Hillstone Networks Inc.

StoneOS CLI User Guide

System Management

Version 5.5R5

Hillstone Networks Inc

Contact Information:

US Headquarters:

Hillstone Networks

292 Gibraltar Drive, Suite 105

Sunnyvale, CA 94089

Phone: 1-408-508-6750

http://www.hillstonenet.com/about-us/contact/

About this Guide:

This guide gives you comprehensive configuration instructions of Hillstone Networks StoneOS.

For more information, refer to the documentation site: http://docs.hillstonenet.com.

To provide feedback on the documentation, please write to us at:

hs-doc@hillstonenet.com

TWNO: TW-CUG-UNI-SYS-5.5R5-EN-V1.0-Y17M10

Table of Contents

About This Guide

This document follows the conventions below:

Content

- **Tip**: provides reference.
- **Note**: indicates important instructions for you better understanding, or cautions for possible system failure.
- Bold font: indicates links, tags, buttons, checkboxes, text boxes, or options. For example, "Click **Login** to log into the homepage of the Hillstone device", or "Select **Objects** > **Address Book** from the menu bar".

CLI

- Braces ({ }): indicate a required element.
- Square brackets ([ ]): indicate an optional element.
- Vertical bar (|): separates multiple mutually exclusive options.
- **`Bold`**: indicates an essential keyword in the command. You must enter this part correctly.
- *`Italic`*: indicates a user-specified parameter.
- The command examples may vary from different platforms.
- In the command examples, the hostname in the prompt is referred to as host-name.

WebUI

When clicking objects (menu, sub-menu, button, link, etc.) on WebUI, the objects are separated by an angled bracket (>).

Command Line Interface

Overview

A command line interface (CLI) is a mechanism for you to interact with the operating system by typing commands which instruct the device to perform specific tasks. This chapter describes how to use StoneOS command line interface.

Note: All command keywords are not case sensitive, but user input is case sensitive.

CLI Modes and Prompts

StoneOS CLI commands and statements are organized under various hierarchical modes. Some of the CLI commands can work only under a particular mode, which can prevent accidental misoperations. For example, configuration commands can only be used in configuration modes. StoneOS uses different prompts to indicate modes.

Execution Mode

When you log in StoneOS CLI, you are in the execution mode. Execution mode prompt is a pound sign (#):

```
hostname#
```

Global Configuration Mode

Commands in the global configuration mode are used to change device settings. To enter the global configuration mode, in the execution mode, use the command configuration. The global configuration mode prompt is shown as follows:

```
hostname(config)#
```

Sub-module Configuration Mode

StoneOS has various functional modules. Some CLI commands only work in their corresponding sub-module configuration modes. To enter a sub-module configuration mode, in the global configuration mode, type a certain command. For example, to enter interface ethernet0/0 configuration mode, type `interface ethernet0/0`, and its command prompt is shown as follows:

```
hostname(config-if-eth0/0)#
```

Switching between CLI Modes

When you log into StoneOS CLI, you are in the execution mode. To switch to other CLI mode, type the commands in the table below.

Table 1: CLI Mode Switching Commands

Mode	Command

From execution mode to global configuration mode	`configure`
From global configuration mode to sub-module configuration mode	The command may vary, specifically depending on the sub-module configuration mode you want to enter
Return to a higher hierarchy	`exit`
From any mode to execution mode	`end`

CLI Error Message

StoneOS CLI checks the command syntax. Only correct command can be executed. StoneOS shows error message for incorrect syntax. The following table provides messages of common command errors:

Table 2: Error Messages and Description

Message	Description
Unrecognized command	StoneOS is unable to find the command or keyword
	Incorrect parameter type
	Input value excesses its defined value range
Incomplete command	User input is incomplete
Ambiguous command	User input is not clear

Command Input

To simplify input operation, you can use the short form of CLI commands. In addition, StoneOS CLI can automatically list available command keywords and fill incomplete commands.

Command Short Form

You can use only some special characters in a command to shorten your typing. Most of the commands have short form. For example, you can use `sho int` to check the interface information instead of typing `show interface`, and use `conf` to enter the configuration mode to replace the complete command `configure`.

Listing Available Commands

When you type a question mark (?), the system completes the unfinished commands or gives a list of available commands.

- If you type a question mark (?) behind an incomplete command, the system gives available commands (with short description) started with the last typed letter.
- If you type a question mark (?) at any level, the system displays a list of the available commands along with a short description of each command.

Completing Partial Commands

Command completion for command keywords is available at each level of the hierarchy. To complete a command that you have partially typed, press the Tab key. If the partially typed letters begin a string that uniquely identifies a command, pressing the Tab key completes the command; otherwise, it gives a list of command suggestions. For example, type `conf` in the execution mode and press TAB, the command `configure` appears.

Using CLI

This topic describes how to view previously typed commands and how to use CLI shortcut keys.

Previous Commands

StoneOS CLI can record the latest 64 commands. To scroll the list of the recently executed commands, press the up arrow key or use Ctrl-P; to scroll forward the list, press the down arrow key or use Ctrl-N. You can execute or edit the command texts displayed in the prompt.

Shortcut Keys

StoneOS CLI supports shortcut keys to save time when entering commands and statements. The following table gives the supported shortcut keys and their functions.

Table 3: Shortcut Key List

Shortcut Key	Action
Ctrl-A	Moves cursor to the beginning of the command line.
Ctrl-B	Moves cursor back one letter.
Ctrl-D	Deletes the letter at the cursor.
Ctrl-E	Moves cursor to the end of the command line.
Ctrl-F	Moves cursor forward one letter.
Ctrl-H	Deletes the letter before the cursor.
Ctrl-K	Deletes all characters from the cursor to the end of the command line.
Ctrl-N	Scrolls forward the list of recently executed commands.
Ctrl-P	Scrolls backward the list of recently executed commands.
Ctrl-T	Switches the character at the cursor and the one before it.
Ctrl-U	Deletes all characters on the command line.
Ctrl-W	Deletes all characters before the cursor.
META-B	Moves cursor to the beginning of the word.
META-D	Deletes the word after the cursor.
META-F	Moves cursor to the end of the word.
META-Backspace	Deletes the word before the cursor.
META-Ctrl-H	Deletes the word before the cursor.

Note: For the computer without the META key, press ESC first and then press the letter. For example, to use shortcut key META-B, press ESC and then press B.

Filtering Output of Show Commands

In StoneOS CLI, the show commands display device configuration information. You can filter command output according to filter conditions separated by the pipe symbol (|). The filter conditions include:

- include {filter-condition}: Shows results that only match the filter condition. The filter condition is case sensitive.
- exclude {filter-condition}: Shows results that do not match the filter condition. The filter condition is case sensitive.
- begin {filter-condition}: Shows results that match the filter condition from the first one. The filter condition is case sensitive.

CLI output filter syntax is shown as follows:

```
hostname# show command | {include | exclude | begin} {filter-condition}
```

In this syntax, the first pipe symbol (|) is part of the command, while other pipe symbols just separate keywords, so they should not appear in the command line.

The filter conditions comply with the format of regular expression. The table below shows some common regular expressions and their meanings.

Table 4: Regular Expression and Meaning

Regular Expression	Meaning
. (period)	Represents any character.
* (star)	Indicates that there is zero or more of the preceding element.
+ (plus)	Indicates that there is one or more of the preceding element.
^ (caret)	Used at the beginning of an expression, denotes where a match should begin.
$ (dollar)	Used at the end of an expression, denotes that a term must be matched exactly up to the point of the $ character.
_(underscore)	Represents ",", "{", "}", "(", ")", beginning of a line, end of a line or space.
[] (square bracket)	Matches a single character that is contained within the brackets.
- (hyphen)	Separates the start and the end of a range.

CLI Page Display

The output messages of a command may be more than one page. When the output texts exceed one page, the CLI shows `-- More --` at the end of a page to indicate that there are more messages. In such a situation, you can make the following operations:

- To view the next line: press Enter.
- To terminate the output display: press the Q key.
- To view the next page, press any key other than Enter and Q.

Specifying Screen Size

You can specify the width and length of the CLI output screen which determines the extent of the output displayed before `-- More --` appears. The default screen length is 25 lines and the width is 80 characters.

To change the size of output screen, use the following commands:

Width: **`terminal width`** *`character-number`*

- *`character-number`* - Specifies the number of characters. The value range is 64 to 512.

Length: **`terminal length`** *`line-number`*

- *`line-number`* - Specifies the number of lines. CLI displays message lines one line less than the value specified here, but if the value is 1, the screen shows one line. The value range is 0 to 256. Setting the length to 0 disables page display option, which means it displays all messages without page split.

These settings are only available for the current connection and won't be saved to the configuration file of the device. If you close the terminal and login again, the screen width and length are restored to their default values.

Specifying Connection Timeout

Specifying connection timeout value is to set the maximum time that a session (over Console, SSH or Telnet) can be idle before the user is forced to log out.

To set the timeout value, in the global configuration mode, use the following commands:

`console timeout` *`timeout-value`*

- *`timeout-value`* - Specifies the timeout value for Console session. The range is 0 to 60 minutes. 0 means the session will never time out. The default value is 10.

To restore to the default value, in the global configuration mode, use the command **`no console timeout`**.

ssh timeout *timeout-value*

- *timeout-value* - Specifies the timeout value for SSH session. The range is from 1 to 60 minutes. The default value is 10.

To restore to the default value, in the global configuration mode, use the command **no ssh timeout**.

telnet timeout *timeout-value*

- *timeout-value* - Specifies the timeout value for Telnet session. The range is 1 to 60 minutes. The default value is 10.

To restore to the default value, in the global configuration mode, use the command **no telnet timeout**.

Redirecting the Output of Show Commands

StoneOS allows you to redirect the output messages of show commands to other destinations including FTP server and TFTP server.

To redirect the output of show commands, use the following command:

show command | **redirect** *dst-address*

The destination address (*dst-address*) can be one of the following formats:

- FTP - `ftp://[useranme:password@]x.x.x.x[:port]/filename`
- TFTP - `tftp://x.x.x.x/filename`

Diagnostic Commands

You can use `ping` to determine if a remote network is reachable, or use `traceroute` to trace the route to a network device.

System Management

Overview

This chapter describes about how to perform basic configurations of StoneOS. Topics include:

- Naming rule
- Configuring a host name
- Configuring the language of system messages
- Configuring an admin account
- Configuring a trusted host
- Management of system user
- Configuring a management interface
- Configuring a storage device
- Managing configuration files
- System maintenance and debugging
- Rebooting the system
- Upgrading StoneOS
- Graceful Shutdown
- SCM HA
- Managing license
- Simple Network Management Protocol (SNMP)
- HSM Agent
- Network Time Protocol (NTP)
- Configuring a schedule
- Configuring a track object
- Configuring Monitoring
- The maximum concurrent sessions

Naming Rules

When you name an object, follow the conventions below:

- Hillstone recommends you to not use the following special characters: comma (,), single quotation marks (‘), quotation marks (“), tab, space, semicolons (;),

backslash (\), slash (/), angle brackets (<>), and other special characters (&, #). It is recommend that you should use figures (0-9) and letters (a-z, A-Z) in the name.

- If an object name has space in it, you need to enclose the entire name in quotation marks when you use CLI, but this does not apply to WebUI operations.

Configuring a Host Name

A host name distinguishes one device from another. The default host name is the platform model.

To edit a host name, in the global configuration mode, use the following command:

hostname *host-name*

- *host-name* – Specifies the host name of the Hillstone device. You can specify up to 63 characters. After executing the command, the command prompt will be changed to the specified host name.

To restore to default value, in global configuration mode, use the command **no hostname**.

For example, the following commands change the host name to **hillstone**:

```
hostname# configure
hostname(config)# hostname hillstone
hillstone(config)#
```

Configuring System Admin Users

Device administrators of different roles have different privileges. The system supports pre-defined administrator roles and customized administrator roles.

By default, the system supports the following administrators, which cannot be deleted or edited:

- **admin**: can write, execute and write the system. Administrator role can manage all functions of the device, view configurations and execute commands like **import**, **export** and **save** etc. under configuration mode.
- **admin-read-only**: can write and execute, view configurations, and execute **export** command under configuration mode.
- **operator**: can write, execute and write the system. Operator can modify settings others than administrator privileges, reboot the system, restore factory defaultand upgrade StoneOS, view configurations, but operators cannot view log messages, and execute some commands.
- **auditor**: can manage log messages, including view, export and clear logs.

The table lists admin user's permissions.

Operation	Permissions

	Adminisrator	Adminisrator-read-only	Operator	Auditor
Configure (including save configuration)	√	X	√	X
Managing admin users	√	X	X	X
Restore factory default	√	X	X	X
Delete configuration file	√	X	√	X
Roll back configuration	√	X	√	X
Reboot	√	X	X	X
View configuration information	√	√	√	X
View log information	√	√	X	√
Modify current admin password	√	√	√	√
Command `import`	√	√	√(except upgrading StoneOS)	√
Command `export`	√	X	√	X
Command `clear`	√	√	√	√
Command `ping/traceroute`	√	√	√	√
Command `debug`	√	√	√	X
Command `exec`	√	√	√	X
Command `terminal width`	√	√	√	√

Note:

- The system has a default administrator "hillstone". This default administrator can be edited, but not deleted.
- Except administrator, other roles cannot edit properties of a system admin user, but only its own password.
- Auditor can manage one or more log messages, but an auditor's log types are defined by users of administrator role.

You can also customize the administrator roles, specify the privileges of CLI and WebUI.

- CLI privileges includes read-write and unavailable.
- Privileges of each module's WebUI includes read-write, read-only, and unavailable.

The property settings of a system administrator are:

- Creating administrator roles
- Specifying administrator role's privileges
- Specifying administrator role's description
- Creating an admin user
- Assigning a role
- Configuring password
- Configuring accesses for admin users
- Configuring log types for auditors
- Specifying login limit
- Viewing admin users
- VSYS admin users

Creating Administrator Roles

To create a new administrator role, use the following command in the global configuration mode:

admin role *role-name*

- *role-name* – Specifies the name of the administrator role. The length varies from 4 characters to 95 characters. After executing this command, the system will create the administrator role and enter the administrator role configuration mode. If the name already exists, it will enter the administrator role configuration mode directly.

To delete an administrator role, use the **no admin role** *role-name* command.

Specifying Administrator Role's Privileges

To specify the administrator role's privileges of CLI, use the following command in the administrator role configuration mode:

cli-privilege all {rw | none}

- **rw | none** – **rw** represents the administrator role has the read-write privilege to all CLI commands. **none** represents the administrator role does not have privilege of CLI and cannot use CLI.

To specify the administrator role's privileges of WebUI, use the following command in the administrator role configuration mode:

ui-privilege *module-name* **{none | r | rw}**

- *module-name* – Specify the module name. To obtain the module list, enter the question mark (?) behind **ui-privilege**.
- **none | r | rw** – Set the administrator role's privilege of the specified module. **none** represents the administrator role does not have privilege of the specified module, and cannot read and write the configurations of the specified module. **r** represents the administrator role has the read privilege of the specified module, and cannot write the configurations. **rw** represents the administrator role can read and write the configurations of the specified module.

To cancel the privilege settings, use the **no ui-privilege** *module-name* command.

Specifying Administrator Role's Description

To specify administrator role's description, use the following command in the administrator role configuration mode:

description *description*

- *description* – Specify the description for the administrator role. You can specify up to 255 characters.

Use the **no description** command to delete the description.

Creating an Admin User

To create an admin user and enters its configuration mode, under glocal configuration mode, use the following command:

admin user *user-name*

- *user-name* - Specifying a name for the admin user. The length is from 4 to 31 characters. This command not only creates the admin user, also enters the user's configuration mode; if the admin user exists, it enters its configuration mode directly.

To delete an admin user, under global configuration mode, use the command **no admin user** *user-name*.

When you are under an admin user's mode, you can edit its role, password, access methods and log types (for auditor roles).

Assigning a Role

To assign a role for an admin user, in the user's configuration mode, use the following command:

role {admin | operator |auditor |admin-read-only}

- **admin** - Specifying the role of this user as an Administrator.
- **operator** - Specifying the role of this user as an Operator.

- **auditor** - Specifying the role of this user as an Auditor.
- **admin-read-only** - Specifying the role of this user as an Administrator-read-only.

Configuring Password

Password is required for an admin account. To define a password, in the admin user's configuration mode, use the following command:

password *password*

- *password* – Specify a password for admin user. The length is from 4 to 31 characters.

To cancel a password, under the admin user's conguration mode, use the command **no password**.

If you login as an operation, auditor or administrator-read-only, you can edit your own password under any mode:

exec admin user password update *password*

- *password* –Enter the new password. The length is from 4 to 31.

Note:If you use an Administrator account, you have the privilege to edit the password of every user.

Configuring Password Policy for Admin Users

Password policy defines admin user's password complexity. The password complexity controls the total length of the password, the length of each element, and the validity period of the password. A password can be a combination of elements from the following types:

- Capital letters A to Z.
- Lowercase letters a to z.
- Figures 0 to 9.
- Other visible characters such as semicolon,slash(only support DBC case).

You must enter the password policy mode before you can change the complexity requirement. Use the command **password-policy** to enter password policy conifiguration mode.

You can set the password complexity if the default-settings can not fit the security requirement.You must enable password complexity checking before setting the password complexity.

To enable or disable password complexity checking, in password policy configuration mode, use the following command:

admin complexity {**enable** | **disable**}

- **enable** | **disable** – Enable or disable password complexity checking.By default, the password complexity checking is disabled.After the feature is enabled, the default complexity requires that the password must contain all the four types of formats: two captalized letters, two lowercase letters, two figures and two other visible characters (e.g.@).

