Hillstone Networks Inc.

StoneOS 命令行用户手册

系统管理 分册

Version 5.5R6

联系信息

公司总部（北京总部）：

地址： 北京市海淀区宝盛南路 1 号院 20 号楼 5 层

邮编： 100192

联系我们：http://www.hillstonenet.com.cn/about/contact_Hillstone.html

关于本手册

本手册介绍 Hillstone Networks 公司的防火墙系统 StoneOS 的使用方法。

获得更多的文档资料，请访问：http://docs.hillstonenet.com

针对本文档的反馈，请发送邮件到：hs-doc@hillstonenet.com

TWNO: TW-CUG-UNI-SYS-5.5R6-CN-V1.0-Y18M10

目录

关于本手册

手册约定

为方便用户阅读与理解，本手册遵循以下约定：

内容约定

本手册内容约定如下：

- 提示：为用户提供相关参考信息。
- 说明：为用户提供有助于理解内容的说明信息。
- 注意：如果该操作不正确，会导致系统出错。
- 『 』：用该方式表示 Hillstone 设备 WebUI 界面上的链接、标签或者按钮。例如，“点击『登录』按钮进入 Hillstone 设备的主页”。
- < >：用该方式表示 WebUI 界面上提供的文本信息，包括单选按钮名称、复选框名称、文本框名称、选项名称以及文字描述。例如，“改变 MTU 值，选中<手动>单选按钮，然后在文本框中输入合适的值”。

CLI 约定

本手册在描述 CLI 时，遵循以下约定：

- 大括弧（{ }）：指明该内容为必要元素。
- 方括弧（[ ]）：指明该内容为可选元素。
- 竖线（|）：分隔可选择的互相排斥的选项。
- 粗体：粗体部分为命令的关键字，是命令行中不可变部分，用户必须逐字输入。
- 斜体：斜体部分为需要用户提供值的参数。
- 命令实例中，需要用户输入部分用粗体标出；需要用户提供值的变量用斜体标出；命令实例包括不同平台的输出，可能会有些许差别。
- 命令实例中，命令提示符中的主机名称均使用“hostname”。

命令行接口（CLI）

CLI 介绍

Hillstone 山石网科多核安全网关操作系统 StoneOS 提供一系列命令以及命令行接口（Command Line Interface），使用户能够对安全网关进行配置和管理。以下各节将介绍 StoneOS 命令行接口的使用方法及特点。

注意：使用 CLI 配置安全网关时，命令本身的关键字不区分大小写，但是，用户输入的内容区分大小写。

命令模式和提示符

StoneOS CLI 有不同级别的命令模式，一些命令只有在特定的命令模式下才可使用。例如，只有在相应的配置模式下，才可以输入并执行配置命令，这样也可以防止意外破坏已有的配置。不同的命令模式都有其相应的 CLI 提示符。

执行模式

用户进入到 CLI 时的模式是执行模式。执行模式允许用户使用其权限级别允许的所有的设置选项。该模式的提示符如下所示，包含了一个井号（#）：

```
hostname#
```

全局配置模式

全局配置模式允许用户修改安全网关的配置参数。用户在执行模式下，输入 `configure` 命令，可进入全局配置模式。该模式的提示符如下所示：

```
hostname(config)#
```

子模块配置模式

安全网关的不同模块功能需要在其对应的命令行子模块模式下进行配置。用户在全局配置模式输入特定的命令可以进入相应的子模块配置模式。例如，运行 `interface ethernet0/0` 命令进入 ethernet0/0 接口配置模式，此时的提示符变更为：

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

CLI 命令模式切换

用户登录到安全网关 CLI 就进入到 CLI 的执行模式。用户可以通过不同的命令在各种命令模式之间进行切换。下表列出 CLI 的模式切换命令：

表 1：CLI 模式切换命令

模式	命令
执行模式到全局配置模式	configure
全局配置模式到子模块配置模式	不同功能使用不同的命令进入各自的命令配置模式。
退回到上一级命令模式	exit
从任何模式退回到执行模式	end

命令行错误信息提示

StoneOS CLI 具有命令语法检查功能，只有通过了 CLI 语法检查的命令能够正确执行。对于不能通过 CLI 语法检查的命令，StoneOS 会输出错误信息提示。常见的错误信息如下表所示：

表 2：命令行常见错误信息

提示信息	描述
Unrecognized command	StoneOS 找不到输入的命令或者关键字。
	输入的参数类型错误。
	输入的参数值越界。
Incomplete command	输入的命令不完整。
Ambiguous command	输入的参数不明确。

命令行的输入

为简化用户的输入操作，用户可以使用命令的缩写形式进行配置，除此之外，StoneOS CLI 还提供自动列出命令关键字和自动补齐命令功能。

命令行的缩写形式

命令的缩写形式一般是由命令中的几个独特字符组成。大部分 StoneOS 命令都有缩写形式。例如，用户可以仅输入 `sho int` 来查看设备的接口配置信息，而不用输入 `show interface`；仅输入 `conf` 就可进入全局配置模式。

自动列出命令关键字

StoneOS CLI 具有输入问号（？）列出命令关键字的功能。具体包括以下两种情况：

- 在一个或一组有效字符后输入问号，CLI 将自动列出以这个或该组字母开头的可用命令（包括命令功能的简短介绍）或者该有效字符后可以输入参数值。
- 如果直接输入问号，CLI 将列出所在模式下所有的可用命令和命令的简短介绍。

自动补齐命令关键字

StoneOS CLI 支持 TAB 键补齐命令关键字的功能。在部分字符后按 TAB 键，以该字符开头的命令会被自动补齐。但是，该自动补齐功能仅在只有唯一命令匹配时有效。例如，在执行模式下输入“conf”后敲 TAB 键，系统会自动将命令补齐为“configure”。

命令行的编辑

StoneOS 命令行的编辑操作简单，主要包括以下几方面：

查看历史命令

StoneOS CLI 可记录最近输入的 64 条命令，用户可以通过上、下键或快捷键 Ctrl+P、Ctrl+N 来查看上一条或者下一条历史命令。用户可以编辑或是使用任何一条找到的历史命令。

快捷键

StoneOS CLI 支持快捷键的使用。下表列出 StoneOS 支持的快捷键及其功能：

表 3：StoneOS 快捷键

快捷键	功能
Ctrl-A	将光标移至所在行的行首。
Ctrl-B	将光标向回移动一个字符。
Ctrl-D	删除光标所在的字符。
Ctrl-E	将光标移至所在行的行尾。
Ctrl-F	将光标向前移动一个字符。
Ctrl-H	删除光标前一个字符。
Ctrl-K	删除光标后所有字符。

Ctrl-N	显示下一条历史命令。
Ctrl-P	显示上一条历史命令。
Ctrl-T	调换光标所在字母及其前一字母的顺序。
Ctrl-U	删除光标所在行。
Ctrl-W	删除光标前的词。
META-B	将光标移至所在词的词首。
META-D	删除光标后的词。
META-F	将光标移至所在词的词尾。
META-Backspace	删除光标前的词。
META-Ctrl-H	删除光标前的词。

说明：在没有 META 键的电脑上，请先按 ESC 键，再按字母键。例如，META-B 的操作过程为先按一下 ESC 键，然后再按字母 B。

过滤 CLI 输出信息

StoneOS CLI 用 `show` 命令显示设备的配置信息。用户可以根据需要对 show 命令的输出信息进行过滤。过滤方法为在 show 命令后添加一个过滤条件并用竖线（|）把命令和过滤条件隔开。过滤条件有三种：

- include <过滤条件>：输出符合过滤条件的信息。<过滤条件>中的字母区分字母大小写。
- exclude <过滤条件>：输出过滤条件以外的信息。<过滤条件>中的字母区分大小写。
- begin <过滤条件>：从第一条符合过滤条件的信息开始输出。<过滤条件>中的字母区分大小写。

CLI 输出信息过滤的语法格式为：

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

在以上命令行中，第一个竖线（|）是命令的一部分，指明输出信息要按照过滤条件进行过滤。以后的竖线用来分隔命令的不同参数，并不是命令包含的部分。

过滤条件符合正则表达式规范。下表列出正则表达式中常用的字符及其表示的含义：

表 4：字符及含义

字符	含义
句点（.）	匹配任意单字符。
星号（*）	一个单字符后紧跟*，匹配 0 个或多个此单字符。
加号（+）	一个单字符后紧跟+，匹配 1 个或多个此单字符。
脱字符号（^）	只匹配行首。
美元符号（$）	只匹配行尾。
下划线（_）	匹配逗号（,）、左大括号（{）、右大括号（}）、左圆括号（(）、右圆括号（)）、

	行首、行尾或者空格。
方括号（[]）	指定单个字符的范围。
连字符（-）	分隔范围的终点。

分页显示 CLI 输出信息

一些命令回显输出信息比较长，可能需要许多页显示，CLI 会用提示符“--More--”表示一页的结束。用户可以通过不同的操作指定继续显示信息或者终止显示信息。用户可执行的操作有：

