed information about MAPI optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # no policy id 1 mapi mac enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id mapi outlook-anywhr auto-detect

Enables Outlook Anywhere auto-detection on the specified policy.

Syntax

[no] policy id <id> mapi outlook-anywhr auto-detect

Parameters

<id>	Policy ID number.

Usage

For detailed information about the Outlook Anywhere auto-detection, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 mapi outlook-anywhr auto-detect
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id mapi outlook-anywhr enable

Enables Outlook Anywhere optimization on the specified policy.

Syntax

[no] policy id <id> mapi outlook-anywhr enable

Parameters

<id>	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 SteelHead Mobile.

For detailed information about Outlook Anywhere, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 mapi outlook-anywhr enable
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id mapi prepop enable

Enables MAPI Exchange prepopulation on the SteelHead Mobile.

Syntax

[no] policy id <id> mapi prepop enable

Parameters

<id>	Policy ID number.

Usage

MAPI Exchange prepopulation is disabled by default.

The **no** command option disables MAPI Exchange prepopulation.

For more information about MAPI optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 mapi prepop enable
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id mapi prepop max-connections

Sets the maximum number of connections used for MAPI Exchange prepopulation.

Syntax

[no] policy id <id> mapi prepop max-connections <connections>

Parameters

<id>	Policy ID number.
<connections>	Maximum number of connections. The default is 10. **Note:** For the **no** command option, this variable is not applicable and is not included in the command syntax.

Usage

This command does not limit the number of connections to a specific range.

The **no** command option resets the maximum number of connections to 10 (the default).

For more information about MAPI optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 mapi prepop max-connections 5
```

The following is an example of the **no** command option. Notice that the **<connections>** variable is not used in the command syntax.

```
amnesiac (config) # no policy id 1 mapi prepop max-connections
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id mapi prepop poll-interval

Sets the polling interval used for MAPI Exchange prepopulation.

Syntax

[no] policy id <id> mapi prepop poll-interval <minutes>

Parameters

<id>	Policy ID number.
<minutes>	Polling interval in minutes. The default is 20. For the **no** command option, this variable is not applicable and is not included in the command syntax.

Usage

This command does not limit the polling interval to a specific time period.

The **no** command option resets the polling interval to 20 minutes (the default).

For more information about MAPI optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 mapi prepop poll-interval 5
```

The following is an example of the **no** command option. Notice that the **<minutes>** variable is not used in the command syntax.

```
amnesiac (config) # no policy id 1 mapi prepop poll-interval
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id mapi prepop timeout

Sets the timeout value used for MAPI Exchange prepopulation.

Syntax

[no] policy id <id> mapi prepop timeout <hours>

Parameters

<id>	Policy ID number.
<hours>	Timeout value in hours. The default is 96. **Note:** For the **no** command option, this variable is not applicable and is not included in the command syntax.

Usage

This command does not limit the timeout value to a specific time period.

The **no** command option resets the timeout value to 96 hours (the default).

For more information about MAPI optimization, see the *SteelHead Management Console User’s Guide*.

Example

```
amnesiac (config) # policy id 1 mapi prepop timeout 24
```

The following is an example of the **no** command option. Notice that the **<hours>** variable is not used in the command syntax.

```
amnesiac (config) # no policy id 1 mapi prepop timeout
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id mapi port-remap enable

Enables MAPI port remapping.

Syntax

[no] policy id <id> mapi port-remap enable

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables the port remapping feature.

For detailed information about the MAPI optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 mapi port-remap enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id mapi strip level2

Removes the MAPI Exchange DCE/RPC Level 2 (Connect) authentication verifiers for the specified policy.

Syntax

[no] policy id <id> mapi strip level2

Parameters

<id>	Policy ID number.

Usage

The **no** command option does not remove the DCE/RPC Level 2 authentication verifiers.

For more information about MAPI optimization, see the *SteelHead Management Console User’s Guide*.

Example

```
amnesiac (config) # policy id 1 mapi strip level2
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id nfs enable

Enables the NFS protocol settings on the specified policy.

Syntax

[no] policy id <id> nfs enable

Parameters

<id>	Policy ID number.