To define the length of password elements, in password policy configuration mode, use the following command:

admin {**capital-letters | non-alphanumeric-letters | numeric-characters | small-letters}** *value*

- **capital-letters** *value* – Specify the length of capital letters in password. The default value is 2 and the range is 0 to 16.
- **non-alphanumeric-letters** *value* – Specify the length of visible characters except letters and figures in password. The default value is 2 and the range is 0 to 16.
- **numeric-characters** *value* – Specify the length of figures in password. The default value is 2 and the range is 0 to 16.
- **small-letters** *value* – Specify the length of lowercase letters in password. The default value is 2 and the range is 0 to 16.

To define the minimum length of password for the admin users, in password policy configuration mode, use the following command:

admin min-length *length-value*

- **min-length** *length-value* – Specify the minimum length of the password. The default value is 4, and the range is 4 to 16. After password complexity checking is enabled, the default value is 8(two captalized letters, two lowercase letters, two figures and two other visible characters), and the range is 8 to 16.

Note: You can define the minimum length of the password in order to strengthen the security whether the password complexity checking is enabled or not.

The validity period of the password is used to limit the time that you use password. When you log in, if the entered password has expired, the system will prompt to reset the password.After pressing Enter,please enter the new password again. If the new password does not meet the password complexity requirements or the new passwords for the two times are not consistent, you need to reinput. Given that continuous input for three times does not meet the requirement of the password, you can not connect to the device. You are still required to set a new password when logging in again. The new password can be the same as the old one.

To define the validity period of the password for the admin users, in password policy configuration mode, use the following command:

admin password-expiration *value*

- **password-expiration** *value* – Specify the validity period of the password. The unit is day. The range is 0 to 365. The default value is 0, which indicates that there is no restriction on validity period of the password.

Under the password poicy configuration mode, use the command **no admin complexity** to resume the default setting of password complexity checking.

Viewing Password Policy for Admin Users

To view password policy for admin users, in any mode, use the command:

show password-policy

Configuring Accesses for Admin Users

By default, a newly created admin user does not have its access opened to visit the device.

access {**console** | **http** | **https** | **ssh** | **telnet** | **any**}

- **console** – Allows admin user to use Console port to access the device.
- **http** – Allows admin user to use Console port to access the device.
- **https** – Allows admin user to use Console port to access the device.
- **ssh** – Allows admin user to use Console port to access the device.
- **telnet** – Allows admin user to use Console port to access the device.
- **any** – Allows admin user to use Console port to access the device.

Use this command to add access for admin user.

To cancel an access, use the command **no access** {**console** | **http** | **https** | **ssh** | **telnet** | **any**}.

Configuring Log Types for Auditors

An admin user of auditor role is only allowed to view, export and clear log messages. The log types that can be visited by auditor is also defined by Administrator. To specify the log types, under auditor's configuration mode, use the command:

log {**config** | **event** | **nbc** | **ips** | **traffic** | **network | security**}

- **config** – Specify that the auditor can manage configuration logs.
- **event** – Specify that the auditor can manage event logs.
- **nbc** – Specify that the auditor can manage NBC logs.
- **ips** – Specify that the auditor can manage IPS logs.
- **traffic** – Specify that the auditor can manage traffic logs.
- **network** – Specify that the auditor can manage network logs.
- **security** – Specify that the auditor can manage security logs.

Repeat this command to spcify more than one log types.

To cancel access to a log type, use the command **no log** {**config** | **event** | **nbc** | **ips** | **traffic** | **network | security**}

Specifying Login Limit

If an admin user failes to enter correct password for the specified times, the user will be disallowed to login again within the specified duration. To specify a lockout duration, under global configuration mode, use the following command:

admin lockout-duration *time*

- **lockout-duration** *time* – Specifying lockout duration. The unit is minute. The length is 1 to 65525. The default value is 2.

Use the command **no admin lockout-duration** to resume to the default value.

To specify the maximum login failure time, under the global configuration mode, use the command:

admin max-login-failure *times*

- **max-login-failure** *times* – Specify the maximum error password times. The default value is 3, and the range is 1 to 256.

Use the command **no admin max-login-failure** to resume to the default failure time.

Note: This command is available only for admin user of administrator role.

Viewing Admin Users

To view admin users, under any mode, use the command:

- To show admin users: **show admin user**
- To show details of an admin user: **show admin user** *user-name*
- To show lockout duration: **show admin lockout-duration**
- To show maximum login failure time: **show admin max-login-failure**

VSYS Admin Users

The admin users of each VSYS are independent from other VSYS. VSYS admin users also have different roles of Administrator, Administrator-ready-only, operator and auditor. Their roles and previleges are the same with normal admin users.

When creating VSYS administrators, you must follow the requirements listed below:

- Backslash (\) cannot be used in administrator names.
- The non-root administrators are created by root RXW administrators after logging into non-root VSYS.
- After logging into root VSYS, the root administrators can switch to non-root VSYS and configure it.
- Non-root administrators can enter the corresponding non-root VSYS after the successful login, but the non-root administrators cannot switch to the root VSYS.
- Each administrator name should be unique in the VSYS it belongs to, while

administrator names can be the same in different VSYSs. In such a case, when logging in, you must specify the VSYS the administrator belongs to in the format of vsys_name\admin_name. If no VSYS is specified, you will enter the root VSYS.

The table lists VSYS admin user's permissions.

Operation	Permissions							
	Root VSYS Administrator	Root VSYS Administrator-read-only	Root VSYS Operator	Root VSYS Auditor	Non-root VSYS Administrator	Non-root VSYS Administrator-read-only	Non-root VSYS Operator	Non-root VSYS Auditor
Configure (including save configuration)	√	X	√	X	√	X	√	X
Managing admin users	√	X	X	X	√	X	X	X
Restore factory default	√	X	X	X	X	X	X	X
Delete configuration file	√	X	√	X	√	X	√	X
Roll back configuration	√	X	√	X	√	X	√	X
Reboot	√	X	√	X	X	X	X	X
View configuration information	√	√	√	X	View info in current VSYS	View info in current VSYS	View info in current VSYS	X
Modify current admin password	√	√	X	√	√	√	X	√
Command `import`	√	√	√	√	√	√	√	√
Command `export`	√	X	√	X	√	X	√	X
Command `clear`	√	√	√	√	√	√	√	√
Command `ping/traceroute`	√	√	√	√	√	√	√	√
Command `debug`	√	√	√	X	√	√	√	X
Command `exec`	√	√	√	X	X	X	X	X
Command `terminal width`	√	√	√	√	√	√	√	√

Operation	Permissions							
	Root VSYS Adminisrator	Root VSYS Adminisrator-read-only	Root VSYS Operator	Root VSYS Auditor	Non-root VSYS Adminisrator	Non-root VSYS Adminisrator-read-only	Non-root VSYS Operator	Non-root VSYS Auditor
View configuration information	√	√	√	√	√	√	√	X

Creating a Trusted Host

Hillstone device allows only trusted host to manage the system. Trusted hosts are recognized by their IP addresses. If the host IP address is in the specified IP range, the host is a trusted host.

By default, the trusted IP range is 0.0.0.0/0, which means all hosts are trusted. Therefore, you are suggested to configure a proper trusted IP range and delete the default range afterwards.

Note: When you cannot access the device from a particular host, check the IP settings of trusted host.

To set the IP range for the trusted host, in the global configuration mode, use the following command:

admin host {*A.B.C.D A.B.C.D* | **range** *A.B.C.D A.B.C.D* | *A.B.C.D/M* | **any**} {**http** | **https** | **ssh** | **telnet** | **any**}

- *A.B.C.D A.B.C.D* | **range** *A.B.C.D A.B.C.D* | *A.B.C.D/M* | **any** - Specifies the start IP and end IP of trusted hosts, for example, "1.1.1.1 255.255.0.0". **any** means you can access the device from any host.
- **http** | **https** | **ssh** | **telnet** | **any** - Specifies the protocol you can use to access the device from a trusted host. **any** means all the four protocols are enabled.

You can specify up to 128 trusted IP ranges.

To delete a trusted IP range, use the command **no admin host** *A.B.C.D A.B.C.D*.

To disable access to the device over the specified protocol, use the command **no admin host** {*A.B.C.D A.B.C.D* | **range** *A.B.C.D A.B.C.D* | *A.B.C.D/M* | **any**} {**http** | **https** | **ssh** | **telnet** | **any**}.

Viewing Trusted Host IP

To view information on configured trusted IP range, in any mode, use the following command:

show admin host

Configuring NetBIOS Name Resolution

The feature of NetBIOS name resolution enables the system to get all registered NetBIOS names of computers in the managed network, and store them in the cache, so that it can provide IP address-NetBIOS name resolution service for functional modules.

So far, NetBIOS name resolution is only used by the traffic logging feature to display the host name in its logs. Therefore, you should enable the NetBIOS name resolution if you want to view host names in traffic logs. For information about how to configure traffic log, see "Displaying Hostname/Username in the Traffic Logs" of "Logs".

To configure NetBIOS name resolution, take the following steps:

1. Enable the NetBIOS host name resolution service for the specified zone (the zone should not the one being connected to WAN).
2. StoneOS automatically looks up NetBIOS names for IP addresses in the stat-sets.

This process may take a while and the results are stored in the NetBIOS cache table. The table is updated regularly by the system.

Note: The computer's host name cannot be searched unless it is enabled with NetBIOS.

Enabling NetBIOS Name Resolution

To enable NetBIOS name resolution for a zone, in the zone configuration mode, use the following command:

```
nbt-cache enable
```

To disable NetBIOS name resolution, use the following command:

```
no nbt-cache enable
```

Note: To enter a zone configuration mode, use the command **zone** *zone-name*.

Resolving an IP to NetBIOS Name

To resolve an IP address of a host to its NetBIOS host name and MAC address, in the global configuration mode, use the following command:

nbtstat ip2name *ip-address* [**vrouter** *vrouter-name*]

- *ip-address* - Specifies the IP address to be resolved.
- **vrouter** *vrouter-name* - Specifies the VR of the host. If this parameter is not defined, StoneOS uses the default VR (trust-vr).

Clearing NetBIOS Cache

To clear NetBIOS cache, in the global configuration mode, use the following command:

clear nbt-cache [*ip-address*][**vrouter** *vrouter-name*]

- *ip-address* - Specifies the IP address and NetBIOS cache data related to this IP address are cleared by the system. If this parameter is not defined, all NetBIOS cache data are cleared.
- **vrouter** *vrouter-name* - Specifies the VR and NetBIOS cache data related to this VR are cleared by the system. If this parameter is not specified, all NetBIOS cache data are cleared.

Viewing NetBIOS Cache

To view NetBIOS cache data (including IP address, host name, MAC address and VR), in any mode, use the following command:

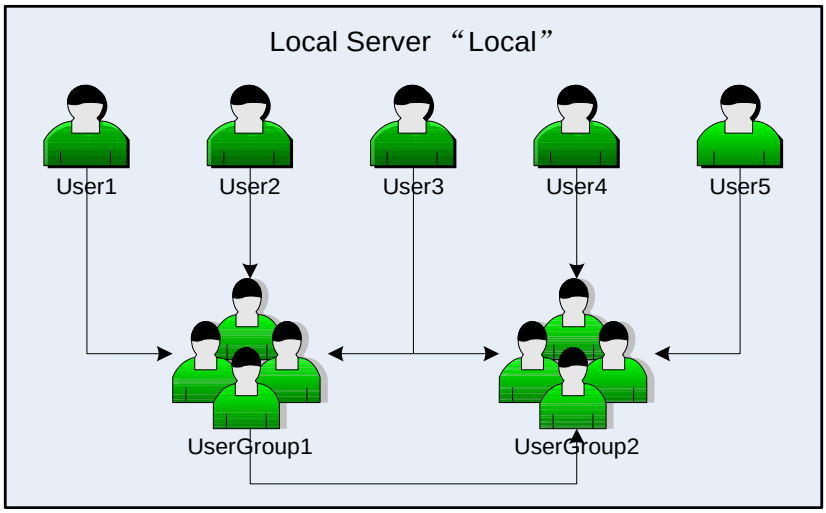
show nbt-cache [*ip-address*][**vrouter** *vrouter-name*]

- *ip-address* - Shows NetBIOS cache data related to the specified IP address. If this parameter is not defined, all NetBIOS cache data are displayed.
- **vrouter** *vrouter-name* - Shows NetBIOS data of the specified VR. If this parameter is not defined, all NetBIOS cache data are displayed.

Management of System User

In StoneOS, user refers to the user who uses the functions and services provided by the Hillstone device, or who is authenticated or managed by the device. The authenticated users consist of local user and external user. The local users are created by administrators. They belong to different local authentication servers, and are stored in system's configuration files. The external users are stored in external servers, such as AD server or LDAP server. StoneOS supports user group to facilitate user management. Users belonging to one local authentication server can be allocated to different user groups, while one single user can belong to different user groups simultaneously; similarly, user groups belonging to one local authentication server can be allocated to different user groups, while one single user group can belong to different user groups simultaneously. The following diagram takes the default AAA server Local as an example and shows the relationship between users and user groups:

Figure 1: Relationship between User and User Group



As shown above, User1, User2 and User3 belong to UserGroup1, while User3 also belongs to UserGroup2, and UserGroup2 also contains User4, User5 and UserGroup1.

Roles are designed with certain privileges. For example, a specific role can gain access to some specified network resources, or exclusively use some bandwidth. In StoneOS, users and privileges are not directly associated. Instead, they are associated by roles. The mappings between roles and users are defined by role mapping rules. When a role is assigned with some services, its mapped users receive the corresponding services as well. StoneOS supports the AND, NOT or OR logical calculation of roles.

Hillstone device supports the following role-based functions:

- Role-based policy: Access control over users according to their roles.
- Role-based QoS: Bandwidth control over users according to their roles.
- Role-based stat-set: Collects statistics on bandwidth, sessions and new sessions based on roles.
- Role-based session limit: Implements session limits for specific users.
- SCVPN role-based host security check: Resource access control over users according to roles.

Configuring Users

User configurations include static user binding configuration and authenticated user configuration.

Binding an IP/MAC Address to a User

To bind an IP address or MAC address to a user, in the global configuration mode, use the following command:

user-binding *aaa-server-name user-name* {**ip** *ip-address* [**auth-check-only** | **vrouter** *vr-name*] | **mac** *mac-address*}

- *aaa-server-name* - Specifies the name of the user's AAA server.
- *user-name* - Specifies the user name.
- **ip** *ip-address* - Specifies the IP address.
- **auth-check-only** - If this parameter is configured, the system checks if the user IP address conforms with the bound IP of this user. If it conforms, the user is allowed to enter authentication stage.
- **vrouter** *vr-name* - Specifies the VR of the designated IP/MAC address. The default value is the default VR (trust-vr).**mac** *mac-address* - Specifies the MAC address.

To remove the binding of IP/MAC and user, in the global configuration mode, use the following command:

no user-binding *aaa-server-name user-name* {**ip** *ip-address* [**auth-check-only**] | **mac** *mac-address*} [**vrouter** *vr-name*]

WebUI: Select **Objects** > **User Binding** from the menu bar.

Configuring Users in the Local AAA Servers

You can configure users/user groups to a local AAA server.

To enter the local AAA server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type local**.

To create a local user, in the local AAA server configuration mode, use the following command:

user *user-name*

- *user-name* - Specifies the user name. You can specify up to 63 characters. This command creates a user and leads you into its configuration mode; if the user name exists, you will directly enter the user configuration mode.

To delete the specified user, in the AAA server configuration mode, use the following command:

no user *user-name*

Configurations of a local user include:

- Basic settings: password, expiration, description and user group configuration.
- Dial-up VPN settings: IKE ID configuration.
- PnPVPN settings: DNS server, WINS server, IP/netmask/gateway/tunnel routing of DHCP address pool and tunnel routes. For detailed information, see "Configuring User's Network" of "Firwall".

Configuring Password

To specify a password, in the user configuration mode, use the following command:

password *password*

- *password* - Specifies the user password. You can specify up to 31 characters.

To delete a password, in the user configuration mode, use the following command:

no password

Specifying a User Expiration Date

An expired user cannot pass the authentication, so it becomes an invalid user. By default, all users have no expiration date set.

To specify the expiration date and time for a user, in the user configuration mode, use the following command:

expire *Month/day/year HH:MM*

- *Month/day/year HH:MM* - Specifies the date and time in the format of month/date/year hour:minute. For example, expire 02/12/2010 12:00 indicates that the user is invalid since 12:00, February 12nd, 2010.

To cancel the expiration date configuration, in the user configuration mode, use the following command:

no expire

Describing a User

To give some description for a user, in the user configuration mode, use the following command:

desc *string*

- *string* - Specifies description at a maximum of 31 characters.

To delete the description, in the user configuration mode, use the following command:

no desc

Specifying an IKE ID

The Dial-up VPN users need IKE IDs. To specify an IKE ID, in the user configuration mode, use the following command:

ike_id {**fqdn** *string* | **asn1dn** *string* | **key-id** *string*}

- **fqdn** *string* - Uses IKE ID of the FQDN (Fully Qualified Domain Name) type. *string* is the ID content.
- **asn1dn** *string* - Uses IKE ID of the Asn 1dn type, which is only applicable to the user with a certificate. *string* is the ID content.
- **key-id** *string* – Specifies the ID that uses the type of the Key ID. This type can only be used in the XAUTH function.

To delete the IKE ID of a user, in the user configuration mode, use the following command:

no ike_id

Specifying a User Group

You can categorize users into a group according to your need. One user is allowed to be in multiple groups.

To specify a group for a user, in the user configuration mode, use the following command:

group *user-group-name*

- *user-group-name* - Specifies the name of an existing group in the system. You can specify up to 127 characters.

Repeat this command to define more user groups for a user.

To cancel a user-user group relationship, in the user configuration mode, use the following command:

no group *user-group-name*

For more information about user group settings, see Configuring a User Group.

Viewing User/User Group Information

To view the information of user/user group, in any mode, use the following commands:

- Show all users: **show user**
- Show a specific user: **show user aaa-server** *server-name* [**name** *user-name*]
- Show the IP/MAC and user bindings: **show user-binding aaa-server** *server-name*
- Show user groups: **show user-group aaa-server** *server-name*

Configuring a User Group

You can configure users or user groups on a local AAA server. To enter the local AAA server configuration mode, in the global configuration mode, use the command **aaa-server** *aaa-server-name* **type local**.