- 显示下一行信息：按回车键。
- 返回到命令行：按“Q”键或者“q”键。
- 继续显示下一页信息：按除回车、“Q”和“q”以外的任意键。

设置终端属性

用户可以通过命令设置所使用终端的宽度和长度。默认情况下，终端宽为 80 个字符，长为 25 行。请使用以下命令设置终端的宽度和长度：

- 宽度：**terminal width** *character-number*

  character-number – 指定字符数。范围是 64 到 512 个字符。
- 长度：**terminal length** *line-number*

  line-number – 指定行数，终端显示的行数为指定行数减 1（但是如果配置行数为 1，则显示 1 行）。范围是 0 到 256 行，0 的含义为不分屏显示。

终端的设置只对当前连接有效，不会被记录到配置文件。终端断开连接后再次登录时，终端的宽度和长度又会恢复到默认值。

设置连接超时时间

StoneOS CLI 可以设置 Console、SSH 或 Telnet 连接的超时时间。在全局配置模式下，输入以下命令设置超时时间：

- **console timeout** *timeout-value*

  timeout-value – 指定 Console 超时时间。范围是 0 到 60 分钟，0 表示永不超时。默认值为 10 分钟。

  在全局配置模式使用 **no console timeout** 命令恢复 Console 超时时间的默认值。
- **ssh timeout** *timeout-value*

timeout-value - 指定 SSH 超时时间。范围是 1 到 60 分钟。默认值是 10 分钟。

在全局配置模式使用 **no ssh timeout** 命令恢复 SSH 超时时间的默认值。

- **telnet timeout** *timeout-value*

  timeout-value - 指定 Telnet 超时时间。范围是 1 到 60 分钟，默认是 10 分钟。

  在全局配置模式使用 **no telnet timeout** 命令恢复 Telnet 超时时间的默认值。

重定向输出

StoneOS 允许用户将 show 命令的输出信息重定向输出到其它的目的地址，包括安全设备的 FTP Server 和 TFTP Server。重定向输出命令的格式为：

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

目的地址（*dst-address*）的格式为：

- FTP – ftp://[username:password@]x.x.x.x[:port]/filename
- TFTP – tftp://x.x.x.x/filename

诊断命令

StoneOS CLI 支持 ping 和 traceroute 两个诊断命令。用户可以通过这两个命令查看网络和路由是否连通。

系统管理

系统管理介绍

StongOS 的系统维护与管理主要包括以下各项：

- 命名规则
- 配置主机名称
- 配置系统信息显示语言
- 配置系统管理员
- 配置可信主机
- 配置 NetBIOS 名字解析功能
- 系统用户管理
- 配置管理接口
- 配置存储设备
- 配置文件管理
- 系统维护与调试
- 配置系统重启
- StoneOS 版本升级
- 双主控 HA
- 许可证管理
- 简单网络管理协议（SNMP）
- HSM 代理
- 网络时间协议（NTP）
- 配置时间表功能
- 配置监测对象
- 系统监控报警
- 系统最大并发连接数变化

命名规则

为不同的对象命名时，请遵循以下规则：

- 系统不建议使用以下特殊符号：逗号（,）、单引号（‘’）、双引号（“”）、制表符、空格、分号（;）、反斜杠（\）、斜杠（/）、尖括号（<>）、特殊字符（&、#）。为避免产生错误，建议用户尽量使用数字（0-9）和字母（a-z，A-Z）组成对象名称。
- 使用 CLI 创建对象时，如果对象名称中包含空格，请用双引号引住对象名称。在 WebUI 上创建带空格名称的对象时则无此限制，可直接输入对象名称。

配置主机名称

有些情况下，用户的网络环境中会配有一台以上 Hillstone 设备，为区分这些 Hillstone 设备，就需要为每一台 Hillstone 设备指定不同的名称。Hillstone 设备的默认名称是其平台名称。通过 CLI 配置 Hillstone 设备名称，在全局配置模式输入以下命令：

hostname *host-name*

- *host-name* – 指定 Hillstone 设备名称。长度范围是 1 到 63 个字符。执行该命令后，命令行提示符也会变为新的 Hillstone 设备的名称。在全局配置模式下使用 no hostname 命令恢复 Hillstone 设备的默认名称。

以下是配置 Hillstone 设备名称的命令示例：

```
hostname# configure （进入全局配置模式）
hostname(config)# hostname hillstone
hillstone(config)#
```

配置系统信息显示语言

系统信息包括日志信息、错误信息和提示信息。设备支持简体中文和英文两种系统信息显示语言，在全局配置模式下，使用以下命令设置显示语言：

language {**en** | **zh_CN**}

- **en** – 设置系统信息显示语言为英文。默认情况下，系统信息显示语言为英文。
- **zh_CN** – 设置系统信息显示语言为简体中文。

在全局配置模式下使用 **no language** 命令恢复显示语言为默认情况。

需要注意的是，该命令的设置不会影响 Web 管理界面的语言。

配置管理员

Hillstone 设备的管理员根据角色的不同，对系统可执行的管理和配置权限不同。系统支持预定义管理员角色和自定义管理员角色。

系统默认预定义如下四类管理员角色，这四类管理员角色不可被删除和编辑：

- 系统管理员（admin）：拥有读、执行和写权限，可以通过 show 命令查看当前或者历史配置信息、在执行模式下运行 `import`、`export` 和 `save` 等命令以及在任何模式下对设备所有功能模块进行配置。
- 系统管理员（只读）（admin-read-only）：拥有读和部分执行权限，可以通过 show 命令查看当前或者历史配置信息，可以在执行模式下运行 `export` 命令。
- 系统操作员 (operator)：拥有读、执行和部分写权限，可以修改除管理员配置、重启设备、恢复出厂设置以及升级版本以外的其他功能模块配置，通过 show 命令查看当前或者历史配置信息、但是不能查看日志信息，以及在执行模式下运行部分执行命令。
- 系统审计员（auditor）：只可以对日志信息进行操作，包括查看、导出和清除。

下表为管理员的详细权限列表。

表 1：管理员权限列表

功能	权限			
	系统管理员	系统管理员（只读）	系统操作员	系统审计员
配置(包括保存配置)	√	X	√	X
管理员配置	√	X	X	X
恢复出场配置	√	X	X	X
删除配置文件	√	X	√	X
回退起始配置信息	√	X	√	X
重启设备	√	X	X	X
查看配置信息	√	√	√	X
查看日志信息	√	√	X	√
修改当前管理员密码	√	√	√	√
`import` 命令	√	X	√（除系统升级外）	X
`export` 命令	√	√	X	√
`clear` 命令	√	√	√	√

功能	权限			
	系统管理员	系统管理员（只读）	系统操作员	系统审计员
ping/traceroute 命令	√	√	√	X
debug 命令	√	√	√	X
exec 命令	√	√	√	√
terminal width 命令	√	√	√	√

注意：

- Hillstone 设备拥有一个默认系统管理员 “hillstone”，用户可以对系统管理员 “hillstone” 进行编辑（只可编辑密码和访问方式），但是不能删除该管理员。
- 除了系统管理员，其他角色的管理员不能编辑管理员的任何属性，只能修改自身密码。
- 系统审计员可以管理一种或多种日志信息，管理日志类型需要系统管理员配置。

用户可自定义管理员角色，指定管理员角色对 CLI 的权限和 WebUI 的权限。

- 对 CLI 的权限包括 “读写” 和 “不可用”。
- 针对 WebUI 的各个功能模块，用户可设定 “读写”、“只读”、或 “不可用” 三个权限。

管理员配置包括：

- 新建管理员角色
- 指定管理员角色的权限
- 指定管理员角色的描述信息
- 创建管理员
- 配置管理员角色
- 配置管理员密码
- 配置管理员访问方式
- 配置系统审计员可管理日志类型
- 配置管理员登录限制
- 显示管理员角色的配置
- 显示管理员配置
- VSYS 管理员

新建管理员角色

新建管理员角色， 在全局配置模式下，使用如下命令：

admin role *role-name*

- **role-name** – 指定管理员角色的名称。长度范围是 4 到 95 个字符。执行该命令后，系统创建指定名称的管理员角色，并且进入管理员角色配置模式；如果指定的管理员角色名称已经存在，则直接进入管理员配置模式。

使用 **no admin role** *role-name* 命令删除指定的管理员角色。

指定管理员角色的权限

指定管理员角色的 CLI 权限，在管理员角色配置模式下，使用如下命令：

cli-privilege all {rw | none}

- **rw | none** – **rw** 表示管理员角色对全部 CLI 具有读写权限；**none** 表示管理员角色不具有 CLI 权限，不可使用 CLI 命令。