Usage

The NFS optimizer provides latency optimization improvements for NFS operations primarily by prefetching data, storing it on the client SteelHead Mobile 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 User Guide*.

Example

```
amnesiac (config) # policy id 1 nfs enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id notes enable

Enables Lotus Notes optimization.

Syntax

[no] policy id <id> notes enable

Parameters

<id>	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 User Guide*.

Example

```
amnesiac (config) # policy id 1 notes enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id notes port

Configures a port for Lotus Notes optimization.

Syntax

[no] policy id <id> notes port

Parameters

<id>	Policy on the Mobile Controller.
<port>	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 User Guide*.

Example

```
amnesiac (config) # policy id 1 notes port 1234
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id oracle-forms enable

Configures preoptimization processing for the Oracle Forms browser plug-in.

Syntax

[no] policy id <id> oracle-forms enable

Parameters

<id>	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 User Guide*.

Example

```
amnesiac (config) # policy id 1 oracle-forms enable
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id probe-tcp-opt

Configures the TCP probing option for optimization.

Syntax

[no] policy id <id> probe-tcp-opt <probe-tcp-option-value>

Parameters

<id>	Policy on the Mobile Controller.
<probe-tcp-option-value>	TCP probe value.

Usage

The **no** command option disables TCP optimization.

For detailed information about TCP probing, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 probe-tcp-opt 2
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id smb2 enable

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>	Policy on the Mobile Controller.

Usage

For detailed information about SMB2 optimization, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 smb2 enable
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id smb2 smb3-support enable

Enables SMB3 optimization for the specified policy.

Syntax

[no] policy id <id> smb2 smb3-support enable

Parameters

<id>	Policy ID number.

Usage

Before using this command, you must first enable SMB2. For more information about SMB2, see the *SteelHead Management Console User's Guide*.

The **no** command option disables SMB3 optimization.

Example

```
amnesiac (config) # policy id 1 smb2 smb3-support enable
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id ssl backend client-tls-1.2

Enables support for TLS version 1.1 and 1.2 encryption between the SSL server and the client-side SteelHead Mobile.

Syntax

[no] policy id <id> ssl backend client-tls-1.2

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables support for TLS version 1.1 and 1.2 encryption between the SSL server and the client-side SteelHead Mobile.

Use this command in traditional SSL mode to control how the client-side SteelHead Mobile negotiates its SSL connections to the server.

TLS versions 1.1 and 1.2 support is disabled by default. Use the **show running-config** command to determine if this command is enabled.

For detailed information about SSL, see the *SteelHead Management Console User's Guide*.

Example

```
amnesiac (config) # policy id 1 ssl backend client-tls-1.2
```

Product

Mobile Controller

Related Commands

"show policy id" "show running-config"

policy id ssl backend no-byp-hs-fail

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>	Policy ID number.

Usage

The **no** command option disables the SSL bypass feature.

For detailed information about SSL, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 ssl backend no-byp-hs-fail
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id ssl enable

Configures SSL for the policy.

Syntax

[no] policy id <id> ssl enable

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables SSL support.

For detailed information about SSL, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 ssl enable
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id ssl fallback-no-enc

Configures fallback to no encryption on the inner channel.

Syntax

[no] policy id <id> ssl fallback-no-enc

Parameters

<id>	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 SteelHead Mobile and the server-side SteelHeads.

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 User Guide*.

Example

```
amnesiac (config) # policy id 1 ssl fallback-no-enc
amnesiac (config) # service restart
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id ssl proxy-support enable

Enables SSL proxy support for the specified policy.

Syntax

[no] policy id <id> ssl proxy-support enable

Parameters

<id>	Policy ID number.

Usage

The **no** command option disables SSL proxy support.