To create a local user group, in the local AAA server configuration mode, use the following command:

user-group *user-group-name*

- *user-group-name* - Specifies a name for the user group.

This command creates the user group and leads you into the user group configuration mode; if the user group of the specified name exists, you will enter the user group configuration mode directly.

To delete the specified user group, use the following command:

no user-group *user-group-name*

To add a member (either a user or another user group) to the user group, in the user group configuration mode, use the following command:

member {**user** *user-name* | **group** *user-group-name*}

- *user-name* - Specifies the user name.
- *user-group-name* - Specifies the user group name. A user group can include up to five nested layers, but a group cannot add itself as a member.

Repeat this command to add more members to a group.

To delete a member from a user group, in the user group configuration mode, use the following command:

no member {**user** *user-name* | **group** *user-group-name*}

Configuring a Role

Role configurations include:

- Creating a role
- Creating a role mapping rule
- Configuring a role combination

Creating a Role

To create a role, in the global configuration mode, use the following command:

role *role-name*

- *role-name* - Specifies a name for the role. You can specify up to 31 characters.

To delete a role, in the global configuration mode, use the following command:

no role *role-name*

Creating a Role Mapping Rule

Role mapping rule defines the mapping relationship between a role and user/user group. StoneOS supports up to 64 role mapping rules, and each rule has a maximum number of 256 entries.

When the authentication for SCVPN is set to USB Key only, the system can map a role for the user according to the CN or OU field of the USB Key certificate. For more

information about USB Key authentication, see "Authentication With USB Key Certificate" of "VPN".

To enter the role mapping rule configuration mode, in the global configuration mode, use the following command:

role-mapping-rule *rule-name*

- *rule-name* - Specifies a name for the role mapping rule. You can specify up to 31 characters. This command creates a rule and leads you in the role mapping rule configuration mode; if this rule exists, you will enter its configuration mode directly.

To delete the specified role mapping rule, in the global configuration mode, use the following command:

no role-mapping-rule *rule-name*

To configure a role mapping rule, in the role mapping rule configuration mode, use the following command:

match {**any** | **user** *user-name* | **user-group** *user-group-name* | **cn** *cn-field* | **ou** *ou-field*} **role** *role-name*

- **any** | **user** *user-name* | **user-group** *user-group-name* | **cn** *cn-field* | **ou** *ou-field* - Specifies the user, user group, certificate name or organization unit for the mapping. **any** refers to any user, user group, certificate name or organization unit in the system.
- **role** *role-name* - Specifies a role to be mapped in this rule.

Repeat this command to add more mapping rules.

To delete the specified mapping rule, in the role mapping rule configuration mode, use the following command:

no match {**any** | **user** *user-name* | **user-group** *user-group-name* | **cn** *cn-field* | **ou** *ou-field*} **role** *role-name*

Configuring a Role Combination

Roles can be grouped using logical calculation into a role combination. To configure a role combination, in the global configuration mode, use the following command:

role-expression [**not**] *r1* [{**and** | **or**} [**not**] *r2*] **role** *r3*

- [**not**] *r1* - Specifies the first role in this combination. **not** means excluded; *r1* refers to the name of an existing role. For example, "not testrole1" means all roles other than testrole1.
- **and** | **or** - Specifies the logical operator.
- [**not**] *r2* - Specifies the second role in this combination. *r2* refers to the name of an existing role.

- **role** *r3* - Specifies the calculated result. *r3* refers to the name of the result.

To delete the specified role combination, in the global configuration mode, use the following command:

no role-expression [**not**] *r1* [{**and** | **or**} [**not**] *r2*] **role** *r3*

Viewing Role Information

To view role related information, use the following commands:

- Show role information: **show role**
- Show role mapping rule information: **show role-mapping-rule** [*rule-name*]
- Show role combination information: **show role-expression**

Configuring a MGT Interface

You can login to the Hillstone device over Console port, Telnet, SSH, or WebUI and configure their timeout settings, port number and PKI trust domain of HTTPS.

If you fail to login to the device three times in one minute over Telnet, SSH, HTTP or HTTPS, your login attempts will be refused in two minutes.

WebUI: Select **System** > **Device Management** > **MGT Interface** from the menu bar

Configuring a Console MGT Port

This section describes how to configure the baud rate and timeout value of the console port.

Configuring the Baud Rate

To configure the baud Rate of console port, in any mode, use the following command:

exec console baudrate {**9600** | **19200** | **38400** | **57600** | **115200**}

- **9600** | **19200** | **38400** | **57600** | **115200** - Specifies the baud rate. The unit is bps and the default value is 9600.

Note that when you login to the device, the baud rate of your console terminal should conform to the console baud rate specified here.

Configuring Timeout

If there is no configuration performed by the logged-in administrator until timeout, the system will disconnect the connection.

To configure the console timeout value, in the global configuration mode, use the following command:

console timeout *timeout-value*

- *timeout-value* - Specifies console timeout value. The value range is 0 to 60 minutes; the value of 0 means no time limit. The default value is 10.

To restore to the default value of console timeout, in the global configuration mode, use the following command:

no console timeout

Configuring a Telnet MGT Interface

When you login to the device over Telnet, your Telnet port should conform with the device Telnet port specified here. If an established Telnet connection does not send Telnet request until timeout, it will be disconnected.

To configure the Telnet timeout value, in the global configuration mode, use the following command:

telnet timeout *timeout-value*

- *timeout-value* - Specifies the Telnet timeout value. The range is 1 to 60 minutes. The default value is 10.

To restore to the Telnet default timeout value, in the global configuration mode, use the following command:

no telnet timeout

To configure the allowed maximum number of sessions, in the global configuration mode, use the following command:

telnet max-session *max-session*

- *max-session* – Specifies the allowed maximum number of sessions. The maximum number of sessions of difference platforms differs. The default value of each platform is the maximum number of sessions.

To restore the session numbers to the default value, in the global configuration mode, use the following command:

no telnet max-session

To specify the port number of Telnet, in the global configuration mode, use the following command:

telnet port *port-number*

- *port-number* - Specifies Telnet port number. The range is 1 to 65535. The default value is 23.

To restore to the default value, in the global configuration mode, use the following command:

no telnet port

Telnet maximum login number defines how many times you can try to login to the device over Telnet. If you fail more than the maximum times, your Telnet login attempts will be refused.

To specify the Telnet maximum login number, in the global configuration mode, use the following command:

telnet authorization-try-count *count-number*

- *count-number* - Specifies the maximum login number. The value range is 1 to 10 times. The default value is 3.

To restore to the default value, in the global configuration mode, use the following command:

no telnet authorization-try-count

Configuring a SSH MGT Interface

This section describes how to configure SSH timeout value, port number and connection interval.

SSH timeout value defines the maximum idle time of a SSH connection. If an established SSH connection does not send any SSH request until timeout, it will be disconnected.

To configure the SSH timeout value, in the global configuration mode, use the following command:

ssh timeout *timeout-value*

- *timeout-value* - Specifies the SSH maximum idle time. The value range is 1 to 60 minutes. The default value is 10.

To restore to the default value, in the global configuration mode, use the following command:

no ssh timeout

To configure the allowed maximum number of sessions, in the global configuration mode, use the following command:

ssh max-session *max-session*

- *max-session* – Specifies the allowed maximum number of sessions. The maximum number of sessions of difference platforms differs. The default value of each platform is the maximum number of sessions.

To restore the session numbers to the default value, in the global configuration mode, use the following command:

no ssh max-session

To set up the SSH port number, in the global configuration mode, use the following command:

ssh port *port-number*

- *port-number* - Specifies the SSH port number. The value range is 1 to 65535. The default value is 22.

To restore to the default SSH port number, in the global configuration mode, use the following command:

no ssh port

SSH connection interval specifies the frequency of receiving SSH requests. When an SSH connection is established, the device receives the next SSH connection request at an interval of the time specified here.

ssh connection-interval *interval-time*

- *interval-time* - Specifies an interval time. The value range is 2 to 3600 seconds. The default value is 2.

To restore to the default value, in the global configuration mode, use the following command:

no ssh connection-interval

Configuring a WebUI MGT Interface

This section describes how to configure parameters of WebUI (HTTP or HTTPS) access.

To define the WebUI timeout value, in the global configuration mode, use the following command:

web timeout *timeout-value*

- *timeout-value* - Specifies the WebUI timeout value. The value range is 1 to 1440 minutes. The default value is 10.

To restore to the default WebUI timeout value, in the global configuration mode, use the following command:

no web timeout

To specify the HTTP port number, in the global configuration mode, use the following command:

http port *port-number*

- *port-number* - Specifies the port number of HTTP. When visiting WebUI over HTTP, the browser's HTTP port must be the same as the port number specified here. The value range is 1 to 65535. The default value is 80.

To restore to the default HTTP port number, in the global configuration mode, use the following command:

no http port

To configure the anti-XSS service, in the global configuration mode, use the following command:

http anti-xss { **disable** | **enable** | **mode** {**normal**| **strict**}}

- **disable** | **enable** – Disables/Enables the anti-XSS service. By default, this service is enabled.
- **mode** {**normal**| **strict**} – Specifies the mode of the anti-XSS service, including the character matching mode and the regular expression mode.

In the global configuration mode, use the following command to restore the configurations to the default.

no http anti-xss { **disable** | **enable** | **mode** {**normal**| **strict**}}

To specify the HTTPS port number, in the global configuration mode, use the following command:

https port *port-number*

- *port-number* - Specifies the HTTPS port number. When visiting WebUI over HTTPS, the browser's HTTPS port number must be the same as the port number specified here. The value range is 1 to 65535. The default value is 443.

To restore to the default HTTPS port number, in the global configuration mode, use the following command:

no https port

To specify the PKI trust domain of HTTPS, in the global configuration mode, use the following command:

https trust-domain *trust-domain-name*

- *trust-domain-name* - Specifies the name of PKI trust domain. When HTTPS starts, HTTPS server uses the certificates of the specified PKI trust domain. If no trust domain is specified, the default PKI domain (trust_domain_default) will be used.

To restore the default PKI trust domain, in the global configuration mode, use the following command:

no https trust-domain

Viewing MGT Interface Configuration Information

To view management interface configuration information, in any mode, use the following commands:

- Show console port configuration information: **show console**
- Show Telnet configuration information: **show telnet**
- Show SSH configuration information: **show ssh**
- Show Web configuration information: **show http**

Configuring a Storage Device

Hillstone network behavior control feature allows you to keep full records of user network behaviors. The logs are stored in a local database in form of a database file.

The storage device that can accommodate local database can be an SD card, USB disk or the storage expansion module provided by Hillstone.

Formatting a Storage Device

If a storage device cannot function, or its file system is not supported by StoneOS, or it has not been formatted yet, you can execute formatting command to repair it, change its file system or format it.

To format a storage device, in any mode, use the following command:

exec format [**sd0** | **usb0** | **usb1** | **storage***X*]

- **sd0** - Formats the SD card in the SD slot.
- **usb0** | **usb1** - Formats the USB disk inserted to the device's USB port.
- **storage***X* - Formats the storage expansion module in the specified slot. *X* is the slot number and its value range varies from platform types.

Note: Formatting a storage device erases all the data in it. You should back up your files.

Removing a Storage Device

If you pull out the storage device with force, unsaved data may be lost. To ensure data integrity, you should use the command below to safely remove the device.

To safely remove a storage device, in any mode, use the following command:

exec detach [**sd0** | **usb0** | **usb1** | **storage***X*]

- **sd0** - Removes the SD card from the SD slot.
- **usb0** | **usb1** - Removes the USB disk from the specified USB port.
- **storage***X* - Removes the storage expansion module from the specified slot.

Managing Configuration Files

All information of system configuration, such as its initial and current configuration information, is stored in the configuration files. You can use command lines or visit the WebUI to view all sorts of system configurations. The information is stored and displayed in the format of command line.

Managing Configuration Information

This section describes how to view, import, export and save the configuration information.

Note: Passwords of local users won't be exported when you export configuration information.

Viewing Configuration Information

Initial configuration information, stored in the configuration file, is used to configure the system parameters when the device is powered on. If no proper initial configuration information is found, the device uses default parameters to initialize the system. Similarly, the parameter settings the system is using now are called current configuration information.

StoneOS saves ten versions of initial configuration information. The latest one is used by the system as its initial configuration information when it starts up; the other versions are backup files. The last saved configuration information is marked as "current" and the nine backup versions are marked by number from 0 to 8 based on their saved time.

To view the initial configuration information, in any mode, use the following command:

show configuration [**startup**]

To view configuration information other than the current one, in any mode, use the following command:

show configuration backup *number*

- *number* - Specifies the number of the configuration information.

To view the configuration information record other than the current one, in any mode, use the following command:

show configuration record

To view the current interface configuration information, in any mode, use the following command:

show configuration interface *interface-name*

To view the current configuration information, in any mode, use the following command:

show configuration

To view the current configuration information the system is using, in any mode, use the following command:

show configuration running

To view the current address book configuration information the system is using, in any mode, use the following command:

show configuration address

To view the current policy configuration information the system is using, in any mode, use the following command:

show configuration policy

To view the current routing configuration information the system is using, in any mode, use the following command:

show configuration vrouter

Output the current configuration information using the XML format, in any mode, use the following command:

show configuration xml

WebUI: Select **System** > **Configuration File Management** from the menu bar.

Reverting to Previous Configurations

StoneOS saves the latest ten versions of system configurations as initial configuration files for you to use in system initiation.

To revert the system configurations to an earlier backup version, in the configuration mode, use the following command and then restart the device:

rollback configuration backup *number*

- *number* - Specifies the number of initial configuration file. When the system restarts, the specified configurations will be used.

Deleting a Configuration File

To delete a configuration file from the system, in the configuration mode, use the following command:

delete configuration {**startup** | **backup** *number*}

- **startup** - Deletes the current configuration file.
- **backup** *number* - Deletes the specified backup configuration file.

Saving Configuration Information

When the current configurations are saved, they become the initial configuration information used by the system as next start-up configurations.

To save the current configurations, in any mode, use the following command:

save [*string*]

- *string* - Give some description for the saved configuration. If you leave this parameter blank, the former configurations will be replaced.

Exporting Configuration Information

Current and backup configurations can be exported to external destinations, including FTP server, TFTP server and USB flash disk.

To export system configurations to an FTP server, in the execution mode, use the following command:

export configuration {**startup** | **backup** *number*} **to ftp server** *ip-address* [**vrouter** *vrouter-name*][**user** *user-name* **password** *password*] [*file-name*]

- **startup** | **backup** *number* - Exports the current configurations or the specified backup configurations.
- *ip-address* - Specifies the IP address of FTP server.
- *vrouter-name* - Exports the configuration information of the specified VRouter.
- **user** *user-name* **password** *password* - Specifies the username and password of the FTP server.
- *file-name* - Specifies the name for the file.

To export configurations to a TFTP server, in the execution mode, use the following command:

export configuration {**startup** | **backup** *number*} **to tftp server** *ip-address* [**vrouter** *vrouter-name*] [*file-name*]

To export system configurations to USB flash disk, in the execution mode, use the following command:

export configuration {**startup** | **backup** *number*} **to** {**usb0** | **usb1**} [**vrouter** *vrouter-name*] [*file-name*]

Importing Configuration Information

Configuration files can be imported into the system from the FTP server, TFTP server, or USB flash disk inserted to the device USB port.

To import configurations from an FTP server, in the execution mode, use the following command:

import configuration from ftp server *ip-address* **user** *user-name* **password** *password* [**vrouter** *vrouter-name*] *file-name*

- *ip-address* - Specifies the IP address of FTP server.
- **user** *user-name* **password** *password* - Specifies the username and password of the FTP server.
- *vrouter-name* - Exports configuration information for the specified VRouter.
- *file-name* - Specifies a name for the configuration file.

To import configurations from a TFTP server, in the execution mode, use the following command:

import configuration from tftp server *ip-address* [**vrouter** *vrouter-name*] *file-name*

To import configurations from a USB flash disk, in the execution mode, use the following command:

import configuration from {**usb0** | **usb1**} [**vrouter** *vrouter-name*] *file-name*

Backing up Configuration File Automatically

You can configure the function of back up the configuration file automatically, the device will check the configuration file regularly, when the configuration file chenges, the system will udate the congfiguration files to a FTP server or a TFTP server.

To back up configuration file to a FTP server automatically, in the global configuration mode, use the following command：

configuration auto-backup ftp *ip-address* [**user** *user-name* **password** *password*] [**vrouter** *vrouter-name*] **path** *path* [**interval** *time-value*]

- *ip-address* - Specifies the IP address of FTP server.
- **user** *user-name* **password** *password* – Specifies the user name and password accessing FTP server.
- **vrouter** *vrouter-name* – Specifies the VRouter name.
- *path* – Specifies the path of transferring the configuration files.
- **interval** *time-value* – Specifies the update interval. The value range is 1 to 7*24 hours. The default value is 1 hour.If this parameter is not specified, the system will check the configuration file hourly, and back up the changed configuration files to FTP server when configurations are changed.

In the global configuration mode, use **no configuration auto-backup ftp** command to cancel the settings of backing up configuration file to a FTP server automatically.

To back up configuration file to a TFTP server automatically, in the global configuration mode, use the following command:

configuration auto-backup tftp *ip-address* [**vrouter** *vrouter-name*] **path** *path* [**interval** *time-value*]

In the global configuration mode, use **no configuration auto-backup tftp** command to cancel the settings of backing up configuration file to a TFTP server automatically.

Viewing backing up configuration file automatically Information

To view backing up configuration file automatically Information, in any mode, use the following command:

show configuration auto-backup

Restoring Factory Defaults

You can either press the CLR button on the device or use the command in this section to reset the device and restore factory defaults.