指定管理员角色的 WebUI 权限，在管理员角色配置模式下，使用如下命令：

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

- *module-name* – 指定模块名称。获取完整的模块列表，在 **ui-privilege** 命令后输入问号(?)。
- **none | r | rw** – 对指定的模块设置相应的权限。**none** 表示对模块无权限，管理员角色无法在 WebUI 查看到此模块； **r** 表示对模块具有读权限，可在 WebUI 查看此模块配置，但无法修改配置； **rw** 表示对模块具有读写权限，可在 WebUI 查看并修改模块的配置。

使用 **no ui-privilege** *module-name* 命令取消对此模块的权限设置。

指定管理员角色的描述信息

指定管理员角色的描述信息，在管理员角色配置模式下，使用如下命令：

description *description*

- *description* – 指定描述信息标示此管理员角色。长度范围是 0 到 255 个字符。

使用 **no description** 命令删除描述信息。

创建管理员

创建管理员并进入管理员配置模式，请在全局配置模式下输入以下命令：

admin user *user-name*

- *user-name* - 指定管理员名称。长度范围是 4 到 31 个字符。执行该命令后，系统创建指定名称的管理员，并且进入管理员配置模式；如果指定的管理员名称已经存在，则直接进入管理员配置模式。

在全局配置模式下使用 **no admin user** *user-name* 命令删除指定的管理员。

在管理员配置模式下，用户可以配置管理员角色、管理员密码、访问方式和系统审计员可管理日志类型。

配置管理员角色

配置管理员角色，在管理员配置模式下输入以下命令：

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

- **admin** - 指定管理员角色为系统管理员（Administrator）。
- **operator** - 指定管理员角色为系统操作员（Operator）。
- **auditor** - 指定管理员角色为系统审计员（Auditor）。
- **admin-read-only** - 指定管理员角色为系统管理员(只读)(Administrator-read-only)。

配置管理员密码

Hillstone 设备具有密码策略。请为管理员指定符合密码策略的密码。指定管理员密码，在管理员配置模式下，输入以下命令配置管理员的密码：

password *password*

- *password* – 指定管理员的密码。范围是 4 到 31 个字符。

在管理员配置模式下使用 **no password** 命令取消管理员密码的配置。

系统允许当前登录的系统操作员、系统审计员或系统管理员（只读）修改自身密码，在任意模式下使用以下命令：

exec admin user password update *password*

- *password* – 指定管理员的新密码，为 4 到 31 个字符的字符串。

注意：系统管理员可以修改所有管理员的密码。

配置管理员密码策略

管理员密码策略中可以配置管理员密码的复杂度。密码复杂度包括密码的总长度、密码中组成

元素的长度以及密码的有效期。其中组成元素包括以下 4 种类型：

- 大写字母（从 A 到 Z）。
- 小写字母（从 a 到 z）。
- 数字（从 0 到 9）。
- 其他可见字符。例如：分号（;）、斜杠（/）等字符（仅支持半角字符）。

管理员密码策略的配置需要在管理员密码策略配置模式下进行。进入管理员密码策略配置模式，在全局配置模式下，使用以下命令：

password-policy

如果系统默认的管理员密码复杂度设置无法满足安全性的需求，用户可以自定义密码复杂度。自定义密码复杂度前，用户必须先开启复杂度检测功能。

开启或关闭管理员密码的复杂度检测功能，在管理员密码策略配置模式下，使用以下命令：

admin complexity {**enable | disable**}

- **enable | disable** – 开启或关闭管理员密码的复杂度检测功能。默认情况下，管理员密码的复杂度检测功能为关闭状态。开启后，该功能默认要求密码中必须包含以下各项：两个大写字母、两个小写字母、两个数字和两个特殊字符（例如“@”等）。

用户自定义密码组成元素长度，在管理员密码策略配置模式下，使用以下命令：

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

- **capital-letters** *value* – 指定管理员密码中大写字母的长度。默认值是 2 个字符，范围是 0 到 16。
- **non-alphanumeric-letters** *value* – 指定管理员密码中其他可见字符的长度。默认值是 2 个字符，范围是 0 到 16。
- **numeric-characters** *value* – 指定管理员密码中数字的长度。默认值是 2 个字符，范围是 0 到 16。
- **small-letters** *value* – 指定管理员密码中小写字母的长度。默认值是 2 个字符，范围是 0 到 16。

用户自定义管理员密码的最小长度，在管理员密码策略配置模式下，使用以下命令：

admin min-length *length-value*

- **min-length** *length-value* – 指定管理员密码的最小长度。默认值是 4 个字符，范围是 4 到 16 个字符。当开启管理员密码的复杂度检测功能时，最小长度的默认值为 8 个字符（两个大写字母、两个小写字母、两个数字和两个特殊字符），范围是 8 到 16 个字符。

注意：无论管理员密码的复杂度检测功能是否开启，用户都可以配置管理员密码的最小长度，以提高密码的安全性。

密码的有效期用来限制管理员密码的使用时间。当用户登录时，如果用户输入已经过期的密码，系统将提示重新设置密码，回车后再次输入新密码。如果输入的新密码不符合密码复杂度要求，或连续两次输入的新密码不一致，系统将要求用户重新输入。连续输入三次不符合要求的密码系统将会断开连接，用户重新登录时系统仍要求用户设置新密码。用户设置的新密码可以和旧密码相同。

用户自定义管理员密码的有效期，在管理员密码策略配置模式下，使用以下命令：

admin password-expiration *value*

password-expiration *value* – 指定管理员密码的有效期。单位为天，范围是 0 到 365 天，默认值是 0，表示不对有效期进行限制。在管理员密码策略配置模式下，使用 **no admin complexity** 命令恢复管理员密码的复杂度检测功能的默认情况。

显示管理员密码策略信息

用户可以在任何模式下，随时使用 show 命令查看管理员密码策略信息：

show password-policy

配置管理员访问方式

默认情况下，新建的管理员不可以访问 Hillstone 设备进行配置。用户需指定管理员的访问方式。系统只允许系统管理员指定其他角色的管理员的访问方式。在管理员配置模式下，输入以下命令配置管理员的访问方式：

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

- **console** – 指定管理员通过 Console 访问。
- **http** – 指定管理员通过 HTTP 访问。
- **https** – 指定管理员通过 HTTPS 访问。
- **ssh** – 指定管理员通过 SSH 访问。
- **telnet** – 指定管理员通过 Telnet 访问。
- **any** – 指定管理员可以通过以上任何一种方式访问。

使用多条该命令为管理员指定多种访问方式。

使用 **no access** {**console** | **http** | **https** | **ssh** | **telnet** | **any**}命令取消指定的访问方式。

配置系统审计员可管理日志类型

系统审计员只允许对日志信息进行查看、导出和清除，可管理的日志类型需要系统管理员来指定。在管理员配置模式下，输入以下命令配置系统审计员可管理日志类型：

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

- **config** – 指定系统审计员可管理配置日志信息。
- **event** – 指定系统审计员可管理事件日志信息。
- **nbc** – 指定系统审计员可管理 NBC 日志信息。
- **ips** – 指定系统审计员可管理 IPS 日志信息。
- **traffic** – 指定系统审计员可管理流量日志信息。
- **network** – 指定系统审计员可管理网络日志信息。
- **security** – 指定系统审计员可管理安全日志信息。

使用多条该命令为管理员指定多种可管理的日志类型。

使用 **no log** {**config** | **event** | **nbc** | **ips** | **traffic** | **network | security**} 命令取消指定的系统审计员可管理日志类型。

配置管理员登录限制

管理员使用某一账户登录设备时，密码输入错误次数超过设定次数时，系统会在指定时间内禁止使用该账户登录设备。指定禁止访问时长，在全局配置模式下，使用以下命令：

admin lockout-duration *time*

- **lockout-duration** *time* – 指定禁止访问时长。单位为分钟。范围是 1 到 65535。默认值是 2 分钟。

使用 **no admin lockout-duration** 命令恢复管理员登录时长默认配置。

指定密码输入错误最大次数，在全局配置模式下，使用以下命令：

admin max-login-failure *times*

- **max-login-failure** *times* – 指定管理员密码输入错误最大次数。默认值是 3，范围是 1 到 256。

使用 **no admin max-login-failure** 命令恢复管理员密码输入错误次数默认配置。

注意：只允许系统管理员配置管理员登录限制。

显示管理员角色的配置

显示管理员角色的配置：**show admin role** [*role-name*]

显示管理员配置

用户可以在任何模式下，随时使用 show 命令查看管理员配置：

- 显示管理员信息：**show admin user**
- 显示管理员具体配置信息：**show admin user** *user-name*
- 显示管理员禁止访问时长配置信息：**show admin lockout-duration**
- 显示管理员密码输入错误最大次数配置信息：**show admin max-login-failure**