Example

```
amnesiac (config) # policy id 1 ssl proxy-support enable
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id ssl sfe-mode

Configures SSL safe mode.

Syntax

[no] policy id <id> ssl sfe-mode

Parameters

<id>	Policy ID number.

Usage

The **no** command option resets SSL safe mode.

For detailed information about SSL, see the *SteelHead User Guide*.

Example

```
amnesiac (config) # policy id 1 ssl sfe-mode
```

Product

Mobile Controller

Related Commands

"show policy id"

policy id ssl traffic-type

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>	Policy ID number.
<type>	Specifies one of the following traffic types: ▪ **ssl-only** - The SteelHead Mobile and the server-side SteelHead 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 SteelHead Mobile and the server-side SteelHead 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 SteelHead Mobile and server-side SteelHead appliances when securing SMB-signed traffic, encrypted MAPI traffic, or encrypted Citrix ICA traffic (RiOS 7.0). Enabling this option requires an optimization service restart. ▪ **all** - The SteelHead Mobile and the server-side SteelHead 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 User Guide*.

Example

```
amnesiac (config) # policy id 1 ssl traffic-type all
```

Product

Mobile Controller

Related Commands

“show policy id”

policy id ssl trust-all

Configures a trust relationship with all preconfigured peering certificates.

Syntax

[no] policy id <id> ssl trust-all

Parameters

<id>	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 User Guide*.

Example

```
amnesiac (config) # policy id 1 ssl trust-all
```

Product

Mobile Controller

Related Commands

"show policy id"

Endpoint commands

This section describes the Mobile Controller commands for endpoint clients.

---

endpoint info clearall

Clears all endpoint statistics.

Syntax

endpoint info clearall

Parameters

None

Example

```
amnesiac (config) # endpoint info clearall
```

Product

Mobile Controller

Related Commands

"endpoint info showall," "endpoint info threshold"

---

endpoint info showall

Shows all endpoint information.

Syntax

endpoint info showall

Parameters

None

Example

```
amnesiac (config) # endpoint info showall
```

Product

Mobile Controller

Related Commands

"endpoint info threshold," "endpoint info threshold"

---

endpoint info threshold

Configures the duration, in seconds, to keep unused endpoint data.

Syntax

endpoint info threshold <seconds>

Parameters

<seconds>	Number of seconds.

Example

```
amnesiac (config) # endpoint info threshold 10
```

Product

Mobile Controller

Related Commands

"endpoint info showall," "endpoint info showall"

stats export endpoint-report email

Generates an endpoint report and exports the report to the specified destination email address.

Syntax

stats export endpoint-report email <email-address>

Parameters

<email-address>	Destination e-mail address.

Usage

The endpoint report is generated and sent to the designated email address. The report includes the following information:

- Client ID
- User ID
- Controller ID
- Connected
- Health
- Health Level
- Health Descriptions
- Version
- Computer
- Datastore Size
- Used Datastore
- OS
- IP Address

Example

```
amnesiac # stats export endpoint-report email jx!smith2@riverbed.com
```

Product

Mobile Controller

Related Commands

"endpoint info showall"

Package commands

package assignment adpath

Configures package assignment by Active Directory path.

Syntax

[no] package assignment adpath <ad-path> package_id <package-id>

Parameters

<ad-path>	Active Directory path.
package_id <package-id>	Specifies 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

Mobile Controller

Related Commands

“show package assignments adpath”

package assignment depid

Configures package assignment by deployment ID.

Syntax

[no] package assignment depid <deploy-id> package_id <package-id>

Parameters

depid <depid>	Specifies the deployment ID.
package_id <package-id>	Specifies 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

Mobile Controller

Related Commands

“show package assignments depid”

package assignment removeall-adpath

Removes all Active Directory path assignments.

Syntax

package assignment removeall-adpath

Parameters

None

Example

```
amnesiac (config) # package assignment removeall-adpath
```

Product

Mobile Controller

Related Commands

“show package assignments adpath”

package assignment removeall-depid

Removes all package deployment ID assignments.

Syntax

package assignment remove-all-depid

Parameters

None

Example