To reset the device using CLI, in any mode, use the following command:

unset all

Note: Use this command with caution. It clears all configurations on the device.

Deleting Configuration Information of Expansion Slots

For some models (SG-6000-X6150, SG-6000-X6180, and SG-6000-X7180) that are running, you might have the requirements of changing/removing the expansion modules.

For the IOM modules, the configuration information of the expansion slots is complex. Before executing the hot-swappable action, you must use the **exec unset slot** *{number}* command to check and delete the configuration information of the expansion slots and initiate the modules.

To delete the configuration information of the expansion slots, use the following command:

exec unset slot *slot-number*

- *slot-number* – Specifies the slot number where the IOM locates. The range is 1 to 128.

After executing this command, the system will display different prompts according to the different situations. You can perform the operations accordingly.

Notes:

- When the expansion slots are related to the interface configurations, you must first delete the interface configurations that related to the expansion slots and then execute the above command to delete the configuration information of the expansion slots.
- When executing the hot-swappable action for the SCM, SSM and QSM, you do not need to execute the above command.

Interface Working Modes

For the interface modules of IOM-2Q8SFP+, IOM-8SFP+, and IOC-8SFP+, partial Hillstone devices can switch the working modes of the interface. The interface working modes support 40G, 10G, and 1G. Switching the working modes can realize the following functions:

- Divide the 40G interface up into four 10G interfaces and realize the connection between the 40G interface and the 10G interface.
- Make the 10G interface work in the working mode of 1G interface and realize the connection between the 10G interface and the 1G interface.

The default working mode of 40G interface is 40G. In the interface configuration mode, use the following command to switch the working mode to 10G:

```
channel-speed 10000
```

The default working mode of 10G interface is 10G. In the interface configuration mode, use the following command to switch the working mode to 1G:

```
channel-speed 1000
```

In the interface configuration mode, use the **`no channel-speed`** command to restore the working mode to the default one.

Notes:

- Before specifying the interface working mode, you need to delete the corresponding configurations of the interface.
- The interface working mode of the IOC-8SFP+ interface module supports 10G and 1G, and you can switch between 10G interface working mode and 1G interface working mode.

Viewing the Configuration of Current Object

After the configuration of the specific object is completed, in the current configuration mode, you can use the command **`show this`** to view the configuration of current object.

The table below shows the object names and its configuration mode that system supported to view.

Object Name	Configuration Mode	Configuration Mode Prompt
Admin	Administrator configuration mode	`hostname(config-admin)#`
AAA server	AAA service configuration mode	`hostname(config-aaa-server)#`
Interface	Interface configuration mode	`hostname(config-if-eth0/0)#`
Zone	Zone configuration mode	`hostname(config-zone-trust)#`
Address	Address configuration mode	`hostname(config-addr)#`
Service	Service configuration mode	`hostname(config-service)#`
Service group	Service group configuration mode	`hostname(config-svc-group)#`
Policy-based Route	PBR configuration mode	`hostname(config-pbr)#`
VRouter	VRouter configuration mode	`hostname(config-vrouter)#`
Configure NAT rules for the default VR trust-vr	NAT configuration mode	`hostname(config-nat)#`

Viewing the Information of Optical Module

To view the information of optical module, including power, temperature and voltage, and module type. In any in any mode, use the following commands:

`show transceiver` *`[interface-name]`*

- *`interface-name`* – Specifies the interface name of optical module.

Configuring Banner

Banner used to display the statement after logining the system, the user can customize the Banner information content. To edit the Banner, in the global configuration mode, use the following command:

`admin login-banner` *`Banner-content`*

- *`Banner-content`* - Specifies the Banner content. The length varies from 1 characters to 4096 characters. After executing this command, the system will

create the Banner of specified content. If the Banner already exists, it will modify the Banner for the specified content.

In the global configuration mode, use **no admin login-banner** command to delete the Banner.

Note:

- In the edit Banner content, if you need to wrap, enter "\n", if you need a space, enter the double quotes "".
- Support for displaying Banner when login to the device over SSH, Telnet, or Console port.

System Maintenance and Debugging

Testing tools, the commands `Ping` and `Traceroute`, are used to test network availability and diagnose system errors. Hillstone device also provides debugging feature for users to check and analyze the system.

Ping

Ping is used mainly for testing network connection and host accessibility.

To check network availability, in any mode, use the following command:

ping [**ipv6**] {*ip-address* | *hostname*} [**count** *number*] [**size** *number*] [**source** *ip-address*] [**timeout** *time*] [**vrouter** *vr-name*]

- *ip-address* | *hostname* - Specifies the IP address or hostname of the destination. When using the dual-stack firmware, you can specify the IPv6 address.
- **count** *number* - Specifies the number of Ping packets. The value range is 1 to 65535. By default, packet number is not limited.
- **size** *number* – Specifies the size of ping packet. The value range is 28 to 65500 bytes.
- **source** *ip-address* - Specifies the source interface name of ping packets.
- **timeout** *time* - Specifies the timeout value for the ping packets. The range is 0 to 3600 seconds. The default number is 0, which means no timeout.
- **vrouter** *vr-name* - Specifies the VRouter of the interface sending ping packets. The default value is trust-vr.

The output of ping command includes the response status for each Ping packet and the final statistics:

- The response status for each Ping packet. If there is no response, the output is "Destination Host Not Responding"; otherwise, the output is the packet sequence, TTL and responding time of the response packet. If the Ping packet

does not reach the destination route or the interface that sends the Ping packet changes, the output is "Network is unreachable". If the destination address of the Ping packet cannot be resolved, the output is "unknown host *hostname*".

- Final statistics. The final statistics includes sent packet number, received packet number, lost packet percentage and time.

Here is a ping command example:

```
hostname(config)# ping 10.200.3.1
Sending ICMP packets to 10.200.3.1
   Seq     ttl     time(ms)
   1       128     2.53
   2       128     1.48
   3       128     1.48
   4       128     1.47
   5       128     1.46
statistics:
5 packets sent, 5 received, 0% packet loss, time 4006ms
rtt min/avg/max/mdev = 1.464/1.689/2.536/0.423 ms
```

WebUI:

1. Select **System** > **System Tools** from the menu bar.
2. In the System Tools dialog, type an IP address into the **Ping** box.
3. Click **Test**, and the testing result will be displayed in the list below.

Traceroute

Traceroute is used to test and record gateways of packets from source host to the destination. It is mainly used to check whether the destination is reachable, and analyze the fault gateway in the network. The common Traceroute function is performed as follows: first, send a packet with TTL 1, so the first hop sends back an ICMP error message to indicate that this packet cannot be sent (because of the TTL timeout); then this packet is re-sent, with TTL 2, TTL timeout is sent back again; repeat this process till the packet reaches the destination. In this way, each ICMP TTL timeout source address is recorded. As result, the path from the originating host to the destination is identified.

To trace the gateways the command **traceroute** has traversed, in any mode, use the following command:

traceroute {*ip-address* | *hostname*} [**numberic**] [**port** *port-number*] [**probe** *probe-number*] [**timeout** *time*] [**ttl** [*min-ttl*] [*max-ttl*]] [**source** *interface*] [**use-icmp**] [**vrouter** *vr-name*]

- *ip-address* | *hostname* - Specifies the destination IP address or host name of traceroute.
- **numberic** - Specifies to display the address in numeric format without resolution.

- **port** *port-number* - Specifies the UDP port number. The value range is 1 to 65535. The default value is 33434.
- **probe** *probe-number* - Specifies the number of probe packet in each hop. The range is 1 to 65535. The default value is 3.
- **timeout** *time* - Specifies the timeout value of next probe packet. The range is 1 to 3600 seconds. The default value is 5.
- **ttl** [*min-ttl*] [*max-ttl*] - *min-ttl* is the minimum TTL value, with range from 1 to 255 and default value being 1. *max-ttl* is the maximum TTL value, with range from 1 to 255 and default value being 30. Specifying TTL is used to display the echo from the *min-ttl* hop to the *max-ttl* hop.
- **source** *interface* - Specifies the the name of the interface sending traceroute probe packets.
- **use-icmp** - Uses ICMP packets to probe. If this parameter is not defined, the system uses UDP packets to probe.
- **vrouter** *vr-name* - Specifies the VRouter of the egress interface of traceroute probe packets. The default value is the default VRouter (trust-vr).

Here is an example of applying command **traceroute** in network analysis:

```
hostname(config)# traceroute 210.74.176.150
traceroute to 210.74.176.150 (210.74.176.150), 30 hops max, 52
byte packets
 1  10.200.3.1 (10.200.3.1)  0.572 ms  0.541 ms  0.359 ms
 2  192.168.3.1 (192.168.3.1)  0.601 ms  0.754 ms  0.522 ms
 3  202.106.149.177 (202.106.149.177)  1.169 ms  1.723 ms  1.104
ms
 4  61.148.16.133 (61.148.16.133)  2.272 ms  1.940 ms  2.370 ms
 5  61.148.4.17 (61.148.4.17)  2.770 ms 61.148.4.101
(61.148.4.101)  6.030 ms 61.148.4.21 (61.148.4.21)  2.584 ms
 6  202.106.227.45 (202.106.227.45)  4.893 ms  5.010 ms  3.917
ms
 7  202.106.193.70 (202.106.193.70)  5.407 ms 202.106.193.126
(202.106.193.126)  4.247 ms 202.106.193.70 (202.106.193.70)
6.954 ms
 8  61.148.143.30 (61.148.143.30)  3.459 ms  3.758 ms  2.853 ms
 9  * * *
10  * * *
```

This example shows which gateways the packets have traversed during the process from source host to destination host and fault gateways.

WebUI: To test and record gateways the packet has traversed by Traceroute, take the following steps:

1. Select **System** > **System Tools** from the menu bar.

2. In the System Tools dialog, type an IP address into the **Traceroute** box.
3. Click **Test**, and the testing result will be displayed in the list below.

System Debugging

System debugging helps you to diagnose and identify system errors. Basically, all the protocols and functions can be debugged. By default, debugging of all functions is disabled. The debugging function can only be configured through CLI.

To enable system debugging, in any mode, use the following command:

debug {**all** | *function-name*}

- **all** - Enables all debugging functions.
- *function-name* - Enables the specified protocol or feature debugging.

To disable all or one debugging function, in any mode, use the following command:

undebug {**all** | *function-name*}

You can disable debugging by pressing ESC key. As some debugging information has been cached, the closing process may take several minutes.

To see the status of the debugging function, in any mode, use the following command:

show debug

Note: If you want to view debugging information on your terminal, enable debug logging function (execute the command **logging debug on**).

Collecting and Saving Tech-support Information to File

In order to locate the system fault, you should collect the displayed information of all the **show** commands and save as tech-support file. To collect and save the tech-support information to file, in any mode, use the following command:

show tech-support [cpu *cpu-number* | **all]**

- *cpu-number* – Collects and saves the tech-support information of specified CPU to file. You can configure this parameter only in system with multiple CPUs.
- **all** –Collects and saves all the tech-support information to file. You can configure this parameter only in system with multiple CPUs.

Note: You can collect and save all the tech-support information to file through command **show tech-support** in system with single CPU.

Viewing the Tech-support Information

To view the tech-support information through Console port, in any mode, use the following command:

show tech-support [cpu *cpu-number* | **all] toconsole**

- *cpu-number* – Displays the tech-support information of specified CPU to Console port. You can configure this parameter only in system with multiple CPUs.
- **all** –Displays all the tech-support information to Console port. You can configure this parameter only in system with multiple CPUs.

Note: You can view all the tech-support information though Console port by command **show tech-support toconsole** in system with single CPU.

Collecting the Tech-support Information Automatically

To collect the Tech-support Information Automatically, in any mode, use the following command:

show tech-support-auto interval *interval-time* **count** *count-time*

- *interval-time* – Specifies the interval time to collect the tech-support information automatically. The range is 10 to 1440. The unit is minute.
- *count-time* –Specifies the times to collect the tech-support information automatically. The range is 1 to 10.

Note:

- System can save 10 tech-support files at most. When the number of file exceeds 10, the new file will cover the older file.
- When system executes this command, if you configure another command to collect the tech-support information automatically, the new configuration will cover the previous configuration.

Viewing the Information of Nvramlog or Watchdoglog File

To view the log information of nvramlog or watchdoglog in tech-support file, in any mode, use the following command:

show tech-support *log-name*

- *log-name* –Specifies the name of log information which is required to be displayed. You can specify the name as vramlog or watchdoglog.

Deleting the Function of Automatically Collecting Tech-support Information

To delete the function of automatically collecting tech-support information, in any mode, use the following command:

```
show tech-support-auto clear
```

Rebooting the System

Turning off the device and powering it on again can reboot it. In addition, you can also use command line or WebUI to restart the system.

To reboot the device, in the configuration mode, use the following command:

```
hostname# reboot
System configuration has been modified. Save? [y]/n
```
(type **y** or press Enter to save the settings; type **n** to give up changes.)
```
Building configuration.
Saving configuration is finished
System reboot, are you sure? y/[n]
```
(type **y** to reboot the system; type **n** or press Enter to go back to the configuration mode.)

Save the current settings before rebooting the device if you don't want to lose unsaved configurations. Be careful when you execute this command, because network disconnection occurs during the rebooting process.

WebUI: Select **Tools** > **Reboot** from the menu bar.

Upgrading StoneOS

This section introduces StoneOS starting-up system and describes how to upgrade StoneOS.

Starting Process

The start-up system consists of three parts, which are Bootloader, Sysloader and StoneOS. There functions are listed below:

- Bootloader - The first started program when the device is powered on. Bootloader loads StoneOS or Sysloader and makes them start.
- Sysloader - The program that upgrades StoneOS.
- StoneOS - The operating system running on the device.

When a device is powered on, the Bootloader tries to start StoneOS or Sysloader. The Sysloader is used to select existing StoneOS in the system and upgrade StoneOS via FTP, TFTP or USB port. The upgrade of Sysloader is performed by the Bootloader via TFTP.

Bootloader

The Bootloader has two working modes: automatic mode and interactive mode.

In the automatic mode, Bootloader starts the existing StoneOS first. If no StoneOS exists or only illegal ones present, the system stops and you must upgrade StoneOS in Sysloader.

To enter the interactive mode, press ESC during the starting process according to the prompt. In the interactive mode, you can select a Sysloader stored in the flash to start, or download a new version of Sysloader from the TFTP server and then start it.

StoneOS Quick Upgrading (TFTP)

The Sysloader downloads StoneOS from TFTP server, ensuring a fast system upgrading from network.

To upgrade StoneOS, take the following steps:

1. Power on the device and enter Sysloader:

```
HILLSTONE NETWORKS
Hillstone Bootloader 1.3.2 Aug 14 2008-19:09:37

DRAM:  2048 MB
BOOTROM: 512 KB

Press ESC to stop autoboot: 4 (Press ESC during the 5-second countdown.)

Run on-board sysloader? [y]/n: y (Type y or press Enter)
Loading: ##########################
```

2. Select **Load firmware via TFTP** from the menu:

```
Sysloader 1.2.13 Aug 14 2008 - 16:53:42

1       Load firmware via TFTP
2       Load firmware via FTP
3       Load firmware from USB disks (not available)
4       Select backup firmware as active
5       Show on-board firmware
6       Reset

Please select: 1 (Type 1 and press Enter)
```

3. Specify Sysloader IP, TFTP server IP, gateway IP, and the name of StoneOS:

```
Local ip address     [     ]: 10.2.2.10/16 (Type the IP address of Sysloader and press Enter.)
Server ip address    [     ]: 10.2.2.3 (Type the IP address of TFTP server and press Enter.)
Gateway ip address   [     ]: 10.2.2.1 (If Sysloader and TFTP server are not in the same network segment, you need to provide the gateway IP address and press Enter; otherwise, just press Enter.)
File name  : StoneOS-3.5R2 (Type the name of StoneOS and press Enter, and then the system begins to transfer the file.)
#################################################################
```

```
##################################################################
############
```

4. Save StoneOS. Take the following steps:

```
File total length 10482508
Checking the image...
Verified OK

Save this image? [y]/n: y (Type y or press Enter to save the transferred StoneOS.)
Saving.....................................

Set StoneOS-3.5R2 as active boot image
```

5. Reboot the device.

```
Sysloader 1.2.13 Aug 14 2008 - 16:53:42

1       Load firmware via TFTP
2       Load firmware via FTP
3       Load firmware from USB disks (not available)
4       Select backup firmware as active
5       Show on-board firmware
6       Reset

Please select: 6 (Type 6 and press Enter. The system reboots.)
```

The device can save only two versions of StoneOS. If you want to save a new one, delete an existing one according to the prompt.

Other Upgrading Methods

Though downloading StoneOS from TFTP server is often used to upgrade the system, the device also supports upgrading from FTP server and USB flash disk.

Upgrading StoneOS via FTP

To download StoneOS from FTP server and upgrade it, in the Sysloader program, take following steps:

1. In Sysloader, select **2** and press Enter.
2. Type the Sysloader IP address behind the prompt Local `ip address [ ]:` and press Enter.
3. Type the FTP server IP address behind the prompt `Server ip address [ ]:` and press Enter.
4. If the Sysloader and FTP server are not in the same network segment, type the gateway IP address of Sysloader behind the prompt `Gateway ip address [ ]:` and press Enter.
5. Type FTP user name behind the prompt `User Name [anonymous ]:` and press Enter.
6. Type the password of that user behind `Password :` and press Enter.

7. Type the file name of StoneOS behind the prompt `File name :` and press Enter. The system starts to download the specified StoneOS.
8. When the downloading is complete, type **y** to save this version of StoneOS into the device flash.
9. After the new StoneOS is saved, the system shows Sysloader menu and you can type **6** and press Enter to start the system with the new StoneOS.

Note: If an FTP server allows anonymous login, just press Enter when it requires a username and password.