VSYS 管理员

每个 VSYS 都拥有自己独立的管理员。管理员的角色分为系统管理员（Administrator）、系统管理员 (只读) (Administrator-read-only)、系统操作员 (Operator) 和系统审计员 (Auditor) 四种。关于如何配置管理员及管理员角色，请参阅“配置管理员”。

创建 VSYS 管理员并进行相关配置时，需要遵循以下原则：

- 管理员名称中不能包含“\”符号。
- 根 VSYS 中的系统管理员登录后，进入根 VSYS，可以切换到非根 VSYS 并对该非根 VSYS 进行配置。
- 非根 VSYS 中的管理员登录后，进入到该非根 VSYS，不能进入根 VSYS。
- 每个 VSYS 的管理员名称仅在本 VSYS 中唯一，两个不同 VSYS 中可以有相同名称的管理员，登录时，必须在用户名中指定所属 VSYS，格式为“*vsys_name\admin_name*”，如果不指定所属 VSYS，默认为根 VSYS。

下表为 VSYS 管理员的详细权限列表。

表 2：VSYS 管理员权限列表

功能	权限							
	根 VSYS 系统管理员	根 VSYS 系统管理员（只读）	根 VSYS 系统操作员	根 VSYS 系统审计员	非根 VSYS 系统系统管理员	非根 VSYS 系统管理员（只读）	非根 VSYS 系统操作员	非根 VSYS 系统审计员

功能	权限							
	根 VSYS 系统管理员	根 VSYS 系统管理员（只读）	根 VSYS 系统操作员	根 VSYS 系统审计员	非根 VSYS 系统系统管理员	非根 VSYS 系统管理员（只读）	非根 VSYS 系统操作员	非根 VSYS 系统审计员
配置(包括保存配置)	√	X	√	X	√	X	√	X
管理员配置	√	X	X	X	√	X	X	X
恢复出场配置	√	X	X	X	X	X	X	X
删除配置文件	√	X	√	X	√	X	√	X
回退起始配置信息	√	X	√	X	√	X	√	X
重启设备	√	X	√	X	X	X	X	X
查看配置信息	√	√	√	X	只能查看自己当前 VSYS 配置信息	只能查看自己当前 VSYS 配置信息	只能查看自己当前 VSYS 配置信息	X
查看日志信息	√	√	X	√	√	√	X	√
修改当前管理员密码	√	√	√	√	√	√	√	√
`import` 命令	√	X	√	X	√	X	√	X
`export` 命令	√	√	√	√	√	√	√	√
`clear` 命令	√	√	√	√	√	√	√	√
`ping/traceroute` 命令	√	√	√	X	√	√	√	X
`debug` 命令	√	√	√	X	X	X	X	X
`exec` 命令	√	√	√	√	√	√	√	√
`terminal width` 命令	√	√	√	√	√	√	√	X

配置可信主机

Hillstone 设备使用可信主机来进一步保证系统安全。管理员可以指定一个 IP 地址范围，在该指定范围内的主机为可信主机。只有可信主机才可以对 Hillstone 设备进行管理。

默认情况下，Hillstone 设备的可信主机范围是 0.0.0.0/0，即所有主机都是可信主机。所有

可信主机列表中可信主机范围都是有效的。因此，建议用户在创建好合适的可信主机后，将系统原有的“0.0.0.0/0”可信主机范围删除。

注意：如果远程主机不能访问 Hillstone 设备，请检查 Hillstone 设备的可信主机配置。

配置系统的可信主机，在全局配置模式下，使用以下命令：

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** – 指定可信主机的 IP 地址范围，例如，1.1.1.1 255.255.0.0。**any** 表示任何 IP 地址。
- **http** | **https** | **ssh** | **telnet** | **any** – 指定可信主机的登录类型。**any** 表示可以使用 HTTP、HTTPS、SSH 和 Telnet 任意一种类型登录。

用户可以配置多条该命令添加多个可信主机范围。系统最多允许配置 128 条可信主机范围。

使用 **no admin host** *A.B.C.D A.B.C.D* 命令取消可信主机的指定。

使用 **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** }取消对可信主机特定登录类型的指定。

显示可信主机配置

用户可以在任何模式下，随时使用 show 命令查看可信主机配置：

show admin host

配置 NetBIOS 名字解析功能

StoneOS 支持 NetBIOS 名字解析功能。开启该功能后，系统将自动获取设备所管理网络的所有主机注册的 NetBIOS 主机名，并将其记录在设备缓存中，用于为设备其他功能模块提供 IP 地址到 NetBIOS 主机名的查询服务。

当前版本，系统仅为流量日志的查询提供该功能。开启 NetBIOS 名字解析功能是流量日志中主机名称显示的前提条件。如何使流量日志中显示主机名称，请《监控》的“设置流量日志的主机名称/用户名称的显示状态”。

配置 NetBIOS 名字解析功能，请按照以下步骤进行操作：

1. 开启安全域的 NetBIOS 主机名查询功能。该安全域不能为连接 WAN 网的安全域。
2. 根据统计集统计的信息（IP 地址）系统将自动进行 NetBIOS 查询。

查询过程可能会持续一段时间，查询结果将添加到 NetBIOS 缓存表中。系统每隔一段时间会重新进行一次查询并更新查询结果。

注意：只有开启了 NetBIOS 设置的 PC 才可以被查询到其主机名称。请参阅 PC 操作系统的详细说明来获得开启 NetBIOS 功能的方法。

开启 NetBIOS 主机名查询功能

开启安全域的 NetBIOS 主机名查询功能，在安全域配置模式下，使用以下命令：

nbt-cache enable

在安全域配置模式下使用该命令 no 的形式关闭该功能：

no nbt-cache enable

说明：使用 **zone** *zone-name* 命令进入安全域配置模式。

查询指定 IP 的 NetBIOS 主机名

用户可以通过指定主机的 IP 地址，实时查看该主机的 NetBIOS 主机名称和 MAC 地址。在全局配置模式下，使用以下命令：

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

- *ip-address* – 指定被查询的主机的 IP 地址。
- **vrouter** *vrouter-name* – 指定被查询的主机所属的 VR 名称。如果没有指定 VR，系统使用默认 VR，即 trust-vr。

清除 NetBIOS 缓存数据

清除 NetBIOS 缓存数据，在全局配置模式下，使用以下命令：

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

- *ip-address* – 指定 IP 地址。配置该参数，系统将清除与指定 IP 地址相关的 NetBIOS 缓存数据。如果不配置该参数，系统将清除所有 NetBIOS 缓存数据。
- **vrouter** *vrouter-name* – 指定 VR 名称。配置该参数，系统将清除属于指定 VR 的 NetBIOS 缓存数据。如果没有指定 VR，系统将清除所有 VR 下的 NetBIOS 缓存数据。

查看 NetBIOS 缓存数据

在任何模式下，使用以下命令查看 NetBIOS 缓存数据，包括 IP 地址、主机名称、MAC 地址以及 VR 信息：

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

- *ip-address* – 指定 IP 地址。配置该参数，系统将显示与指定 IP 地址相关的 NetBIOS

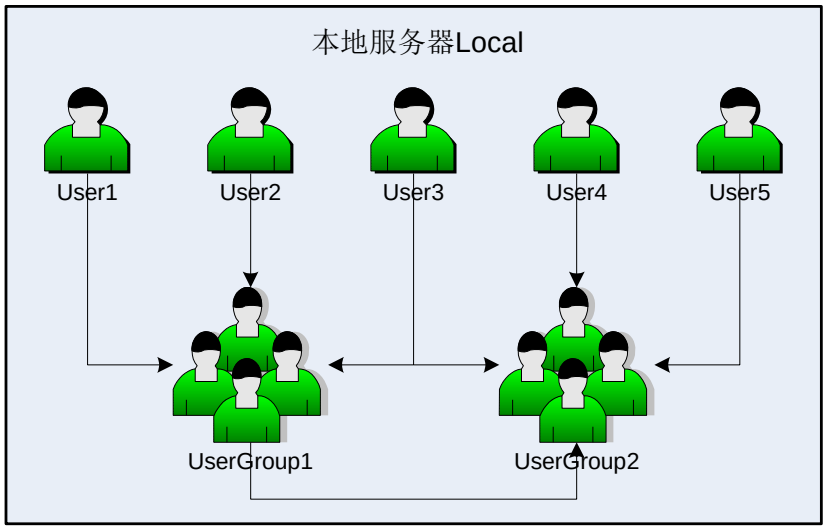
缓存数据。如果不配置该参数，系统将显示所有 NetBIOS 缓存数据。

- **vrouter** *vrouter-name* – 显示属于指定 VR 的 NetBIOS 缓存数据。如果没有指定 VR，系统将显示所有 VR 下的 NetBIOS 缓存数据。