```
amnesiac (config) # package assignment removeall-depid
```

Product

Mobile Controller

Related Commands

“show package assignments depid”

Domain command

This section describes Mobile Controller **domain** command.

ip fqdn override (Mobile Controller)

Enables the SteelHead Mobile Client to override the fully qualified domain name.

Syntax

[no] ip fqdn override <domain-name>

Parameters

<domain-name>	Overrides 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 SteelCentral Controller for SteelHead Mobiles, click **Configure** to open the Configure SteelCentral Controller for SteelHead Mobile 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

Mobile Controller

Related Commands

“show hosts”

Displaying Mobile Controller information

This section describes the Mobile Controller **show** commands.

show cluster licenses

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

Mobile Controller

Related Commands

"cluster license checkout-count"

---

show cluster license settings

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

Mobile Controller

Related Commands

"cluster detach," "**cluster join,**" "cluster remove,"

---

show cluster members

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

Mobile Controller

Related Commands

"cluster detach," "**cluster join,**" "cluster remove"

show package assignments adpath

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

Mobile Controller

Related Commands

“package assignment adpath”

show package assignments depid

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

Mobile Controller

Related Commands

“package assignment depid”

show package list

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

Mobile Controller

Related Commands

“package assignment adpath,” “package assignment removeall-adpath,” “package assignment removeall-depid”

---

show policy assignments adpath

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

Mobile Controller

Related Commands

“policy assignment adpath”

---

show policy assignments depid

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

Mobile Controller

Related Commands

“package assignment depid”

show policy default

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

Mobile Controller

show policy id

Displays policy settings.

Syntax

show policy id <id> {branch-warming | cifs [big-read-blklst] | citrix | connection | endpoint | eos | ftp | http | in-path | mapi |nfs | notes | oracle-forms | probe-tcp-opt | service <connection> | sharepoint internal | smb2 | ssl}

Parameters

<id>	Policy ID number.
branch-warming	Displays branch-warming settings for the specified policy.
cifs	Displays CIFs protocol settings for the specified policy.
big-read-blklst	Displays the CIFS big-cfe-read-black-list settings.
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.
eos	Displays Exchange Optimization Service (EOS) settings.
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.
oracle forms	Displays Oracle forms settings for the specified policy.
probe-tcp-opt	Displays probe TCP settings for the specified policy.
service <connection>	Displays the maximum service connection pooling size for the specified policy.
sharepoint internal	Displays the Web-based Distributed Authoring (WebDAV) and FrontPage Server Extensions (FPSE) statistics 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

Mobile Controller

Related Commands

“Policy commands”

show policy id http server-table

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

Syntax

show policy id <id> http server-table [default]

Parameters

<id>	Policy ID number.
default	Displays the default HTTP server table.

Example

```
amnesiac (config) # show policy id 1 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
FP: FPSE               WD: WebDAV
FS: FSSHTTP

  Hostname/Subnet                     UL  PP   OP   RA   SA   GR   FN   SC   IC   IK   FP   WD   FS
--------------------------------------- --- ----  ---  ---  --- ---  ---  --- ---  --- --- --   --
  all                                  no   no   no   no   no   no   no   no   no   no   no   no   no
  force-nego-ntlm                      no   no   no   no   no   no   no   no   no   no   no   no   no
  gratuitous-401                       no   no   no   no   no   no   no   no   no   no   no   no   no
  insert-cookie                        no   no   no   no   no   no   no   no   no   no   no   no   no
  test                                 yes  no   no   no   no   no   no   no   no   no   no   no   no
  0.0.0.0/0                            yes  yes  no   no   no   no   no   yes  no   no   no   no   no
```

Product

SteelHead CX, SteelHead EX, Mobile Controller

Related Commands

“policy id in-path rule auto-discover”

show policy list

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

Mobile Controller

Related Commands

“policy id ssl enable”

show protocol ssl ca

Displays settings for the signing certificate authority (CA).

Syntax

show policy ssl ca <certificate-name> certificate [raw | text]

Parameters

<certificate-name>	CA certificate name.
raw	Specifies raw PEM format.
text	Specifies 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:
.
.
.
```

Product

Mobile Controller

Related Commands

“policy id ssl enable”

Product

Mobile Controller

Related Commands

“policy id ssl enable”

show protocol ssl chain-cert

Displays the CA certificates.

Syntax

show protocol ssl chain-cert {ca | cert <cert-data>}

Parameters

ca	Specifies the certificate name
cert <cert-data>	Specifies the certificate in PEM format.