Upgrading StoneOS via USB

To upgrade StoneOS to a version saved in the USB flash disk, take the following steps:

1. Copy the StoneOS you want to use in your USB flash disk.
2. Plug the USB flash disk into the device USB port.
3. Enter Sysloader, select **3** in its menu, and press Enter.
4. Select the StoneOS you want and type **y**. The system starts to upload the StoneOS.
5. When it's complete, type **y** if you want to save the StoneOS into the device flash.
6. In the Sysloader menu, select **6** and press Enter. The system starts with the new StoneOS.

Introduction to Sysloader Menu

This section introduces the function of each Sysloader menu item. Type the number of the operation you want, and press Enter, then follow instructions to continue.

Table 5: Sysloader Menu Options

Option	Description
1. Load firmware via TFTP	Upgrades StoneOS by downloading an OS file from a TFTP server.
2. Load firmware via FTP	Upgrades StoneOS by downloading an OS file from an FTP server.
3. Load firmware from USB disks	Upgrades StoneOS by fetching an OS file from an USB disk on the device.
4. Select backup firmware as active	Switches the saved backup StoneOS to be the active StoneOS used when the system rebooting.
5. Show on-board firmware	Shows all saved StoneOS with their status.
6. Reset	Reboot the system.

Upgrading StoneOS Using CLI

Besides Sysloader, you can upgrade StoneOS by typing command lines.

To upgrade StoneOS via FTP, in the configuration mode, use the following commands:

import image from ftp server *ip-address* [**user** *user-name* [**password** *password*]] [**vrouter** *vrouter-name*] *file-name*

- *ip-address* - Specifies the IP address of FTP server.
- **user** *user-name* **password** *password* - Specifies username and password of FTP server.
- *vrouter-name* - Updates StoneOS by using the specified VRouter.
- *file-name* - Specifies the name of StoneOS you want to use.

To upgrade StoneOS via TFTP, in the configuration mode, use the following command:

import image from tftp server *ip-address* [**vrouter** *vrouter-name*] *file-name*

To upgrade StoneOS via USB, in the configuration mode, use the following commands:

import image from {**usb0** | **usb1**} [**vrouter** *vrouter-name*] *file-name*

Reboot the device to make the new StoneOS take effect.

Upgrading StoneOS Using WebUI

In the WebUI, take the following steps to upgrade StoneOS:

1. Select **System** > **Firmware Management** from the menu bar.
2. In the Upgrade Wizard dialog, click **Upgrade to a new version**, and then click **Next**.
3. From the **Select backup version** drop-down list, select a StoneOS version as the backup version.
4. Click **Browse** after the Upload a new version box, navigate to the file location, select the file, and then click **Open**.
5. Click **Next**, and then select whether to reboot the system. The system must be rebooted to make the configurations take effect.
6. Click **OK** to save your settings.

Backing up and Restoring Data

This feature may not be available on all platforms. Please check your system's actual page to see if your device delivers this feature.

When upgrading firmware to the latest versions, you may fail to upgrade successfully, which made system data lost. StoneOS support to backup and restore data. You can backup data to FTP server you specified when upgrading; and if upgrading failed, you can restore data from the FTP server.

In executive mode, type the following mode to backup data to the specified FTP server:

export db-data to ftp server *ip-address* [**vrouter** *VR-name*]{**user** *username* **password** *password filename* | *filename*}

- *ip-address* – Specifies FTP server IP address.
- **vrouter** *VR-name* – Backup files through the VR.
- **user** *username* **password** *password* – Specifies the username and password of the FTP server.
- *filename* – Specifies the file name you want to export. If not specified, system will export files with the name of its version.

In executive mode, type the following mode to restore data from the specified FTP server:

import db-data from ftp server *ip-address* [**vrouter** *VR-name*][**user** *username* **password** *password*]*filename*

- *ip-address* – Specifies FTP server IP address.
- **vrouter** *VR-name* – Restore files through the VR.
- **user** *username* **password** *password* – Specifies the username and password of the FTP server.
- *filename* – Specifies the file name you want to import.

Graceful Shutdown

Some of the modularized Hillstone platforms (SG-6000-X6150, SG-6000-X6180, SG-6000-X7180) support graceful-shutdown on a single hardware module. Graceful shutdown will not interrupt any service running on the module, thus assuring uninterrupted operation of the whole system. At the time of writing only SSM and QSM support this function.

You need to stop the module from receiving new traffic in order to execute graceful shutdown. After all the services have been processed, the status of the module will change to offline automatically (you can view the status by command **show module**). At this point graceful shutdown is completed. To reboot the module, use the command **reboot slot** {*number*}.

To shutdown the specified module gracefully, in any mode, use the following command:

exec system graceful-shutdown slot {*number*}

- *number* - Specifies the slot number for SSM/QSM. The value range is 1 to 10.

After executing the command, the system provides different prompts as listed below, specifically depending on your running environment. Determine your next operation as prompt.

- Only one SSM is available, the operation is not supported .
- The module is not SSM or QSM. Can't do the operation.
- Graceful-shutdown slot number is started. Don't do any operation before it is finished. It will take about a minute. You can use **`show system graceful-shutdown status`** to get status.

To reboot the specified module, use the command **`reboot slot`** {*number*}.

Tip: Graceful shutdown commands are also applicable to hot swap of SSM or QSM. Before hot swap, use the command to shut down the module, and then plug it.

SCM HA

Some Hillstone devices (SG-6000-X6150, SG-6000-X6180, and SG-6000-X7180) support SCM HA. When a device is installed with two SCMs, the SCM that is plugged into slot SC0 is used as the master module, and working in the Master mode; the SCM that is plugged into slot SC1 is used as the backup module, and working in the Slave mode. If a device is installed with only one SCM, the SCM is used as the master module, and the newly installed SCM (if any) is used as the backup module. In such a case the master and backup modules are not determined by the slot positions. If the master SCM fails, the backup SCM will be promoted to the master module automatically to assure continuous business operation.

When using SCM HA, keep in mind that:

- Never configure any option on the backup SCM.
- After master-backup switching, the new backup SCM still works in the Slave mode after rebooting, and will not preempt the master SCM.
- After master-backup switching, you need to re-establish the management connection, such as Telnet or HTTP connection.
- To assure proper synchronization of license information, the system might prompt to reboot the system (with network disconnection) or perform ISSU (without network disconnection). Continue your operation as prompted.

To view the SCM HA status, use the command **`show module`**. In the output the module that is labeled with M (e.g., Master) is the master SCM, and the module that is labeled with B (e.g., Backup) is the backup SCM.

License Management

License used to authorize users features, services or extending the performance. If you do not buy and install the corresponding License, the features, services and performances which is based on License will not be used, or can not achieve the higher performance.

License classes and rules.

Table 6: Sysloader Menu Options

Platform License	Description	Valid Time
Platform Trial	Platform license is the basis of the other licenses operation. If the platform license is invalid, the other licenses are not effectve. The device have been preinstalled platform trial license for 15 days in the factory.	You cannot modify the existing configuration when License expired. System will restore to factory defaults when the device reboot.
Platform Base	You can install the platform base license after the device formal sale. The license provide basic firewall and VPN function.	System cannot upgrade the OS version when License expired. But system could work normally.
Function License	**Description**	**Valid Time**
VSYS	Authorizing the available number of VSYS.	Permanent
SSL VPN	Authorizing the maximum number of SSL VPN access. Through installing multiple SSL VPN licenses, you can add the maximum number of SSL VPN access.	Permanent
QoS/iQoS	Enable QoS function.	System cannot upgrade the QoS/iQoS function and cannot provide the maintenance service when License expired.
WAP Traffic Distribution	Providing WAP traffic distribution.	Permanent
Sandbox License	Providing sandbox function and white list update, authorizing the number of suspicious files uploaded per day. Including 3 licenses: • Sandbox-300 license: 300 suspicious files are allowed to upload every day. • Sandbox-500 license: 500 suspicious files are allowed to upload every day. • Sandbox-1000 license: 1000 suspicious files are allowed to upload every day.	The valid time including 1 year, 2 years and 3 years. System cannot provide to analyze the collected data and cannot update the white list when License expired. Only can using the sandbox protection function according to the local database cache results. If you restart the device, the function cannot be used.
Service License	**Description**	**Valid Time**
AntiVirus	Providing antivirus function and antivirus signature database update.	System cannot update the antivirus signature database when License expired. But antivirus function could be used normally.

URL	Providing URL database and URL signature database update.	System cannot provide to search URL database online function when License expired. But user-defined URL and URL filtering function could be used normally.
IPS	Providing IPS function and IPS signature database update.	System cannot update the IPS signature database when License expired. But IPS function could be used normally.
APP signature	APP signature license is issued with platform license, you do not need to apply alone. The valid time of license is same as platform license.	System cannot update the APP signature database when License expires. But the functions included and rules could be used normally.
Threat Prevention	A package of features, including AntiVirus, IPS and corresponding signature database update.	System cannot update all signature databases when license expires. But the functions included and rules could be used normally.
PTF	Providing Perimeter Traffic Filtering function of predefined black list and IP reputation database update.	System cannot update IP reputation database when license expires.
StoneShield	A package of features, including Abnormal Behavior Detection, Advanced Threat Detection, and corresponding signature database update.	System cannot update all signature databases when license expires. But the functions included and rules could be used normally.
Expansion and Enhancement License	**Description**	**Valid Time**
AEL	Advance the maximum value of concurrent sessions and performance.	Permanent

Applying for a License

To apply for a license, take the following steps:

1. Generate a request.

   WebUI: Select **System** > **License** from the menu bar. Under License request, type the customer's information, and click **Generate**.

   CLI: Use the command **`exec license apply applicant`** *`string`* to generate a license application request. For more information, see Generating a Request for License.

2. Send the request to the Hillstone agent.

Installing a License

A license contains a string of characters. When you get the license, take the following steps to install it in the device:

1. Select **System** > **License** from the menu bar.
2. Under License installation in the License dialog, configure options as below:
   - Upload file: Click **Browse** and select the license file in your local PC.
   - Manual input: Type the license string into the box.
3. Click **OK** to save your settings.

If you use CLI to install a license, in any mode, use the command **`exec license install`** *`license-string`*. For more information, see Generating a Request for License. After installing, you need to reboot system to make the license effective.

Note: Although license can be removed, you are strongly suggested not to uninstall any license.

Connecting to License server

For Hillstone CloudEdge virtual firewall, after installing the license, you need to connect to the license server to verify the validity of the license to prevent the license from being cloned. System supports two ways, one is connecting the firewall to the public network license server via Internet to verify, the other is connecting the firewall to the internal network vLMS (virtual License Management System) via LAN to verify.You can choose one of the two ways according to the need.

- The way that used to verify validity via public network license server is applicable in some small private clouds or industry cloud scenarios. After the virtual firewall being connected to the public server, the server will verify validity of the license, (currently the public network server does not support the distribution and management of the license). If the cloned license is found or the virtual firewall is not connected to server to verify, the virtual firewall will be restarted in 7 days.
- The way that used to verify validity via LAN vLMS is applicable in the large-scale public cloud scenarios. After the virtual firewall being connected to the vLMS, the vLMS not only verifies the validation of license, but also support automatic distribution and management of license. If the cloned license is found, the server will recycle all virtual firewall licenses of either the clone or the cloned one and restart the virtual firewall; if the virtual firewall does not connect to the server to verify, it will restart in 7 days.

If you use CLI to connect to the license server, in any mode, use the command **`exec connect { public-server | license-server`** *`A.B.C.D`* **`ssl-port`** *`port-number`*`}`. For more information, see Connecting to License server. After connecting, you need to reboot system to make the license effective.

Note: For more information about vLMS, refer to 《vLMS-Virtual License

Managing a License Using CLI

This section describes how to apply, install and uninstall a license using command lines.

Generating a Request for License

To generate a request for license, in any mode, use the following command:

exec license apply applicant *string*

- *string* - Specifies the name of the applicant.

Installing/Uninstalling a License

After obtaining the license, to install it, in any mode, use the following command:

exec license install *license-string*

- *license-string* - Pastes the license string.

To uninstall a license, in any mode, use the following command:

exec license uninstall *license-name*

- *license-name* - Specifies the name of the license you want to uninstall.

Type **reboot** to reboot system to make the license effective.

Connecting to License server

For Hillstone CloudEdge virtual firewall, after installing the license, you need to connect to the license server to verify the validity of the license, in any mode, use the following command :

exec connect { public-server | license-server *A.B.C.D* **ssl-port** *port-number***}**

- **public-server** – Specifies the license server as a public server.
- **license-server** *A.B.C.D* – Specifies the license server as LAN vLMS and specifies its IP address.
- **ssl-port** *port-number* – Specifies the port number of connection to the LAN vLMS.The value ranges from 1 to 65535.

After connecting, you need to reboot system to make the license effective.

Note: When you verify your license through a public server, make sure that the interface connected to the public server is in the trust-vr zone and that you can access the Internet through the trust-vr zone.

View License Server Information

To view license server information, in any mode, use the following command:

```
show connected license-server
```

Batch Installing Licenses

When installing licenses to a large amount of devices, using this batch method will simplify the process and minimize the mistakes.

Batch Installing Procedure

To install licenses in batch, take the following steps:

1. If you require many licenses, you need provide the device serial numbers and license types information to Hillstone. For information about license, consult the local agent.
2. Hillstone generates license files according to your requests and send them to you in proper ways, like email.
3. When you receive the license files, copy them to a FAT32 USB disk under the directory named "\license" (the name must be in lower case). The license files cannot be changed; otherwise they are unable to be installed.
4. Install the licenses to all the devices in the USB disk. See the section below.

Installing a License

After copying the license files to the proper directory in the USB disk, insert the USB disk into the USB port of the device, the device automatically scans the USB disk and install the matched license. You can view the status by checking the LED lights.

1. Power on the device, wait until it shows login prompt.
2. Insert the USB disk into the USB port.
3. The device automatically scans the USB disk, searches for a license with the same serial number of the device, and installs it. The ALM light shows the installation status, as shown in the table below:

Table 7: **ALM Description for Installation Status**

Status	ALM Indicator
Searching for a matched license from the directory "license" in USB disk.	Blinking green until installation completes
The installation is completed.	Restore to former status
No matched license is found.	Blinking red for 10 seconds and then restore to the former status.
No "license" directory is found.	No change.

4. Remove the USB disk from the device and you can install licenses to other devices using the same method.

All matched licenses can be installed into the devices. To avoid reinstallation, used licenses are removed from the "license" directory to a "license_installed" directory (automatically created).

Reboot system to make license effective.

Simple Network Management Protocol (SNMP)

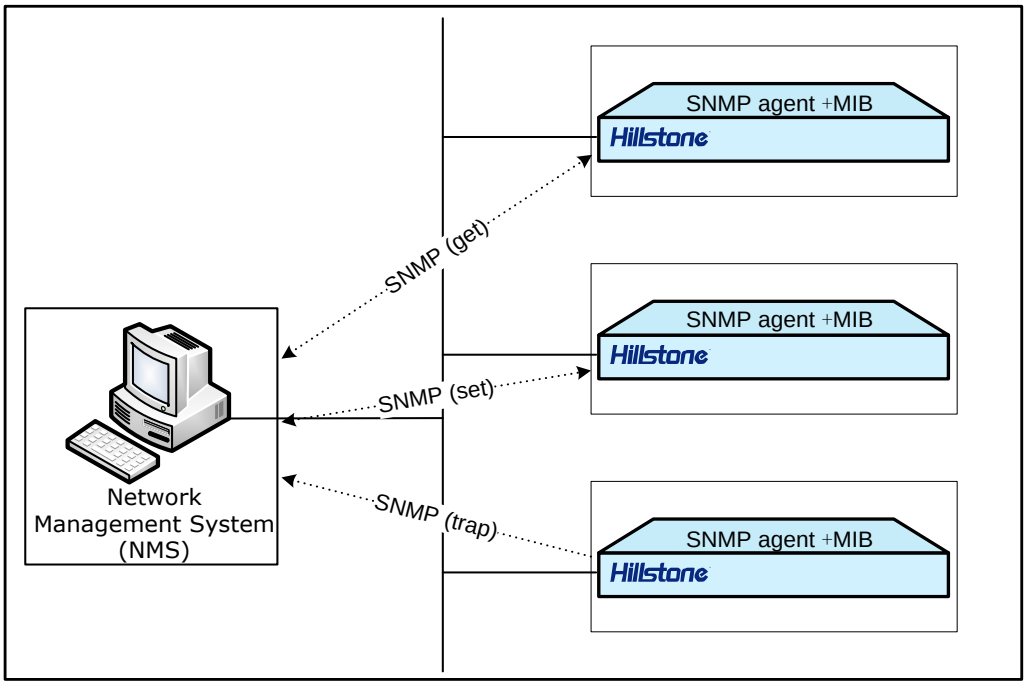
Simple Network Management Protocol (SNMP) is an application layer protocol for managing devices on IP networks. It consists of four key components: Network Management System (NMS), Network Management Protocol, SNMP agent and Management Information Base (MIB).

- Network Management System (NMS): A software system which uses the network managers (like adventnet, solarwinds) to send requests, such as Get and Set, and receives the responses from the SNMP agent so that it can manage and monitor network devices.
- SNMP Agent: A software module on a managed network device, which sends the local device information to NMS.
- Network Management Protocol: It is used to exchange SNMP packets between NMS and SNMP agent. It supports three basic functions, which are GET, SET and Trap. Get is used by NMS to fetch the MIB value from the SNMP agent; Set is used by NMS to configure the MIB value of the SNMP agent; Trap is used by the SNMP agent to sent event notifications to NMS.
- Management Information Base (MIB): An information database maintained by SNMP Agent, which contains specific characteristics of managed network devices, comprises object variables. The object variables can be requested or set by NMS.

Hillstone SNMP

Hillstone devices support SNMP agent function, which receives requests from and responds the device information to NMS. Figure below illustrates how a NMS interacts with a security device via SNMP.