系统用户管理

StoneOS 中的用户（User）是指使用 Hillstone 设备设备提供的功能、服务、被设备认证、管理的用户。被设备认证的用户有本地和外部两种。本地用户（Local User）由系统管理员创建，分属于不同的本地认证服务器，储存在系统的配置文件中；外部用户（External User）储存在外部服务器上，例如 RADIUS 服务器、LDAP 服务器。为方便管理用户，系统支持用户组功能，属于同一本地认证服务器的用户可以划分到不同的用户组中，并且同一个用户可以同时属于不同的用户组，属于同一个本地认证服务器的用户组可以划分到不同的用户组中，并且同一个用户组可以同时属于不同的用户组。下图以缺省本地 AAA 认证服务器“Local”的用户配置说明用户以及用户组关系：

图 1：用户及用户组关系图解



如上图所示，用户 User1、User2 和 User3 均属于用户组 UserGroup1，而 User3 又同时属于用户组 UserGroup2，UserGroup2 中还包含 User4、User5 以及用户组 UserGroup1。

角色拥有某些特定的权限，例如某角色可以访问某指定网络资源或者某角色可以独享一定带宽等。在 StoneOS 系统中，用户与权限并不直接关联，而是需要通过角色把二者联系起来。角色映射规则定义角色和用户的对应关系，功能配置中，为不同的角色指定不同的服务，由此，角色对应的用户即可拥有其角色的服务。StoneOS 支持角色组合，即通过对角色进行“与”、“或”逻辑运算，将角色进行组合。被不同功能模块引用的角色对应的用户将是经过运算后的角色对应的用户。

StoneOS 支持以下基于角色的功能：

- 基于角色的策略规则：实现不同用户的访问控制。
- 基于角色的 QoS：实现不同用户的带宽控制。
- 基于角色的统计集：统计不同用户的带宽、会话数以及新建会话速率。
- 基于角色的会话限制：实现对特定用户的会话数限制。
- SCVPN 基于角色的主机安全检测：实现不同用户对特定资源的访问控制。
- 基于角色的策略路由：实现根据不同源用户选择路由。

用户配置

用户配置包括静态绑定用户的配置和系统认证用户的配置。

配置静态绑定用户

在全局配置模式下，使用以下命令将 IP 地址或 MAC 地址绑定到用户：

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

- *aaa-server-name* – 指定用户所属的 AAA 服务器名称。
- *user-name* – 指定用户名称。
- **ip** *ip-address* – 指定 IP 地址。
- **auth-check-only** – 配置了该参数后，系统在对用户进行认证之前将会先检查该用户 IP 地址的合法性，即检查是否与该用户绑定的 IP 地址一致。如果一致，则允许对用户进行认证。
- **vrouter** *vr-name* – 指定 IP 地址或 MAC 地址所属的 VRouter 的名称。默认为缺省 VR，即 trust-vr。
- **mac** *mac-address* – 指定 MAC 地址。

在全局配置模式下，使用该命令 no 的形式取消将 IP 地址或 MAC 地址绑定到用户：

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

配置认证用户

用户可以为不同的本地 AAA 服务器配置用户或者用户组。进入本地 AAA 认证服务器配置模式，在全局配置模式下使用 **aaa-server** *aaa-server-name* **type local** 命令。创建本地用户，

在本地 AAA 服务器配置模式下，使用以下命令：

user *user-name*

- *user-name* – 指定用户名称。长度范围是 1 到 63 个字符。

执行该命令后，系统创建指定名称的用户并且进入用户配置模式；如果指定的用户名称已存在，则直接进入用户配置模式。在本地 AAA 服务器配置模式下，使用该命令 no 的形式删除指定用户：

no user *user-name*

用户配置可分三类，分别是

- 用户基本配置：用户密码配置、用户过期时间配置、用户描述以及用户组配置。
- 拨号 VPN 相关配置：IKE ID 配置
- PnPVPN 相关配置：DNS 服务器配置、WINS 服务器配置、DHCP 地址池 IP 地址配置、DHCP 地址池网络掩码配置、DHCP 地址池网关配置以及隧道路由配置。具体配置命令，请参阅《防火墙》的“网络参数”。

指定用户密码

指定用户密码，在用户配置模式下，使用以下命令：

password *password*

- *password* – 指定用户的密码。长度范围是 1 到 31 个字符。

在用户配置模式下使用该命令 no 的形式取消密码的配置：

no password

指定用户有效期

超过有效期的用户不可以通过设备的认证，因此不可以在系统中继续使用。默认情况下，用户没有有效期限制。指定用户的有效期，在用户配置模式下，使用以下命令：

expire *Month/day/year HH:MM*

- *Month/day/year HH:MM* – 指定用户有效期时间，格式为“月/日/年 小时:分钟”。例如命令 **expire 02/12/2010 12:00** 表示用户将在 2010 年 2 月 12 日的 12：00 过期。

在用户配置模式下使用该命令 no 的形式取消用户有效期配置：

no expire

配置用户描述信息

为用户提供描述信息，在用户配置模式下，使用以下命令：

desc *string*

- *string* – 指定描述信息，范围是 1 到 31 个字符。

在用户配置模式下，使用该命令 no 的形式取消用户描述信息的指定：

no desc

指定 IKE ID

对于拨号 VPN 用户，需要为其指定 IKE ID。指定 IKE ID，在用户配置模式下，使用以下命令：

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

- **fqdn** *string* – 指定使用 FQDN（Fully Qualified Domain Name）类型的 IKE ID。*string* 为 ID 的具体内容。
- **asn1dn** *string* – 指定使用 Asn1dn 类型的 ID，该类型只可应用于使用证书的情况。*string* 为 ID 的具体内容。
- **key-id** *string* – 指定使用 Key ID 类型的 ID。该类型仅应用于 XAUTH 功能。

在用户配置模式下使用该命令 no 的形式取消 IKE ID 的配置：

no ike_id

指定用户组

用户可以根据不同类别组织到不同的用户组中。同一个用户可以同时属于多个用户组。为用户指定用户组，在用户配置模式下，使用以下命令：

group *user-group-name*

- *user-group-name* – 指定系统中已配置的用户组的名称。长度范围是 1 到 127 个字符。

配置多条该命令为同一用户指定多个用户组。

在用户配置模式下使用该命令 no 的形式取消用户组的指定：

no group *user-group-name*

提示：关于如何配置用户组，请参阅下一节“用户组配置”。

显示用户/用户组信息

在任何模式下，使用以下命令查看用户或用户组的信息。

- 查看系统中所有用户的信息：
  show user
- 查看系统中的用户信息：
  show user aaa-server *server-name* [**name** *user-name*]
- 查看静态绑定用户的信息：
  show user-binding aaa-server *server-name*
- 查看系统中的用户组信息：
  show user-group aaa-server *server-name*

用户组配置

用户可以为不同的本地 AAA 服务器配置用户或者用户组。进入本地 AAA 认证服务器配置模式，在全局配置模式下使用 **aaa-server** *aaa-server-name* **type local** 命令。创建本地用户组，在本地 AAA 服务器配置模式下，使用以下命令：

user-group *user-group-name*

- *user-group-name* – 指定用户组名称。

执行该命令后，系统创建指定名称的用户组并且进入用户组配置模式；如果指定的用户组名称已存在，则直接进入用户组配置模式。在本地 AAA 服务器配置模式下，使用该命令 no 的形式删除指定用户：

no user-group *user-group-name*

在用户组配置模式下，使用以下命令为用户组添加成员，用户组成员可以是用户或者其它的用户组：

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

- *user-name* – 指定用户的名称。
- *user-group-name* – 指定用户组的名称。系统支持的用户组的嵌套层数最多为 5 层，并且不支持回环嵌套，用户组不可以再嵌套它所属的用户组。

配置多条该命令为用户组添加多个成员。

在用户组配置模式下，使用该命令 no 的形式将成员从用户组中删除：

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

角色配置

角色配置包括：

- 创建角色
- 配置角色映射规则
- 配置角色组合

创建角色

创建角色，在全局配置模式下使用以下命令：

role *role-name*

- *role-name* – 指定角色名称。长度范围是 1 到 31 个字符。

在全局配置模式下使用该命令 no 的形式删除指定的角色：

no role *role-name*

配置角色映射规则

角色映射规则表达式指定角色与用户或者用户组的映射关系。系统最多支持 64 条角色映射规则，每个规则中最多可以包含 256 条映射条目。

当 SCVPN 用户以“只用 USB Key”方式登录并通过认证时，系统可以根据 USB Key 数字证书中的证书名称（证书 CN 字段）或者组织机构（证书 OU 字段）为用户映射相应的角色。关于如何只用 USB Key 证书进行认证的详细信息，请参阅《VPN》的“配置客户端 USB Key 证书认证”。