Example

```
amnesiac # show protocol ssl chain-cert ca Coast_Bank
CA "Coast_Bank" added to chain.
```

Product

Mobile Controller

Related Commands

"policy id ssl enable"

show protocol ssl signing certificate

Displays SSL signing status.

Syntax

show protocol SSL signing certificate [raw | text]

Parameters

raw	Specifies raw PEM format.
text	Specifies 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

Mobile Controller

Related Commands

"policy id ssl enable"

SteelHead (in the cloud) feature commands

This section describes feature commands used by the SteelHead (in the cloud). 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 SteelHead (in the cloud) GUI to configure the SteelHead (in the cloud) appliance. This section also contains:

For detailed information about the SteelHead (in the cloud), see the *SteelHead Cloud Services User Guide*.

discovery enable

Enables the Discovery Agent on the appliance.

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 SteelHead-c in its optimization group. Then, the client SteelHead discovers and starts peering and optimizing with the SteelHead-c. 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 SteelHead-c in its optimization group. The SteelHead-c 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 *SteelHead Cloud Services User Guide*.

The **no** command option disables the Discovery Agent on the SteelHead-c.

Example

```
amnesiac (config) # discovery enable
```

Product

SteelHead-c, SteelHead-v

Related Commands

"show discovery"

discovery local

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>	Specifies the local client ID.
node-key <key>	Specifies the local client key.
discovery-type {riverbed-portal| local-portal url <portal-url>}	Specifies the portal with which the Discovery Agent should communicate: ▪ **riverbed-portal** - This is the default value. ▪ **local-portal url** - You can use your own local portal by specifying this option and typing the URL of the local portal.
refresh-time <time>	Specifies the refresh time in seconds for the Discovery Agent. The time must be between 300 and 3600 seconds. The default value is 300.

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

SteelHead-c, SteelHead-v

Related Commands

“show discovery”

in-path agent-intercept

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>	Specifies the IP port that transmits a regular heartbeat.
keepalive count <int>	Specifies a value for the keepalive count. This is the total number of acknowledgments (ACKs) for which the SteelHead-c waits before it reports that the Discovery Agent is down.
keepalive interval <int>	Specifies the time interval in seconds between keep-alive messages of the SteelHead-c for a heartbeat connection with the Discovery Agent.
server-nat-mode <mode>	Specifies the transparency mode for client connections. You configure the transparency mode in the SteelHead-c 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 SteelHead-c 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 SteelHead-c IP address. ▪ **restricted-transparent** - This is the default mode. 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. ▪ **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 SteelHead-c and the Discovery Agent.

Example

```
amnesiac (config) # in-path agent-intercept heartbeat port 8081
```

Product

SteelHead-c, SteelHead-v

Related Commands

“show in-path agent-intercept”

in-path agent-intercept enable

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 SteelHead-c for this command to take effect.

The **no** command option disables the in-path intercept mode on the SteelHead-c.

Example

```
amnesiac (config) # in-path agent-intercept enable
```

Product

SteelHead-c, SteelHead-v

Related Commands

"show in-path agent-intercept"

in-path agent-intercept keepalive non-zero

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 SteelHead-c 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

SteelHead-c, SteelHead-v

Related Commands

"show in-path agent-intercept"

ip addrmap

Creates a new IP address map between the public IP address of the server to its private IP address in Amazon Web Services (AWS).

Syntax

[no] ip addrmap public-addr <public-ip-address> private-addr <private-ip-address>

Parameters

public-addr <public-ip- address>	Specifies the public IP address of the server.
private-addr <private-ip-address>	Specifies 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

SteelHead-c

Related Commands

“show ip addrmap”

ip addrmap enable

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 SteelHead-c 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 SteelHead-c 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

SteelHead-c

Related Commands

“show ip addrmap”

license client fetch

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. This command is only relevant for SteelHead-c licensing using the Riverbed Cloud Portal.

Example

```
amnesiac # license client fetch
```

Product

SteelHead-c, SteelHead-v

Related Commands

"show license-client"

license client init

Uses the one-time token you provide to retrieve a license for the SteelHead-c.

Syntax

[no] license client init <one-time-token>

Parameters

<one-time-token>	One-time token that the SteelHead-c uses to retrieve the license.