Figure 2: **SNMP implementation on Hillstone next-generation fireware**



Supported RFCs

Hillstone security device supports the following SNMP versions:

- SNMPv1: Simple Network Management Protocol. See RFC-1157.
- SNMPv2: See the following RFCs:
  - RFC-1901 - Introduction to Community-based SNMPv2;
  - RFC-1905 - Protocol Operations for Version 2 of the Simple Network Management Protocol;
  - RFC-1906 - Transport Mappings for Version 2 of the Simple Network Management Protocol.
- SNMPv3: See the following RFCs:
  - RFC-2263 - SNMPv3 Applications;
  - RFC-2264 - User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3);
  - RFC-2265 - View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP).

SNMPv1 protocol and SNMPv2 protocol use community-based strings to limit the NMS to get device information. SNMPv3 protocol introduces a user-based security module for information security and a view-based access control module for access control.

Supported MIBs

Hillstone device supports all relevant Management Information Base II (MIB II) groups defined in RFC-1213 and the Interfaces Group MIB (IF-MIB) using SMIv2 defined in RFC-2233. Besides, StoneOS offers a private MIB, which contains the system information, IPsec VPN information and statistics information of the device. You can use the private MIB by loading it into a SNMP MIB browser on the management host.

Supported Traps

Trap is an asynchronous notification from SNMP agent to SNMP client. The following traps are supported in StoneOS:

- Warm start
- Authentication Ffailure
- Interface link down/up
- VPN SA negotiation status change
- HA status change
- System status changes, including CPU utilization over 80%, fan status change, memory low, etc.
- Network attacks, including ARP spoofing, IP Spoofing, SYN Flood attack, etc.
- Configuration changes

Configuring SNMP

Hillstone device provides the following SNMP configuration options:

- Enabling/Disabling the SNMP agent function
- Configuring the SNMP port number
- Configuring SNMP engineID
- Creating an SNMPv3 user group
- Creating an SNMPv3 user
- Configure the IP address of the management host
- Configuring the recipient of a SNMP trap
- Configuring sysContact
- Configuring sysLocation
- Specifying the VRouter on which the SNMP is enabled

WebUI: Select **System** > **SNMP** from the menu bar.

Enabling/Disabling the SNMP Agent Function

By default, the SNMP agent function is disabled. To enable the function, in the global configuration mode, use the following command:

snmp-server manager

To disable it, use the command **no snmp-server manager**.

Configuring the SNMP Port Number

To specify the port number of the SNMP agent, in the global configuration mode, use the following command:

snmp-server port *port-number*

- *port-number* - Specifies the port number. The value range is 1 to 65535. The default value is 161.

Configuring SNMP Engine ID

SNMP EngineID is a unique identifier for the SNMP engine. The SNMP engine is the essential component of the SNMP entity (NMS or network devices managed by SNMP). The functions of the SNMP engine are sending/receiving SNMP messages, authenticating, extracting PDU, assembling messages, communicating with SNMP applications, etc.

To configure the SNMP engineID of the local device, in the global configuration mode, use the following command:

snmp-server engineID *string*

- *string* - Specifies the engineID. The length is 1 to 23 characters.

Creating an SNMPv3 User Group

To configure a SNMPv3 user group, in the global configuration mode, use the following command:

snmp-server group *group-name* **v3** {**noauth** | **auth** | **auth-enc**} [**read-view** *readview*] [**write-view** *writeview*]

- *group-name* - Specifies a name for the user group. The value range is 1 to 31 characters.
- **noauth** | **auth** | **auth-enc** - Specifies the security level of the user group. The security level determines the security mechanism used when handling a SNMP packet. **noauth** means no authentication nor encryption; **auth** means it requires MD5 or SHA authentication; **auth-enc** indicates that it uses MD5 or SHA authentication and AES or DES packet encryption.
- **read-view** *readview* - Specifies the read-only MIB view names of the user group. If this parameter is not specified, all MIB views are none.

- **write-view** *writeview* - Specifies the writable MIB view names of the user group. If this parameter is not specified, all MIB views are none.

The system allows up to five user groups, each of which with a maximum of five users.

To delete the specified user group, in the global configuration mode, use the command **no snmp-server group** *group-name*.

Creating an SNMPv3 User

To configure a SNMPv3 user, in the global configuration mode, use the following command:

snmp-server user *user-name* **group** *group-name* **v3 remote** *remote-ip* [**auth-protocol** {**md5** | **sha**} **auth-pass** [**enc-protocol** {**des** | **aes**} **enc-pass**]]

- **user** *user-name* - Specifies a name for the user. The value range is 1 to 31 characters.
- **group** *group-name* - Specifies a configured user group to the user.
- **remote** *remote-ip* - Specifies the IP address of the remote management host.
- **auth-protocol** {**md5** | **sha**} - Specifies that the user should be authenticated with MD5 or SHA algorithm. If this parameter is not specified, no authentication nor encryption is required for the user.
- **auth-pass** - Specifies authentication password. Use 8 to 40 characters.
- **enc-protocol** {**des** | **aes**} - Specifies that the user is encrypted with DES or AES.
- **enc-pass** - Specifies the encryption password. Use 8 to 40 characters.

The system allows up to 25 users. To delete the specified user, in the global configuration mode, use the command **no snmp-server user** *user-name*.

Configuring the IP Address of the Management Host

To configure the management host's address, in the global configuration mode, use the following command:

snmp-server host {*ip-address* | *ip-address/mask* | **range** *start-ip end-ip*} {**version** [*1* | *2c*] **community** *string* [**ro** | **rw**] | **version** *3*}

- *ip-address* | *ip-address/mask* | **range** *start-ip end-ip* – Specifies the IP address or IP range of the management host.
- **version** [**1** | **2c**] - Specifies that SNMP version is SNMPv1 (**1**) or SNMPv2C (**2c**).
- **community** *string* - Community strings are shared password between the managing process and agent process, therefore, an SNMP packet whose community string does not match that of the security device will be dropped.

Specifies the community string (31 characters at most) here and it only works for SNMPv1 and SNMPv2C.

- **ro** | **rw** - Specifies the read and write privileges of community string. The **ro** (read-only) community string can only read MIB; **rw** (read and write) community string can read and change MIB. This is optional. By default, community string has read-only privilege.
- **version 3** - Specifies that the SNMP version is version 3.

To delete the specified management host, in the global configuration mode, use the command **no snmp-server host** {*host-name* | *ip-address* | *ip-address/mask* | **range** *start-ip end-ip*}.

Configuring Recipient of SNMP Trap

To configure the recipient of the SNMP trap packets, in the global configuration mode, use the following command:

snmp-server trap-host *host-ip* {**version** {**1** | **2c**} **community** *string* | **version 3 user** *user-name* **engineID** *string* } [**port** *port-number*]

- *host-ip* - Specifies the IP address of SNMP trap recipient.
- **version** {**1** | **2c**} - Specifies the SNMP version used to send trap packets. It can be SNMPv1 or SNMPv2C.
- **community** *string* - Specifies the community string of SNMPv1 or SNMPv2C
- **version 3** - Specifies to use SNMPv3 to send trap packets.
- **user** *user-name* - Specifies the SNMPv3 user name.
- **engineID** *string* - Specifies the engineID of trap recipient.
- **port** *port-number* - Specifies the recipient host port number. The value range is 1 to 65535.The default value is 162.

To delete the specified trap recipient host, in the global configuration mode, use the command **no snmp-server trap-host** {*host-name* | *ip-address*}.

Configuring sysContact

sysContact specifies the contact name for this managed device (here refers to the security device), as well as information about how to contact this person.

To configure a sysContact, in the global configuration mode, use the following command:

snmp-server contact *string*

- *string* - Specifies the contact string. You can specify up to 255 characters.

To delete the contact, in the global configuration mode, use the command **no snmp-server contact**.

Configuring sysLocation

sysLocation specifies the physical location of this managed device (here refers to the security device).

To configure sysLocation, in the global configuration mode, use the following command:

snmp-server location *string*

- *string* - Specifies the location string. You can specify up to 255 characters.

To delete the sysLocation, in the global configuration mode, use the command **no snmp-server location**.

Specifying the VRouter on Which the SNMP is Enabled

You can specify the VRouter on which the SNMP function is enabled. To specify the VRouter, in the global configuration mode, use the following command:

snmp-server vrouter *vrouter-name*

- *vrouter-name* – Specifies the name of the VRouter.

To disable the SNMP function in the VRouter, in the global configuration mode, use **no snmp-server vrouter** command.

Viewing SNMP Information

To view SNMP configurations, in any mode, use the following commands:

- Show SNMP configurations: **show snmp-server**
- Show SNMPv2 user groups: **show snmp-group**
- Show SNMPv3 users: **show snmp-user**

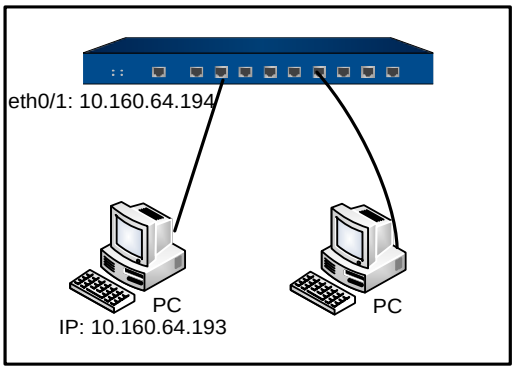
SNMP Configuration Examples

This section provides two SNMP configuration examples.

Requirements

The goal is to connect the NMS (PC with IP address 10.160.64.193) to a security device on interface eth0/1 (IP: 10.160.64.194), as shown below:

Figure 3: SNMP Example Topology



- Example 1: Use NMS (PC of 10.160.64.193) to manage the security device through SNMPv2C with community string "public". In addition, the device is allowed to send trap packets to NMS with community string "private".
- Example 2: Use PC of IP 10.160.64.193 to manage the security device through SNMPv3, with security level of MD5 authentication (password: password1) and DES encryption (password: password2). PC can read MIB-II and only has the right to modify usm MIB. Besides, the security device is allowed to send trap packets.

Example 1

Take the following steps:

1. Configure the security device:

   To enter the global configuration mode:
   ```
   hostname# configure
   ```

   To enable the SNMP service on the interface:
   ```
   hostname(config)# interface ethernet0/1
   hostname(config-if-eth0/1)# manage snmp
   ```

   To enable SNMP of the device:
   ```
   hostname(config)# snmp-server manager
   ```

   To configure community and access privilege:
   ```
   hostname(config)# snmp-server host 10.160.64.193 version 2c
   community public ro
   ```

   To configure sysContact and sysLocation:
   ```
   hostname(config)# snmp-server contact cindy-Tel:218
   hostname(config)# snmp-server location Hostname-Network
   ```

   To allow sending trap packets to NMS 10.160.64.193 with community string "private":
   ```
   hostname(config)# snmp-server trap-host 10.160.64.193 version 2c
   community private
   ```
2. Configure Network Management System (NMS).

Example 2

Take the following steps:

1. Configure the security device:

   To enter the global configuration mode:
   ```
   hostname# configure
   ```

   To enable the SNMP service on the interface:
   ```
   hostname(config)# interface ethernet0/1
   hostname(config-if-eth0/1)# manage snmp
   ```

   To enable SNMP of the device:
   ```
   hostname(config)# snmp-server manager
   ```

   To configure the local engineID:
   ```
   hostname(config)# snmp-server engineID hillstone
   ```

   To specify that the NMS can only read MIB-II but has write privilege over usm MIB:
   ```
   hostname(config)# snmp-server group group1 v3 auth-enc read-view mib2 write-view usm
   ```

   To specify user with MD5 authentication and DES encryption:
   ```
   hostname(config)# snmp-server user user1 group group1 v3 remote 10.160.64.193 auth md5 password1 enc des password2
   ```

   To configure address of NMS:
   ```
   hostname(config)# snmp-server host 10.160.64.193 version 3
   ```

   To configure trap recipient host so that it can send trap packets to NMS:
   ```
   hostname(config)# snmp-server trap-host 10.160.64.193 version 3 user user1 engineID remote-engineid
   ```

   To configure sysContact and sysLocation:
   ```
   hostname(config)# snmp-server contact cindy-Tel:218
   hostname(config)# snmp-server location Hostname-Network
   ```

2. Configure Network Management System (NMS).

HSM Agent

Hillstone Security Management (HSM) is a centralized management platform to manage and control multiple Hillstone devices. HSM system consists of three modules: HSM Agent, HSM Server and HSM Client. After deploying these modules and establishing security connection, you can use the HSM Client to view logs, statistics and attributes of managed security devices, as well as monitor system status and traffic information.

StoneOS running on each security device is designed with an HSM agent. After configuring this agent, the device can connect to the HSM server and will be managed and controlled by the server.

You can use command lines or WebUI to configure HSM agent (Hillstone SR Series only supports WebUI). The HSM agent configurations include:

- Configuring HSM agent
- Specifying a trust domain
- Enabling/Disabling HSM agent
- Viewing HSM agent configurations

WebUI: Select **System** > **HSM** from the menu bar.

Tip: For more information about HSM, see Hillstone Security Management™ User Guide.

Configuring HSM Agent

HSM agent on the security device allows HSM server to connect to and manage it.

To specify the IP address of HSM server, in the global configuration mode, use the following command:

network-manager host *ip-address*

- *ip-address* - Specifies the IP address of HSM server. This address cannot be 0.0.0.0, 255.255.255.255 or a multicast address.

To configure the port number of HSM server, in the global configuration mode, use the following command:

network-manager host port *port-number*

- *port-number* - Specifies the port number of HSM server. The value range is 1 to 65535. The default value is 9090.

To configure the connection interface of the HSM server, in the global configuration mode, use the following command:

network-manager host source *interface-name*

- *interface-name* - Specifies the connection interface of HSM server.

To modify the registering mode of the HSM server to plain mode (unencrypted), in the global configuration mode, use the following command:

network-manager host plain

To specify the password of HSM server, in the global configuration mode, use the following command:

network-manager host password *password*

- *password* - Specifies the password. HSM server uses this password to authenticate the device. The length is 1 to 31 characters.

To specify the VRouter on which the HSM agent is enabled, in the global configuration mode, use the following command:

network-manager host vrouter *vrouter-name*

- *vrouter-name* - Specifies the name of the VRouter.

To clear the configuration of HSM server, in the global configuration, use the following command:

no network-manager host

To ensure that the device can communicate normally with the HSM server in the NAT environment, you can configure the IP addresses of the FTP servers and log server. By default, the IP address of the FTP server is the IP address of the HSM server, the port numb is 21; the IP address of the log server is the IP address of the HSM server, the port number is 514.

To configure the IP address and the port number of the FTP server, in the global configuration mode, use the following command:

network-manager host ftp-server *ip-address* [**port** *port-number*]

- *ip-address* – Specify the IP address of the FTP server.
- *Port-number* – Specify the port number of the FTP server.

In the global configuration mode, use the following command to restore the following values to the default ones:

no network-manager host ftp-server [**port**]

To configure the IP address and the port number of the log server, in the global configuration mode, use the following command:

network-manager host syslog-server *ip-address* [**secure-tcp**] [**port** *port-number*]

- *ip-address* – Specify the IP address of the log server.
- **secure-tcp** – If this parameter is specified, system will transfer logs enerypted to HSM.
- *port-number* – Specify the port number of the log server.

In the global configuration mode, use the following command to restore the following values to the default ones:

no network-manager host syslog-server [**secure-tcp**] [**port**]

Enabling/Disabling HSM Agent

After configuring HSM server parameters on the device, you need to enable the HSM agent service, which by default is disabled.

To enable HSM agent, in the global configuration mode, use the following command:

```
network-manager enable
```

To disable the HSM agent, in the global configuration mode, use the following command:

```
no network-manager enable
```

Viewing HSM Agent Configuration Information

To view configuration information of HSM agent, in any mode, use the following command:

```
show network-manager
```

Network Time Protocol (NTP)

The Network Time Protocol (NTP) is a protocol for synchronizing the clocks of operating systems based on UDP with dedicated port 123.

Tip: For more information about NTP synchronization, see RFC1305.

For a security device, system time influences many functional modules, like VPN tunnel, schedule and signature certificate, etc. NTP is used to synchronize the system time with NTP server. There are two ways to synchronize time: manual setting and using NTP.

Note: When using the signature license for the first time, do synchronize the system time with the computer time in advance.

WebUI: Select **System** > **Date & Time** from the menu bar.

Configuring System Clock Manually

To configure the system clock manually, in the global configuration mode, use the following command:

```
clock time HH:MM:SS Month Day Year
```

- *password* - Specifies the system clock. *HH*, *MM* and *SS* indicate hour, minute and second respectively, *Month*, *Day* and *Year* indicate month, day and year respectively.

Configuring Time Zone Manually

The system provides multiple predefined time zone. To configure time zone more accurately, you can configure a customized time zone, and configure summer time for the customized time zone.

The default time zone of the system is GMT+8. To configure a time zone, in the global configuration mode, use the following command:

clock zone {*timezone-name* | *cus-timezone-name hours minutes*}

- *timezone-name* - Specifies the name of the pre-efined time zone.
- *cus-timezone-name* - Specifies the name of customized time zone. The value range is 1 to 6 characters.
- *hours minutes* - Specifies the offset to UTC (Universal Time Coordinated). The value range of *hours* is -13 to 12; the value range of *minutes* is 0 to 59.

For example, to configure a customized time zone named test, and set the offset to UTC to 6 hours and 30 minutes, use the following command:

hostname(config)# **clock zone test 6 30**

Configuring Summer Time

Summer time is a local time regulation for saving energy. According to the law issued by the authority, during summer the clock will jump forward for one hour, and will jump backward for one hour when the summer ends. You can specify the absolute time period and the periodic time period of the summer time for the customized time zone.