配置角色映射规则，需要首先进入角色映射规则配置模式，在全局配置模式下，使用以下命令：

role-mapping-rule *rule-name*

- *rule-name* – 指定角色映射规则的名称。长度范围是 1 到 31 个字符。执行该命令后，系统创建指定名称的角色映射规则，并且进入角色映射规则配置模式。如果指定的名称已存在，则直接进入角色映射规则配置模式。

在全局配置模式下使用该命令 no 的形式删除指定的角色映射规则：

no role-mapping-rule *rule-name*

在角色映射规则配置模式下，使用以下命令配置角色映射条目：

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* – 指定映射条目中的用户、用户组、证书名称或者组织机构。**any** 表示系统中任何用户、用户组、证书名称或者组织机构。
- **role** *role-name* – 指定用户、用户组、证书名称或者组织机构相对应的角色名称。

配置多条该命令添加多个映射条目。

在角色映射规则配置模式下使用该命令 no 的形式删除指定的映射条目：

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

配置角色组合

Hillstone 设备支持角色组合，即通过逻辑运算重新组合已有角色。配置角色组合，在全局配置模式下使用以下命令：

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

- [**not**] *r1* – 指定表达式中的第一个角色。**not** 表示“非”； *r1* 为系统中已创建的角色名

称。例如，**not testrole1** 表示的结果为非 testrole1 以外的所有角色。

- **and** | **or** – 指定运算符符号。**and** 表示“和”；**or** 表示“或”。
- [**not**] *r2* – 指定表达式中的第二个角色。**not** 表示“非”； *r2* 为系统中已创建的角色名称。
- **role** *r3* – 指定角色运算的结果角色。**role** 关键字为推导符，*r3* 为结果角色名称。

在全局配置模式下使用该命令 no 的形式删除指定的角色表示式：

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

显示角色信息

用户可以在任何模式下使用 show 命令查看角色信息。

- 显示角色信息：**show role**
- 显示角色映射信息：**show role-mapping-rule** [*rule-name*]
- 显示角色组合信息：**show role-expression**

配置管理接口

Hillstone 设备支持 Console、Telnet、SSH 以及 WebUI 方式的访问。用户可以配置各种访问方式的超时时间、端口号以及 HTTPS 的 PKI 信任域。

使用 Telnet、SSH、HTTP 或者 HTTPS 方式登录设备时，如果在一分钟内连续三次登录失败，系统会将登录失败的 IP 地址锁定两分钟。被锁定的 IP 地址在两分钟内不能建立与设备的连接。

配置 Console 管理接口

Console 管理接口的配置包括波特率配置和超时时间配置。

配置波特率

在任何模式下，使用以下命令设置 Console 口的波特率：

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

- **9600** | **19200** | **38400** | **57600** | **115200** – 指定 Console 口波特率，单位为 bps，默认值为 9600bps。

需要注意的是，完成波特率配置后，用户在通过 Console 口登录设备时需保证波特率与设备 Console 口所作配置一致。

配置超时时间

如果在超时时间内未通过 Console 口进行任何配置，系统将断开此次 Console 连接。配置 Console 超时时间，在全局配置模式下，使用以下命令：

console timeout *timeout-value*

- *timeout-value* – 指定 Console 超时时间，单位为分钟。范围是 0 到 60 分钟，0 表示无时间限制。默认值是 10 分钟。

在全局配置模式下，使用该命令 no 的形式恢复 Console 超时默认值：

no console timeout

配置 Telnet 管理接口

用户可以配置 Telnet 的超时时间以及 Telnet 端口号。使用 Telnet 方式连接设备时，使用的端口号必须与此处配置的端口号一致。同时，用户还可以配置 Telnet 最大登录次数。

如果已经建立的 Telnet 连接在超时时间内未发送 Telnet 请求,系统将断开此次 Telnet 连接。配置 Telnet 超时时间，在全局配置模式下，使用以下命令：

telnet timeout *timeout-value*

- *timeout-value* – 指定 Telnet 超时时间，单位为分钟。范围是 1 到 60 分钟。默认值是 10 分钟。

在全局配置模式下，使用该命令 no 的形式恢复 Telnet 超时默认值：

no telnet timeout

配置 Telnet 最大会话数，在全局配置模式下，使用以下命令：

telnet max-session *max-session*

- *max-session* – 指定 Telnet 最大会话数。范围是 1 到 X，不同平台 *X* 的取值不同。默认值为 X。

在全局配置模式下，使用该命令 no 的形式恢复 Telnet 默认会话数：

no telnet max-session

配置 Telnet 端口号，在全局配置模式下，使用以下命令：

telnet port *port-number*

- *port-number* – 指定 Telnet 端口号。范围是 1 到 65535。默认值是 23。

在全局配置模式下，使用该命令 no 的形式恢复 Telnet 默认端口号：

no telnet port

Telnet 最大登录次数，是指允许用户连续失败登录的最大次数。如果连续登录失败次数超出该指定数值，系统将断开此次 Telnet 连接。配置 Telnet 最大登录次数，在全局配置模式下，使用以

下命令：

telnet authorization-try-count *count-number*

- *count-number* – 指定最大连接次数。范围是 1 到 10 次。默认为 3 次。

在全局配置模式下，使用该命令 no 的形式恢复 Telnet 默认登录次数：

no telnet authorization-try-count

配置 SSH 管理接口

用户可以配置 SSH 超时时间以及端口号。并且可以指定 SSH 连接的间隔时间。

如果已经建立的 SSH 连接在超时时间内未发送 SSH 请求，系统将断开此次 SSH 连接。配置 SSH 超时时间，在全局配置模式下，使用以下命令：

ssh timeout *timeout-value*

- *timeout-value* – 指定 SSH 超时时间，单位为分钟。范围是 1 到 60 分钟。默认值是 10 分钟。

在全局配置模式下，使用该命令 no 的形式恢复 SSH 默认超时时间：

no ssh timeout

配置 SSH 最大会话数，在全局配置模式下，使用以下命令：

ssh max-session *max-session*

- *max-session*– 指定 SSH 最大会话数。范围是 1 到 X，不同平台 *X* 的取值不同。默认值为 X。

在全局配置模式下，使用该命令 no 的形式恢复 SSH 默认会话数：

no ssh max-session *max-session*

配置 SSH 端口号，在全局配置模式下，使用以下命令：

ssh port *port-number*

- *port-number* – 指定 SSH 端口号。范围是 1 到 65535。默认值是 22。

在全局配置模式下，使用该命令 no 的形式恢复 SSH 默认端口号：

no ssh port

用户可以指定设备处理 SSH 连接的时间间隔。建立一个 SSH 连接后，在时间间隔过后，设备才接受下一个 SSH 连接请求。配置 SSH 连接时间间隔，在全局配置模式下，使用以下命令：

ssh connection-interval *interval-time*

- *interval-time* – 指定时间间隔，单位是秒。范围是 2 到 3600 秒。默认值是 2 秒。

在全局配置模式下，使用该命令 no 的形式恢复 SSH 连接默认端时间间隔：

no ssh connection-interval

配置 WebUI 管理接口

用户可以通过 HTTP 和 HTTPS 方式访问设备，进行配置。配置 WebUI 超时时间，在全局配置模式下，使用以下命令：

web timeout *timeout-value*

- *timeout-value* – 指定 WebUI 超时时间，单位为分钟。范围是 1 到 1440 分钟。默认值是 10 分钟。

在全局配置模式下，使用该命令 no 的形式恢复 WebUI 超时默认值：

no web timeout

指定 HTTP 端口号，在全局配置模式下，使用以下命令：

http port *port-number*

- *port-number* – 指定 HTTP 端口号。当使用 HTTP 方式访问设备时，浏览器的 HTTP 端口号必须与此处指定的端口号一致。范围是 1 到 65535。默认值是 80。

在全局配置模式下，使用该命令 no 的形式，恢复默认 HTTP 端口号：

no http port

配置防跨站脚本攻击（anti-xss）服务，在全局配置模式下，使用以下命令：

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

- **disable** | **enable**– 启用和禁用防跨站脚本攻击服务。默认情况下，防跨站脚本攻击服务为启用状态。
- **mode** {**normal**| **strict**}–指定防跨站脚本攻击服务模式。包括字符匹配模式（**normal**）和正则表达式匹配模式（**strict**）。

在全局配置模式下，使用该命令 no 的形式，恢复防跨站脚本攻击（anti-xss）服务默认值：

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

指定 HTTPS 端口号，在全局配置模式下，使用以下命令：

https port *port-number*

- *port-number* – 指定 HTTPS 端口号。当使用 HTTPS 方式访问设备时，浏览器的 HTTPS 端口号必须与此处指定的端口号一致。范围是 1 到 65535。默认值是 443。

在全局配置模式下，使用该命令 no 形式恢复默认 HTTPS 端口号：

no https port

指定 HTTPS 方式访问时使用的 PKI 信任域，在全局配置模式下，使用以下命令：

https trust-domain *trust-domain-name*

- *trust-domain-name* – 指定已配置的 PKI 信任域的名称。当 HTTPS 启动时，HTTPS 服务器将使用指定 PKI 信任域中的证书。默认情况下，系统将使用缺省 PKI 信任域 trust_domain_default。