Usage

The license client is part of the SteelHead-c 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

SteelHead-c, SteelHead-v

Related Commands

"show in-path agent-intercept"

license server

Syntax

[no} license server <hostname> [priority <number>] [port <number>]

Parameters

<hostname>	Hostname of the computer that contains the license server.
priority <number>	Specifies 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>	Specifies the port number on which the license server is listening. The default is port 80.

Usage

The license server provides licenses to the appliance. This command is only relevant for SteelHead-c licensing using the Riverbed Cloud Portal.

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

SteelHead-c

Related Commands

“show license-servers”

Displaying SteelHead (in the cloud) information

This section describes the **show** commands for displaying SteelHead (in the cloud) information.

---

show discovery

Displays whether the Discovery Agent is enabled or disabled on the SteelHead-c.

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

SteelHead-c, SteelHead-v

Related Commands

“discovery enable”

---

show in-path agent-intercept

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

SteelHead-c

Related Commands

"in-path agent-intercept"

show in-path agent intercept server-nat mode

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

SteelHead-c

Related Commands

"in-path agent-intercept"

show ip addrmap

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 SteelHead-c.

Example

```
amnesiac (config) # show ip addrmap
IP address mapping: enabled
Public addr     Private addr
-----------     ------------
    10.0.62.164 10.0.62.165
```

Product

SteelHead-c

Related Commands

"ip addrmap enable", "ip addrmap"

show licenses

Displays all of the SteelHead-c 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

SteelHead-c

Related Commands

“license client fetch,” “license client init,” “license server”

show license-client

Displays details of the licenses retrieved by the SteelHead-c.

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

SteelHead-c

Related Commands

“license client fetch”, “license client init”

show license-servers

Displays the name, port number, and priority of the server that the SteelHead-c 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

SteelHead-c

Related Commands

“license server”

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 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”
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”

Problem	Commands
Hardware	"show stats cpu"
	"show stats memory"
	"show stats ecc-ram"
	"show stats fan"
	"show hardware error-log"
	"show hardware spec"
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"
Prepopulation	"show prepop"
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	"image boot"
	"image check upgrades"
	"show images"
	"show bootvar"

Problem	Commands
Collecting System Data for Riverbed Technical Support	"RiOS TCP dump commands"
	"debug health-report enable"
	"debug uptime-report enable"
	"debug generate dump"
	"file debug-dump delete"

A

SteelHead Ports

This appendix provides a reference to ports used by the system. It includes the following sections:

SteelFusion Ports

The following table summarizes SteelFusion default ports with the port label SteelFusion.

Default Ports	Description
7950	Data requests for data blocks absent in Edge appliance from the data center
7951	New data created at the Edge to the data center
7952	Prefetch data for which SteelFusion has highest confidence (for example, file read ahead)
7953	Prefetch data for which SteelFusion has medium confidence (for example, boot)
7954	Prefetch data for which SteelFusion has lowest confidence (for example, prepopulation)
7970	Management information exchange between Edge and Core appliances

Default Ports

The following table summarizes SteelHead default ports with the port label RBT-Proto.

Default Ports	Description
7744	RiOS 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	SteelHead Interceptor
7870	SteelCentral Controller for SteelHead Mobile

Note: Because optimization between SteelHeads 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 SteelHeads, ports 7800 and 7810, must be passed through firewall devices located between the pair of SteelHeads. Also, SYN and SYN/ACK packets with the TCP option 76 must be passed through firewalls for automatic discovery to function properly. For the SCC, 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.

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

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).

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.

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

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).

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.

Type	Port	Description
ssh	22/tcp	SSH Remote Login Protocol
tacacs	49/tcp	TACACS+
kerberos	88	Kerberos
rtsps	322	rtsp over TLS/SSL
https	443/tcp	http protocol over TLS/SSL
smtps	465/tcp	# SMTP over SSL (TLS)

Type	Port	Description
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)
tcp/udp	902/tcp	VMware Server Console
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.

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
csvr-sslproxy	3191/tcp	ConServR SSL Proxy

Type	Port	Description
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

Q

R

S

T

X