To specify the absolute time period of the summer time, in the global configuration mode, use the following command:

clock summer-time *cus-timezone-name* **date** *start-date start-time end-date end-time* [*compensation-time*]

- *cus-timezone-name* - Specifies the name of customized time zone. The value range is 1 to 6 characters.
- **date** – Specifies the absolute time period of the summer time.
- *start-date* - Specifies the start date of summer time. The format is month/day/year, for example, 7/20/2011.
- *start-time* - Specifies the start time of summer time. The format is hour:minute, for example, 10:30.
- *end-date* - Specifies the end date of summer time. The format is month/day/year, for example, 7/20/2011.
- *end-time* - Specifies the end time of summer time. The format is hour:minute, for example, 10:30.
- *compensation-time* – Specifies the compensation time when the summer time starts. The default value is 0. For example, when the summer time starts, in some places the clock will jump forward for 1 hour and 30 minutes; when the summer time ends, the clock will jump backward for 1 hour and 30 minutes. In such a case, the compensation time is 1 hour and 30 minutes. The format is hour:minute, such as 1:30.

For example, to configure a customized time zone named test, set the start time and end time of summer time to 6/22/2011 10:30 and 9/23/2011 10:00 respectively, and the summer time is 2 hours and 30 minutes earlier than the non-summer time, use the following command:

hostname(config)# **clock summer-time test date 6/22/2011 10:30 9/23/2011 10:00 2:30**

To specify the periodical time period of the summer time, i.e. executing the summer time in a specified time period in every year, in the global configuration mode, use the following command:

clock summer-time *cus-timezone-name* **recurring** {[**Mon**] | […] | [**Sun**]} {**after** | **before**} *start-day start-month start-time* {[**Mon**] | […] | [**Sun**]} {**after** | **before}** *end-day end-month end-time* [**compensation-time**]

- *cus-timezone-name* – Specifies the name of customized time zone. The value range is 1 to 6 characters.
- **recurring –** Specifies the periodical time period of the summer time.
- [**Mon**] | […] | [**Sun**]} {**after** | **before**} *start-day start-month start-time* – Specifies the start time of the periodical time period. For example, **Mon before 22 6 10:30** means the start time of the summer time in every year is 10:30 on the Monday of the first week before 22nd, June.
- {[**Mon**] | […] | [**Sun**]} {**after** | **before}** *end-day end-month end-time* – Specifies the end time of the periodical time period. For example, **Fri after 23 9 10:00** means the end time of the summer time in every year is 10:00 on the Friday of the first week after 23rd, September.
- *compensation-time* – Specifies the compensation time of the summer time when the summer time takes effect. The default value is 0. For example, when the summer time starts, the system adjust the time of certain zones 1.5 hours ahead, and when the summer time ends, adjust the time of certain zones 1.5 hours back. 1.5 hours is the compensation time you defined. The format is "hour:minute", for example, 1:30.

For example, to configure a customized time zone named test, set the start time as 10:30 on the Monday of the first week before 22nd, June and set the end time as 10:00 on the Friday of the first week after 23rd, September. The time during the summer time is 2.5 hours ahead.

hostname (config) # **clock summer-time test recurring Mon before 22 6 10:30 Fri after 23 9 10:00 2:30**

Note: The summer time may affect logs and modules that rely on time. For example, in the above example, when the summer time ends on 9/23/2011 10:00, the clock will jump backward for 2 hours and 30 minutes, i.e., jump backward to 7:30. Therefore, time range from 7:30 to 10:00 will appear twice on 9/23/2011.

To cancel the summer time configuration, in the global configuration mode, use the command **no clock summer-time** *cus-timezone-name* **date**.

Viewing System Clock Configuration Information

To view the time zone settings, in any mode, use the command **`show clock`**.

To view the summer time settings, in any mode, use the command **`show config`**.

Configuring NTP Service

NTP is used to synchronize the system clock with NTP server. The system supports the following NTP configurations:

- Enabling/Disabling NTP Service
- Configuring an NTP Sever
- Configuring the Max Adjustment Value
- Configuring the Query Interval
- Enabling/Disabling NTP Authentication
- Configuring NTP Authentication

By default, NTP service on Hillstone devices is disabled.

To enable/disable NTP service, in the global configuration mode, use the following commands:

- Enable: **`ntp enable`**
- Disable: **`no ntp enable`**

Configuring an NTP Server

You can specify up to three NTP servers, one of which with keyword "prefer" is the primary NTP server, or, if no "prefer" is specified, the earliest configured NTP server is the first one for time synchronization.

To configure an NTP server, in the global configuration mode, use the following command:

`ntp server` {*`ip-address`* | *`host-name`*} [**`key`** *`number`*] [**`source`** *`interface-name`*] [**`prefer`**] [**`vrouter`** *`vrouter-name`*]

- *`ip-address | host-name`* - Specifies the IP address or host name of the NTP server. The length of the host name can be 1 to 127 characters.
- **`key`** *`number`* - Specifies the password of the NTP server if it requires so.
- **`source`** *`interface-name`* - Specifies the interface on which the security device sends and receives NTP packets.
- **`prefer`** - If more than one NTP servers are specified, use this keyword to determine the primary server.
- *`vrouter-name`* - Specifies NTP server for the specified VRouter.

To cancel the NTP server settings, use the command **no ntp server** {*ip-address* | *host-name*}.

Here is an example of configuring a NTP server:

```
hostname(config)# ntp server 10.160.64.5 prefer
```

Configuring the Max Adjustment Value

The maximum time adjustment value represents the acceptable time difference between the device system clock and the time received from an NTP server. The device only adjusts its clock with the NTP server time if the time difference between its clock and the NTP server time is within the maximum time adjustment value.

To set the maximum adjustment value, in the global configuration mode, use the following command:

ntp max-adjustment *time-value*

- *time-value* - Specifies the time value. The value range is 0 to 3600 seconds. The value of 0 means no adjustment time. The default value is 10.

To restore to the default value, use the command **no ntp max-adjustment**.

Configuring the Query Interval

The device updates its clock with NTP servers at intervals of the value you set here.

To configure the query interval, in the global configuration mode, use the following command:

ntp query-interval *time-interval*

- *time-interval* - The query interval. The value range is 1 to 60 minutes. The default value is 5.

To restore to the default value, use the command **no ntp query-interval**.

Enabling/Disabling NTP Authentication

By default, NTP authentication is disabled.

To enable/disable NTP authentication, in the global configuration mode, use the following commands:

- Enable: **ntp authentication**
- Disable: **no ntp authentication**

Configuring NTP Authentication

If you choose to use NTP authentication, the security device only interact with servers that pass the authentication.

To configure NTP authentication key ID and key, in the global configuration mode, use the following command:

ntp authentication-key *number* md5 *string*

- *number* - Specifies the key ID number. The value range is 1 to 65535.
- *string* - Specifies MD5 authentication key. The length is 1 to 31 characters.

To cancel the authentication private key settings, in the global configuration mode, use the command **no ntp authentication-key** *number*.

Viewing NTP Status

To view the current NTP configurations, in any mode, use the command **show ntp status**.

NTP Configuration Example

Requirements of this configuration example are:

- NTP server IP address is 10.10.10.10;
- Authentication private key ID and key are 1 and aaaa respectively;
- The query interval is 3 minutes;
- The maximum adjustment time is 5 seconds.

Configure the following commands on the device:

```
hostname(config)# ntp authentication-key 1 md5 aaaa
hostname(config)# ntp server 10.10.10.10 key 1 prefer
hostname(config)# ntp query-interval 3
hostname(config)# ntp max-adjustment 5
hostname(config)# ntp authentication
hostname(config)# ntp enable
hostname(config)# show ntp status
ntp client is enabled, authentication is enabled
ntp query-interval is 3, max-adjustment time is 5
ntp server 10.10.10.10, key 1, prefer
```

Configuring Schedule

Schedules control the effective time for some functional modules, such as allowing a policy rule to take effect in a specified time, and controls the duration for the connection between a PPPoE interface and Internet. There are two types of schedule: periodic schedule and absolute schedule. The periodic schedule specifies a time point or time range by periodic schedule entries, while the absolute schedule decides a time range in which the periodic schedule will take effect.

Creating a Schedule

To create a schedule, in the global configuration mode, use the following command:

schedule *schedule-name*

- *schedule-name* - Specifies a name for the schedule. The length of it can be 1 to 31 characters.

This command creates a schedule and leads you into the schedule configuration mode; if the schedule exists, you will enter its configuration mode directly.

To delete a schedule, use the command **no schedule** *schedule-name*. Note that you should unbind the schedule from all the functional modules before deleting it.

WebUI: Select **Objects** > **Schedule** from the menu bar.

Configuring an Absolute Schedule

Absolute schedule is a time range in which periodic schedule will take effect. If no absolute schedule is specified, the periodic schedule will take effect as soon as it is referenced by any module.

To configure an absolute schedule, in the schedule configuration mode, use the following command:

absolute {[**start** *start-date start-time*] [**end** *end-date end-time*]}

- **start** *start-date start-time* - Specifies the start date and time. *start-date* specifies the start date in the format of month/date/year, e.g. 10/23/2007; *start-time* specifies the start time in the format of hour:minute, e.g. 15:30. If this parameter is not specifies, it uses the present time.
- **end** *end-date end-time* - Specifies the end date and time. *end-date* specifies the finish date in the format of month/date/year, e.g. 11/05/2007; *end-time* specifies the finish time in the format of hour:minute, e.g. 09:00. If the parameters are not specifies, there is no end time for the absolute time.

To disable absolute schedule, use the command **no absolute**.

Configuring a Periodic Schedule

A periodic schedule is the collection of all the schedule entries within the schedule. You can add up to 16 schedule entries to a periodic schedule. These entries can be divided into three types:

- Daily: The specified time of every day, such as Everyday 09:00 to 18:00.
- Days: The specified time of a specified day during a week, such as Monday Tuesday Saturday 09:00 to 13:30.
- Due: A continuous period during a week, such as from Monday 09:30 to Wednesday 15:00.

To specify a periodic schedule, in the schedule configuration mode, use the following command:

periodic {**daily** | **weekdays** | **weekend** | [**monday**] […] [**sunday**]} *start-time* **to** *end-time*

- **daily** - Everyday (from Monday to Sunday).
- **weekdays** - Workday (from Monday to Friday).
- **weekend** - Weekends (Saturday and Sunday).
- [**monday**] […] [**sunday**] - Specifies particular days. For example, if you want Tuesday, Wednesday and Saturday, type the key words tuesday wednesday saturday.
- *start-time* - Specifies the start time in the format of hour:minute, e.g. 09:00.
- *end-time* - Specifies the end time in the format of hour: minute, e.g. 16:30.

Repeat the command to add more entries.

To delete a periodic entry, use the command **no periodic** {**daily** | **weekdays** | **weekend** | [**monday**] […] [**sunday**]} *start-time* **to** *end-time*.

To configure an entry which specifies a period of time in a week, in the schedule configuration mode, use the following command:

periodic {[**monday**] | […] | [**sunday**]} *start-time* **to** {[**monday**] | […] | [**sunday**]} *end-time*

- [**monday**] | […] | [**sunday**] - Specifies the start day in a week.
- *start-time* - Specifies the start time in the format of hour:minute, e.g. 09:00.
- [**monday**] | […] | [**sunday**] - Specifies the end day.
- end-time - Specifies the end time in the format of hour:minute, e.g. 16:30.

Repeat this command to add more entries.

To delete an entry, use the command **no periodic** {[**monday**] | […] | [**sunday**]} *start-time* **to** {[**monday**] | […] | [**sunday**]} *end-time*.

Configuring a Track Object

Track object is used to track if the specified object (IP address or host) is reachable and if the specified interface is connected, and if the specified object or link is congested. If the object is not reachable or the link is not connected, the system will directly conclude the track fails; if the object is reachable or the link is connected, the system will continue to detect if the object or link is congested based on packet delay or interface bandwidth. Track is mainly used in HA, PBR, LLB scenarios. By configuring track, you can assure the system is always selecting a comparatively healthy link.

Notes:

- When the track failed, the system will drop all the sessions to the track object.
- When the track object is congested, the system will still keep all the existing sessions to the object, but will not allow any new session.

To configure a track object, in the global configuration mode, use the following command:

track *track-object-name*

- *track-object-name* - Specifies a name for the track object. The length of it can be 1 to 31 characters.

This command creates the track object and leads you into the track object configuration mode; if the object exists, you will enter its configuration mode directly.

To delete the specified track object, use the following command:

no track *track-object-name*

You are allowed to track your object using five protocols: Ping, HTTP, ARP, DNS and TCP.

Track by Ping Packets

To track an object using Ping packets, in the object configuration mode, use the following command:

ip {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**src-interface** *interface-name* [**prior-used-srcip**]] [**weight** *value*] [**delay high-watermark** *value* **low-watermark** *value*] [**delay-weight** *value*]

- *A.B.C.D* | **host** *host-name* - Specifies the IP address or host name of the tracked object. The length of the host name can be 1 to 63 characters.
- **interface** *interface-name* - Specifies the egress interface sending Ping packets.
- **interval** *value* - Specifies the interval of sending Ping packets . The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the number which determines the tracking fails. If the system does not receive response packets of the number specified here, it determines that the tracking has failed, namely, the destination is unreachable. The value range is 1 to 255. The default value is 3.
- **src-interface** *interface-name* - Specifies the source interface of Ping packets.
- **prior-used-srcip** – If the secondary IP is specified for the source interface and specifies the IP to be prior-used-srcip, system will use the IP to send

track packets priorly. If the parameter is not specified, system will use default IP of the source interface to send track packets.

- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.
- **delay high-watermark** *value* **low-watermark** *value* - Specifies the high watermark and low watermark for the object's delay in responding Ping packets. The value range is 1 to 65535 milliseconds. When the delay is below the specified high watermark, the system will conclude the link is normal; when the delay exceeds or equals to the specified high watermark, the system will conclude the link is congested; if congestion occurred, the system will not conclude the link restores to normal until the delay is below or equals to the specified low watermark. Such a design can avoid link status' frequent switching between normal and congested.
- **delay-weight** *value* – Specifies how important this link congestion is to the judgment of track object congestion. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more Ping tracking entries.

To delete the specified tracking entry, use the following command:

no ip {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**delay**]

Track by HTTP Packets

To track an object using HTTP packets, in the track object configuration mode, use the following command:

http {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**src-interface** *interface-name*] [**weight** *value*] [**delay high-watermark** *value* **low-watermark** *value*] [**delay-weight** *value*]

- *A.B.C.D* | **host** *host-name* - Specifies the IP address or host name of the track object. The length of the host name can be 1 to 63 characters.
- **interface** *interface-name* - Specifies the egress interface of sending HTTP test packets.
- **interval** *value* - Specifies the interval of sending HTTP packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 1.
- **src-interface** *interface-name* - Specifies the source interface of the HTTP packets.

- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.
- **delay high-watermark** *value* **low-watermark** *value* - Specifies the high watermark and low watermark for the object's delay in responding HTTP packets. The value range is 1 to 65535 milliseconds. When the delay is below the specified high watermark, the system will conclude the link is normal; when the delay exceeds or equals to the specified high watermark, the system will conclude the link is congested; if congestion occurred, the system will not conclude the link restores to normal until the delay is below or equals to the specified low watermark. Such a design can avoid link status' frequent switching between normal and congested.
- **delay-weight** *value* – Specifies how important this link congestion is to the judgment of track object congestion. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more HTTP tracking entries.

To delete the specified tracking entry, use the following command:

no http {*A.B.C.D* | **host** *host-name*} **interface** *interface-name* [**delay**]

Track by ARP Packets

To track an object using ARP packets, in the track object configuration mode, use the following command:

arp {*A.B.C.D*} **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**weight** *value*]

- *A.B.C.D* - Specifies the IP address of the track object.
- **interface** *interface-name* - Specifies the egress interface of sending ARP test packets.
- **interval** *value* - Specifies the interval of sending ARP packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the threshold number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 3.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more ARP tracking entries.

To delete the specified tracking entry, use the following command:

no arp {*A.B.C.D*} **interface** *interface-name* [**delay**]

Track by DNS Packets

To track an object using DNS packets, in the track object configuration mode, use the following command:

dns *A.B.C.D* **interface** *interface-name* [**interval** *value*] [**threshold** *value*] [**weight** *value*] [**src-interface** *interface-name*] [**delay high-watermark** *value* **low-watermark** *value*] [**delay-weight** *value*]

- *A.B.C.D* - Specifies the IP address of track object.
- **interface** *interface-name* - Specifies the egress interface of sending DNS test packets.
- **interval** *value* - Specifies the interval of sending DNS packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the threshold number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 3.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.
- **src-interface** *interface-name* - Specifies the source interface of DNS test packets.
- **delay high-watermark** *value* **low-watermark** *value* - Specifies the high watermark and low watermark for the object's delay in responding DNS packets. The value range is 1 to 65535 milliseconds. When the delay is below the specified high watermark, the system will conclude the link is normal; when the delay exceeds or equals to the specified high watermark, the system will conclude the link is congested; if congestion occurred, the system will not conclude the link restores to normal until the delay is below or equals to the specified low watermark. Such a design can avoid link status' frequent switching between normal and congested.
- **delay-weight** *value* - Specifies how important this link congestion is to the judgment of track object congestion. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more DNS tracking entries.