在全局配置模式下，使用该命令 no 的形式恢复默认 PKI 信任域：

no https trust-domain

显示管理接口配置

用户可以在任何模式下，随时使用 show 命令查看管理接口配置信息。命令如下：

- 显示 Console 配置：**show console**
- 显示 Telnet 配置：**show telnet**
- 显示 SSH 配置：**show ssh**
- 显示 Web 配置：**show http**

配置存储设备

Hillstone 设备提供许可证控制的网络行为控制功能。该功能在对用户的网络访问行为进行控制和管理的同时，也对用户的网络行为进行全面记录，记录到的日志信息可以以数据库文件的方式保存到本地数据库中。

能够保存本地数据库的存储设备包括 SD 存储卡、U 盘和 Hillstone 山石网科提供的存储扩展模块。目前只有部分型号的 Hillstone 设备配有 SD 卡槽、USB 接口或支持存储扩展模块的扩展槽。

格式化存储设备

当存储设备不能正常运行、Hillstone 设备不支持存储设备的磁盘文件系统或存储设备未被格式化时，用户可以通过格式化存储设备的方法修复存储设备的故障、更改磁盘文件系统和格式化存储设备。

格式化存储设备，请在任何模式下输入以下命令：

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

- **sd0** – 对 SD 卡槽内插入的 SD 存储卡进行格式化操作。
- **usb0** | **usb1** – 对与指定 USB 口相连的存储设备进行格式化操作。
- **storage***X* – 对指定的存储扩展模块进行格式化操作。*X* 为插入存储扩展模块的扩展槽号，不同平台 *X* 的取值范围不同。

注意：格式化操作会删除存储设备上的所有数据，请自行备份重要文件。

安全删除存储设备

如果用户在信息传输的过程中强行拔下或弹出存储设备，可能会造成数据丢失，导致日志信息存储不全。为了保证数据传输的完整性，请在任何模式下输入以下命令，安全删除存储设备：

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

- **sd0** – 安全删除 SD 卡槽内插入的 SD 存储卡。
- **usb0** | **usb1** – 安全删除指定 USB 口相连的存储设备。
- **storage***X* – 安全删除指定的存储扩展模块。*X* 为插入存储扩展模块的扩展槽号，不同平台 *X* 的取值范围不同。

配置文件管理

Hillstone 设备的配置信息都被保存在系统的配置文件中。用户通过运行相应的命令或者访问相应的 WebUI 页面查看 Hillstone 设备的各种配置信息，例如 Hillstone 设备的初始配置信息和当前配置信息等。配置文件以命令行的格式保存配置信息，并且也以这种格式显示配置信息。

配置 Hillstone 设备配置信息

用户可以查看和保存 Hillstone 设备的配置信息，也可以导出和导入配置信息。

注意：导出配置信息时，系统本地用户的密码信息不会同时导出。关于如何导出本地用户的密码信息，请参阅《VPN》的“导出和导出密码文件“。

查看配置信息

配置文件中保存的用来初始化 Hillstone 设备的配置信息称作起始配置信息，Hillstone 设备通过读取起始配置信息进行启动时的初始化工作；如果找不到起始配置信息，Hillstone 设备则使用 Hillstone 设备的缺省参数初始化。与起始配置信息相对应，Hillstone 设备运行过程中正在生效的配置称为当前配置信息。

系统起始配置信息包括系统的当前起始配置信息（系统启动时使用的配置信息），和系统的备份起始信息。系统纪录最近十次保存的配置信息，最近一次保存的配置信息会纪录为系统的当前起始配置信息，当前系统配置信息以“startup”作为标记。前九次的配置信息按照保存时间的先后以数字 0 到 8 作为标记。

查看 Hillstone 设备的当前起始配置信息，在任何命令模式下输入以下命令：**show**

configuration [**startup**]

查看设备的备份起始信息，在任何命令模式下使用以下命令：

show configuration backup *number*

- *number* – 备份起始信息的数字标记。

查看设备的当前配置信息，在任何命令模式下输入以下命令：

show configuration

查看设备的当前接口配置信息，在任何命令模式下输入以下命令：

show configuration interface [*interface-name* | **last** *number*]

- *interface-name* – 指定显示配置信息的接口名称。
- **last** *number* – 指定显示配置信息的接口条目数。显示从倒数指定数值的条目开始到最后条目的接口配置信息。如果指定数值大于所有接口条目数，则显示所有接口配置信息。

查看设备的备份起始信息记录，在任何命令模式下输入以下命令：

show configuration record

查看设备的当前运行的配置信息记录，在任何命令模式下输入以下命令：

show configuration running

查看设备的当前地址簿配置信息，在任何命令模式下输入以下命令：

show configuration address [**last** *number*]

- **last** *number* – 指定显示配置信息的地址簿条目数。显示从倒数指定数值的条目开始到最后条目的地址簿配置信息。如果指定数值大于所有地址簿条目数，则显示所有地址簿配置信息。

查看设备的当前策略配置信息，在任何命令模式下输入以下命令：

show configuration policy [**last** *number*]

- **last** *number* – 指定显示配置信息的策略条目数。显示从倒数指定数值的条目开始到最后条目的策略配置信息。如果指定数值大于所有策略条目数，则显示所有策略配置信息。

查看设备的当前路由配置信息，在任何命令模式下输入以下命令：

show configuration vrouter [**last** *number*]

- **last** *number* – 指定显示配置信息的路由条目数。显示从倒数指定数值的条目开始到最后条目的路由配置信息。如果指定数值大于所有路由条目数，则显示所有路由配置信息。

以 xml 方式输出当前配置信息，在任何命令模式下输入以下命令：

show configuration xml

回退配置信息

回退配置信息，系统支持以下两种方式：

在执行模式下，使用以下命令回退起始配置信息。系统能够纪录最近十次保存的起始配置信息，

用户可以根据需要回退到已保存的指定的起始配置信息。系统将在重启后使用指定的起始配置信息。

rollback configuration backup *number*

- *number* – 备份起始配置信息的数字标记。

在配置回滚模式下，使用以下命令回退配置信息并退出配置回滚模式。用户不需要重启设备，该配置直接生效。

exec configuration rollback

注意：在执行模式下，使用 **exec configuration start** 进入配置回滚模式。

示例:

```
hostname# exec configuration start （进入配置回滚模式）
hostname[TRN]# configure （进入全局配置模式）
..... （进行任意配置，且所做配置即时生效）
hostname[TRN](config)# exec configuration rollback （回退配置并退出配置回滚模式）
hostname#
```

退出配置回滚模式

直接退出配置回滚模式，系统支持以下两种方式：

在配置回滚模式下，使用以下命令直接退出配置回滚模式：

exec configuration commit

示例:

```
hostname# exec configuration start （进入配置回滚模式）
hostname[TRN]# configure （进入全局配置模式）
..... （进行任意配置，且所做配置即时生效）
hostname[TRN](config)# exec configuration commit （直接退出配置回滚模式）
hostname#
```

在配置回滚模式下，使用 **exit** 命令直接退出登录终端，从而退出配置回滚模式。

说明:

- 当不同用户同时登录设备时，先进入配置回滚模式的用户可以继续配置操作，其他用户无法进行配置操作。
- 当相同用户通过不同访问方式登录设备时，先进入配置回滚模式的某访问方式的用户可以继续配置操作，其他访问方式的用户无法进行配置操作，但其可以使用 **exec configuration commit** 或者 **exec configuration rollback** 命令强制进入配置回滚模式的某访问方式的用户退出配置回滚模式。

配置退出配置回滚模式的动作

当使用 **exit** 命令退出配置回滚模式时，默认情况下，系统会直接退出配置回滚模式。回退配

置后退出配置回滚模式，在全局配置模式下，使用以下命令：

cli-exit-action rollback

恢复直接退出配置回滚模式，在全局配置模式下，使用以下命令：

cli-exit-action commit

删除配置文件

用户可以删除设备的起始配置信息。删除起始配置信息，在执行模式下，使用以下命令：

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

- **startup** – 删除当前起始配置信息。
- **backup** *number* – 删除指定的备份起始配置信息，number 为备份起始配置信息的数字标记。

保存配置信息

用户可以保存 Hillstone 设备的当前配置信息使其成为 Hillstone 设备下次启动时的起始配置。保存 Hillstone 设备的当前配置信息，在任何命令模式下输入以下命令：

save [*string*]