To delete the specified tracking entry, use the following command:

no dns *A.B.C.D* **interface** *interface-name* [**delay**]

Track by TCP Packets

To track an object using TCP packets, in the track object configuration mode, use the following command:

tcp {*A.B.C.D* | **host** *host-name*} **port** *port-number* **interface** *interface-name* [**src-interface** *interface-name*] [**interval** *value*] [**threshold** *value*] [**src-interface** *interface-name*] [**weight** *value*] [**delay high-watermark** *value* **low-watermark** *value*] [**delay-weight** *value*]

- *A.B.C.D* | **host** *host-name* - Specifies the IP address or host name of track object. The length of the host name can be 1 to 63 characters.
- **port** *port-number* - Specifies the destination port of the track object. The value range is 0 to 65535.
- **interface** *interface-name* - Specifies the egress interface for sending TCP test packets.
- **interval** *value* - Specifies the interval of sending TCP packets. The value range is 1 to 255 seconds. The default value is 3.
- **threshold** *value* - Specifies the threshold number which concludes the tracking fails. If the system does not receive response packets of the number specified here, it concludes that the tracking has failed. The value range is 1 to 255. The default value is 3.
- **src-interface** *interface-name* - Specifies the source interface of TCP test packets.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.
- **delay high-watermark** *value* **low-watermark** *value* - Specifies the high watermark and low watermark for the object's delay in responding TCP packets. The value range is 1 to 65535 milliseconds. When the delay is below the specified high watermark, the system will conclude the link is normal; when the delay exceeds or equals to the specified high watermark, the system will conclude the link is congested; if congestion occurred, the system will not conclude the link restores to normal until the delay is below or equals to the specified low watermark. Such a design can avoid link status' frequent switching between normal and congested.
- **delay-weight** *value* - Specifies how important this link congestion is to the judgment of track object congestion. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more TCP tracking entries. For one single track object, you cannot configure both the HTTP track on the host and TCP track on port 80 simultaneously.

To delete the specified tracking entry, use the following command:

no tcp {*A.B.C.D* | **host** *host-name*} **port** *port-number* **interface** *interface-name* [**delay**]

Interface Status Track

To track interface status, in the track object configuration mode, use the following command:

interface *interface-name* [**weight** *value*]

- *interface-name* - Specifies the interface name.
- **weight** *value* - Specifies how important this entry failure is to the judgment of tracking failure. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more tracking entries.

To delete the specified tracking entry, use the following command:

no interface *interface-name*

Interface Bandwidth Track

To track interface bandwidth, in the track object configuration mode, use the following command:

bandwidth interface *interface-name* **direction** {**in** | **out** | **both**} **high-watermark** *value* **low-watermark** *value* [**interval** *value*] [**threshold** *value*] [**weight** *value*]

- *interface-name* - Specifies the interface name.
- **direction** {**in** | **out** | **both**} - Specifies the traffic direction to be tracked. **in** indicates ingress, **out** indicates egress (the default direction), **both** indicates the both directions.
- **high-watermark** *value* **low-watermark** *value* – Specifies the high watermark and low watermark for the interface bandwidth. The value range is 1 to 100000000 kbps. When the interface bandwidth is below the specified high watermark, the system will conclude the link is normal; when the interface bandwidth exceeds or equals to the specified high watermark, the system will conclude the link is congested; if congestion occurred, the system will not conclude the link restores to normal until the interface bandwidth is below or equals to the specified low watermark. Such a design can avoid link status' frequent switching between normal and congested.
- **interval** *value* - Specifies the tracking interval. The value range is 1 to 255 seconds. The default value is 3
- **threshold** *value* – Specifies the threshold number which concludes the entry is congested. If the system detected interface overload for the times specified here in succession, it concludes the entry is congested. The value range is 1 to 255. The default value is 1.
- **weight** *value* - Specifies how important this link congestion is to the judgment of track object congestion. The value range is 1 to 255. The default value is 255.

Repeat the command to configure more tracking entries.

To delete the specified tracking entry, use the following command:

no bandwidth interface *interface-name*

Configuring a Threshold

Threshold is used to conclude if the track object failed or is congested. When the total weight sum of the track entries that belong to the same category in the track object exceeds or equals to the corresponding threshold, the system will conclude the track object failed or is congested. For track object failure, track object congestion caused by response packet timeout and track object congestion caused by interface overload scenarios, you can set different types of thresholds: track object failure threshold, response packet timeout threshold and interface bandwidth threshold.

Monitor Object FailureThreshold

If the sum of weight values of all track entries exceeds or equals to a certain value, the system concludes that the tracking fails. The value is known as the track object failure threshold value.

To configure the track object failure threshold value, in the track object configuration mode, use the following command:

threshold *value*

- *value* - Specifies the threshold value. The value range is 1 to 255. The default value is 255.

To restore to the default threshold value, in the track object configuration mode, use the following command:

no threshold

Response Packet Timeout Threshold

If the sum of weight values of track entry congestion caused by response packet timeout in the track object exceeds or equals to a certain value, the system concludes that the track object is congested. The value is known as the response packet timeout threshold value.

To configure the response packet timeout threshold value, in the track object configuration mode, use the following command:

delay-threshold *value*

- *value* - Specifies the threshold value. The value range is 1 to 255. The default value is 255.

To restore to the default threshold value, in the track object configuration mode, use the following command:

no delay-threshold

For example, configure a track object as below:

```
hostname(config)# track delay-test
hostname(config-trackip)# delay-threshold 250
hostname(config-trackip)# dns 1.1.1.1 interface ethernet0/1
delay high-watermark 100 low-watermark 50 delay-weight 50
hostname(config-trackip)# dns 1.1.1.2 interface ethernet0/1
delay high-watermark 100 low-watermark 50 delay-weight 220
```

After the configuration, if the track entry 1.1.1.1 and 1.1.1.2 are both congested (i.e., response packet delay for the DNS requests sent by the the entries exceed 100ms), the **delay-weight**=50+220=270>250, so the system will conclude the track object **delay-test** is congested.

Interface Bandwidth Threshold

If the sum of weight values of track entry congestion caused by interface overload in the track object exceeds or equals to a certain value, the system concludes that the track object is congested. The value is known as the interface bandwidth threshold value.

To configure the interface bandwidth threshold value, in the track object configuration mode, use the following command:

bandwidth-threshold *value*

- *value* - Specifies the threshold value. The value range is 1 to 255. The default value is 255.

To restore to the default threshold value, in the track object configuration mode, use the following command:

no bandwidth-threshold

For example, configure a track object as below:

```
hostname(config)# track bandwidth-test
hostname(config-trackip)# bandwidth-threshold 250
hostname(config-trackip)# bandwidth interface ethernet0/1
direction both high-watermark 20 low-watermark 10 threshold 5
weight 220
hostname(config-trackip)# bandwidth interface ethernet0/2
direction both high-watermark 20 low-watermark 10 threshold 5
weight 50
```

After the configuration, if the track entry eth0/1 and eth0/2 are both overloaded (i.e., traffic over 20kbps occurred for 5 times or more on the both interfaces), the **bandwidth-threshold**=50+220=270>250, so the system will conclude the track object **bandwidth-test** is congested.

If the track object of a tracked interface fails or is congested, the system automatically disables all routes (static routes, dynamic routes, PBR, etc.) on the interface, i.e., normal traffic forwarding will not be matched to the routes on the failed or congested interface. However, if there is only one default egress route, this rule will void.

To view the configuration of track object, in any mode, use the following command:

show track *tack-object-name*

Fail Close

With this function enabled, system will check application layer IPS, AV, content filtering and Web Content, application-layer behavior control. If you disable this feature , when the system resources is too low , such as CPU usage high, memory or data packets buffer residual capacity is insufficient, system will pass packets for controlling the resources utilization, so as not to affect other functions. By default, this function is disabled.

To enable fail close, under global configuration mode, use the following command:

fail-close enable

To disable fail close, under global mode, use the command:

no fail-close enable

Note: Fail close is not applicable for: FTP behavior control, web surfing, MSRPC/SUNRPC/DNS (UDP) check of IPS.

Viewing Fail Close Status

To view the fail close status, in any mode, use the following command:

show fail-close

Monitor Alarm

The monitor alarm function is designed to monitor the utilization of system resources, and issue an alarm according to the configuration. The current version supports log and SNMP Trap alarms.

You need to enter the monitor configuration mode to configure the monitor alarm function. To enter the monitor configuration mode, in the global configuration mode, use the following command:

monitor

After entering the monitor configuration mode, you can configure a monitor rule as needed for the system resource object:

{**cpu** | **memory utilization** | **interface-bandwidth** *interface-name* **utilization** | **log-buffer** { **config** | **event** | **ips** | **nbc** | **network** | **security** | **traffic {session** | **nat** | **web-surfing**}} **utilization** | **policy utilization** | **session utilization| snat-resource utilization**} **interval** *interval-value* **absolute rising-threshold** *threshold-value* **sample-period** *period-value* [**count** *count-value*] {**log** [**snmp-trap**]| **snmp-trap**}

- **cpu** | **memory utilization** | **interface-bandwidth** *interface-name* **utilization** | **log-buffer** { **config** | **event** | **ips** | **nbc** | **network** | **security** | **traffic** {**session** | **nat** | **web-surfing**}} **utilization** | **policy utilization** | **session utilization** | **snat-resource utilization** - Specifies the monitor object which can be **cpu**, **memory**, **interface-bandwidth**, **log-buffer**, **policy**, **session** or **snat-resource**. When you use the X platforms and enter the **cpu** keyword, proceed to select modules.
  - *interface-name* - Specifies the name of interface.
  - **config** | **event** | **ips** | **nbc** | **network** | **security** | **traffic** {**session** | **nat** | **web-surfing**} - Specifies the log type.
  - **utilization** - Specifies the value of monitor object as the utilization of each object. Since the default value for **cpu** is utilization, so you do not need to specify this parameter for the monitor object of CPU.
- **interval** *interval-value* - Specifies the monitor interval, i.e., the interval for acquiring the value of monitor object within the sampling period (**sample-period** *period-value*). The value range is 3 to 10 seconds.
- **absolute** - Specifies the value of monitor object as an absolute value.
- **rising-threshold** *threshold-value* - Specifies the rising threshold. The system will issue an alarm if the value of monitor object exceeds the percentage specified here. The value range is 1 to 99.
- **sample-period** *period-value* - Specifies the sample period. The value range is 30 to 3600 seconds.
- **count** *count-value* - Specifies the count for the conditions the value of monitor object exceeds the **rising-threshold** within the sampling period (**sample-period**). The value range is 1 to 1000. If this parameter is configured, when the count exceeds the **rising-threshold** within the sampling period, the system will issue an alarm; if this parameter is not configured, when the average value of monitor object exceeds the **rising-threshold**, the system will issue an alarm.
- **log** [**snmp-trap**]| **snmp-trap** - Specifies the method which can be **log**, **snmp-trap** or both..

For example:

To configure the peak CPU utilization monitor:

```
hostname(config)# monitor
hostname(config-monitor)# cpu interval 5 absolute rising-
threshold 65 sample-period 600 count 50 log
```

After the configuration, if the CPU utilization exceeds the rising threshold of 65% within 600 seconds, and such a condition occurs at least 50 times, then the system will issue a log.

To configure the average session utilization monitor:

```
hostname(config)# monitor
hostname(config-monitor)# session utilization interval 8
absolute rising-threshold 90 sample-period 600 log
```

After the configuration, if the average session utilization exceeds the rising threshold of 90% within 600 seconds, then the system will issue a log.

To delete the specified monitor rule, in the monitor configuration mode, use the following command:

no {**cpu** | **memory utilization** | **interface-bandwidth** *interface-name* **utilization** | **log-buffer** { **config** | **event** | **ips** | **nbc** | **network** | **security** | **traffic {session** | **nat** | **web-surfing**}} **utilization** | **policy utilization** | **session utilization**}

Notes:

- For every monitor object, only the last configured monitor rule takes effect.
- The system does not support monitor alarm for port resources whose IP address is translated into an egress IP address (*eif-ip*) after SNAT.

To view the monitor alarm configuration, in any mode, use the following command:

show monitor

The type of the monitor logs is event, and the severity is critical. You can view the logs directly, or configure email notification to send the logs to administrator's mailbox. For more information about how to configure system log, see "Logs".

To view the event logs whose severity is above critical, in any mode, use the following command:

show logging alarm [**severity** *severity-level*]

The Maximum Concurrent Sessions

If multi-VR, AV, IPS and/or URL signature database is enabled on Hillstone devices, or IPv6 firmware version is used, the maximum concurrent sessions might change. For more information, see the table below:

Table 8: Maximum Concurrent Sessions

Platform	Firmware	Max Concurrent Sessions

SG-6000-M8860 SG-6000-M8260 SG-6000-M7260 SG-6000-M7860	StoneOS IPv4 version	With multiple virtual routers, anti-virus, IPS and/or URL signature database enabled on the system , the maximum concurrent sessions will not change.
	StoneOS IPv6 version	The maximum concurrent sessions will not change. IPv6 version does not support multiple virtual routers, anti-virus, IPS and URL signature database.
SG-6000-X7180 SG-6000-X6180 SG-6000-X6150	StoneOS IPv4 version	With multiple virtual routers enabled: the maximum concurrent sessions will drop by 15%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions*(1-0.15). Anti-virus, IPS, and URL signature database are not supported.
	StoneOS IPv6 version	The maximum concurrent sessions is 50% of the IPv4 version. Multiple virtual routers, anti-virus, IPS, and URL signature database are not supported.
Other SG-6000 platforms	StoneOS IPv4 version	• With multiple virtual routers enabled: the maximum concurrent sessions will drop by 15%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions*(1-0.15); • With anti-virus, IPS and/or URL signature database enabled: the maximum concurrent sessions will drop by 50%. The formula is: Actual maximum sessions*(1-0.15)*(1-0.5).concurrent sessions = original maximum concurrent sessions*(1-0.5); • With multiple virtual routers plus anti-virus, IPS and/or URL signature database enabled simultaneously, the maximum concurrent sessions will further drop by 50%. The formula is: Actual maximum concurrent sessions = original maximum concurrent sessions*(1-0.15)*(1-0.5).
	StoneOS IPv6 version	The maximum concurrent sessions is 50% of the IPv4 version. IPv6 version does not support multiple virtual routers, anti-virus, IPS and URL signature database.

Connecting to Hillstone CloudView

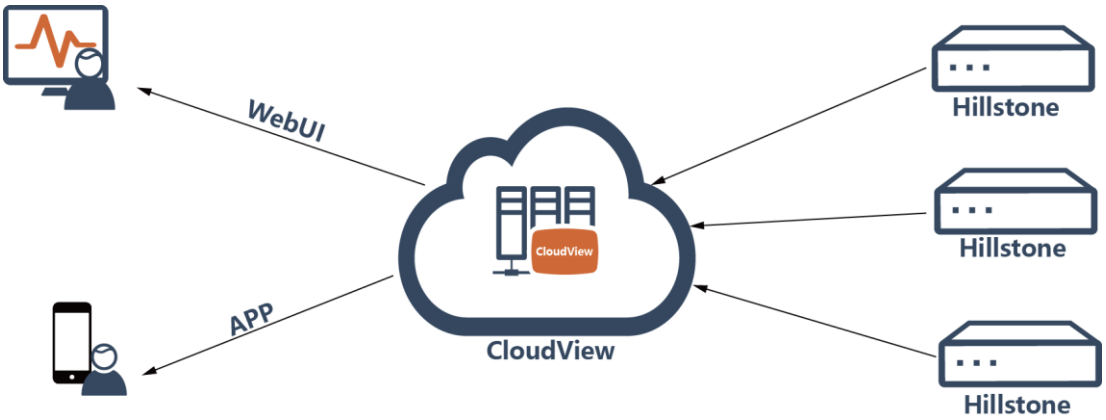
CloudView is a SaaS products of security area and a cloud security services platform in the mobile Internet era. CloudView deployed in the public cloud, to provide users with online on-demand services. Users can get convenient, high quality and low cost value-added security services through the Internet, APP, and get a better security experience.

After the Hillstone device is properly configured to connect the CloudView, you can achieve the Hillstone device registration to the public cloud and the connection with the CloudView, and then to achieve the Cloud View remote monitoring device.

CloudView Deployment Scenarios

The main deployment scenarios of CloudView are described as follows:

Hillstone devices registered to the CloudView, the device information, traffic data, threat event, system logs uploaded to the cloud, the cloud provides a visual display. Users can through the Web or mobile phone APP monitoring device status information, reports, threat analysis, etc.



Configuring Hillstone Device

In the device, configure the following settings:

- Configuring CloudView server
- Enabling CloudView
- Enabling traffic data uploading
- Enabling system log uploading
- Enabling threat event uploading
- Enabling Threat Prevention Data Uploading
- Displaying configurations of CloudView server

Configuring CloudView Server

To configure the URL, username, password of CloudView server, in the global configuration mode, use the following command:

cloud server address *A.B.C.D* |*domain* **[username** user-name **password** password]

- *A.B.C.D/domain* –Specify the URL or domain name of CloudView server. The default URL is http://cloud.hillstonenet.com.cn.
- **username** *user-name* – Specify the username of CloudView. Register the device to this user.
- **password** *password* – Specify the password of the user.

To restore to the default value, use the **no cloud server address** command.

Enabling CloudView

You can enable the Cloud View function by entering the **cloud server enable** command in the global configuration mode.

Enabling Traffic Data Uploading

To upload the monitor data, in the global configuration mode, use the following command:

cloud server upload-type traffic

To disable the traffic data uploading, use the **no cloud server upload-type traffic** command.

Enabling System Log Uploading

To upload the event logs, in the global configuration mode, use the following command:

cloud server upload-type log-event

To disable the system log uploading, use the **no cloud server upload-type log-event** command.

Note: Before enabling this function, please ensure that the device has been enabled the event log function (**logging event on**) and the CloudView server status is connected.

Enabling Threat Event Uploading

To upload the threat events detected by Hillstone device, in the global configuration mode, use the following command:

cloud server upload-type threat-event

To disable the threat events uploading, use the **no cloud server upload-type threat-event** command.

Note: About the configuration of threat detection, see the specific threat protection function section.

Enabling All Types of Data Uploading

To upload the all types of data, in the global configuration mode, use the following command:

cloud server upload-type all

To disable the all types of data uploading, use the **no cloud server upload-type all** command.

Enabling Threat Prevention Data Uploading

To enable threat prevention data uploading, in the global configuration mode, use the following command:

cloud server upload-type hcsp

To can the uploading settings, use the **no cloud server upload-type hcsp** command.

Displaying Configurations of CloudView Server

To display the configurations of CloudView server, in any mode, use the following command:

show cloud server