- *string* – 对所保存配置信息的描述。如果不使用 *string* 对保存的配置文件进行描述，系统会直接覆盖原有配置文件。

自动备份配置文件

用户可以通过配置自动备份配置文件功能，能够实现设备定期检查配置文件，在当前配置文件发生变化时，系统会自动将当前的配置文件上传到 FTP 或 TFTP 服务器上。

指定自动备份配置文件到 FTP 服务器，在全局配置模式下，使用以下命令：

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

- *ip-address* - 指定 FTP 服务器的 IP 地址。
- **user** *user-name* **password** *password* – 指定访问 FTP 服务器的用户名和密码。
- **vrouter** *vrouter-name* – 指定 VRouter 的名称。
- **path** *path* – 指定配置文件的上传路径。
- **interval** *time-value* – 指定自动备份配置文件的时间间隔。单位为小时，默认值是 1 小时。范围是 1 到 7*24 小时。如果不指定该参数，系统将每 1 小时检查配置文件，在发生

变化时，自动备份到 FTP 服务器上。

在全局配置模式下，使用 **no configuration auto-backup ftp** 取消自动备份配置文件到 FTP 服务器。

指定自动备份配置文件到 TFTP 服务器，在全局配置模式下，使用以下命令：

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

在全局配置模式下，使用 **no configuration auto-backup tftp** 取消自动备份配置文件到 TFTP 服务器。

查看自动备份配置文件信息

查看自动备份配置文件功能的信息，在任何命令模式下输入以下命令：

show configuration auto-backup

导出配置信息

用户可以导出系统的当前配置信息和备份配置信息到 FTP 服务器、TFTP 服务器或者 U 盘。

导出系统配置信息到 FTP 服务器，在执行模式下使用以下命令：

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

- **startup** | **backup** *number* – 指定导出的配置信息。**startup** 为导出当前配置信息；*number* 为导出以 *number* 为标识的备份配置信息。
- *ip-address* – 指定 FTP 服务器的 IP 地址。
- *vrouter-name* – 导出指定 VRouter 的配置信息。
- **user** *user-name* **password** *password* – 指定访问 FTP 服务器的用户名和密码。
- *file-name* – 指定导出的配置信息文件的名称。

导出系统配置信息到 TFTP 服务器，在执行模式下使用以下命令：

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

导出系统配置信息到 U 盘，在执行模式下使用以下命令：

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

导入配置信息

用户可以通过 FTP 和 TFTP 服务器导入配置信息，也可以将配置信息放入 U 盘中，通过设备

的 USB 口导入配置信息。

从 FTP 服务器导入配置信息，在执行模式下使用以下命令：

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

- *ip-address* – 指定 FTP 服务器的 IP 地址。
- **user** *user-name* **password** *password* – 指定 FTP 服务器的用户名和密码。
- *vrouter-name* – 为指定的 VRouter 导入配置信息。
- *file-name* – 指定导入的配置信息文件的名称。

从 TFTP 服务器导入配置信息，在执行模式下使用以下命令：

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

从 U 盘导入配置信息，在执行模式下使用以下命令：

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

恢复出厂配置

用户除使用设备上的 CLR 按键使系统恢复到出厂配置外，也可以使用命令恢复。恢复出厂配置，在任何模式下，使用以下命令：

unset all

注意：小心使用该命令。执行该命令后，设备的所有配置将被清除。

切换接口工作模式

部分 Hillstone 设备支持对 IOM-2Q8SFP+、IOM-8SFP+和 IOC-8SFP+模块切换接口工作模式，接口工作模式包括 40G、10G 和 1G 接口模式。可以实现以下功能：

- 将 40G 接口分成 4 个 10G 接口，实现 40G 接口与 10G 接口互联。
- 使 10G 接口工作在 1G 接口工作模式下，实现 10G 接口与 1G 接口互联。

40G 接口默认工作模式为 40G，在接口配置模式下，使用以下命令将 40G 接口工作模式切换为 10G：

channel-speed 10000

10G 接口默认工作模式为 10G，在接口配置模式下，使用以下命令将 10G 接口工作模式切换为 1G,：

channel-speed 1000

在接口配置模式下，使用 **no channel-speed** 命令恢复接口工作模式。

注意：

- 在指定接口工作模式前，需要删除接口相关配置。
- IOC-8SFP+模块接口工作模式只有 10G 和 1G 模式，且只支持将 10G 接口工作模式切换为 1G。

删除模块扩展槽配置信息

在部分 Hillstone 设备（SG-6000-X6150、SG-6000-X6180、SG-6000-X7180）运行过程中，由于各种原因，用户需要更换扩展模块或者拔出扩展模块。Hillstone 设备支持模块卡的热插拔操作，可以保证整个系统不间断运行。

由于模块扩展槽配置信息的依赖关系比较复杂，对于 IOM 模块，执行热插拔操作时，用户需要使用 **exec unset slot** {*number*}命令检查并删除模块扩展槽的配置信息，使模块正常初始化。

删除模块扩展槽的配置信息，在执行模式下，使用以下命令：

exec unset slot *slot-number*

- *slot-number* – 指定 IOM 模块所在的槽位号。取值范围为 1-128。

执行该命令后，根据具体情况，系统会出现不同的提示信息。用户可根据提示信息的描述选择下一步操作。

注意：

- 如果模块扩展槽存在接口配置依赖关系，用户必须先手动删除接口配置依赖关系后，再执行该命令删除模块扩展槽的配置信息。
- SCM 模块、 SSM 模块或 QSM 模块进行热插拔操作时，则无需执行该命令。

查看当前对象的配置信息

当用户在某一配置模式下完成指定对象的配置之后，用户可以当前配置模式下，使用 **show this** 命令查看当前对象的配置信息。

下表列出了目前系统支持查看当前配置信息的对象名称和配置模式：

表 3：查看当前配置信息模式提示符

对象名称	配置模式	配置模式提示符
管理员	管理员配置模式	hostname(config-admin)#
AAA 服务器	AAA 服务配置模式	hostname(config-aaa-server)#
接口	接口配置模式	hostname(config-if-eth0/0)#
安全域	安全域配置模式	hostname(config-zone-trust)#
地址簿	地址配置模式	hostname(config-addr)#

服务	服务配置模式	hostname(config-service)#
服务组	服务组配置模式	hostname(config-svc-group)#
策略路由	PBR 策略配置模式	hostname(config-pbr)#
VRouter	VRouter 配置模式	hostname(config-vrouter)#
为 trust-vr 配置 NAT	NAT 配置模式	hostname(config-nat)#

查看光口模块状态信息

查看光口模块状态信息，包括功率、温度、电压以及模块类型。在任何命令模式下输入以下命令：

show transceiver *[interface-name]*

- *interface-name* – 指定光口模块接口名称。

删除虚拟网卡配置信息

对于虚拟化安全产品云·界，如果用户在信息传输的过程中强行移除虚拟网卡，可能会造成数据丢失或其他异常情况。为了保证数据传输的完整性，删除虚拟网卡时，请按照以下步骤进行：

- 首先，在任何模式下输入以下命令，关闭网卡：

  exec detach-port port *port-number*

  - *port-number* – 指定的需要关闭的虚拟网卡的接口号。即用户在设备上查看接口信息时，Etherent0/X 的“X”的值。

  执行完成上述命令后，相应的接口的物理/协议/连接等状态将变为 Down 状态（通过 **show interface** 命令查看）。

- 然后，在虚拟管理器上移除虚拟网卡。
- 最后，在执行模式下，使用以下命令删除虚拟网卡的配置信息，使模块正常初始化：

  exec unset-port port *port-number*

  - *port-number* – 指定需要删除配置信息的虚拟网卡的接口号。即用户在设备上查看接口信息时，Etherent0/X 的“X”的值。此处 X 数值需与 **exec detach-port port** 命令的端口号保持一致。

  执行完上述命令后，用户即安全删除完成虚拟网卡。

注意：

- 禁止删除接口 ethernet0/0，否则将导致产品的许可证失效。
- 云·界最多可支持 10 块虚拟网卡，虚拟网卡对应的接口号将按照插入顺序递增，直到达到 10 个接口。当用户在接口之间删除一个接口，即产生一个空位后，若再新插入一块虚

拟网卡，新网卡的接口号将继承原空位上的接口号。

配置 Banner 功能

Banner 用于显示登录后的声明信息，用户可以自定义 Banner 信息内容。在全局配置模式下，使用以下命令配置 Banner 功能：

admin login-banner *Banner-content*

- *Banner-content* – 指定 Banner 信息内容，长度范围是 1 到 4096 个字符。执行该命令后，系统创建指定内容的 Banner 信息；如果已存在 Banner 信息，则将 Banner 信息内容修改为指定内容。

使用 **no admin login-banner** 命令删除 Banner 信息内容，显示为空。

注意：

- 在编辑 Banner 信息内容时，如果需要换行，需输入“\n”;需要空格，需输入双引号“”。
- 仅支持在使用 SSH、Telnet 或者 Console 方式登录设备时显示 Banner 信息。

系统维护与调试

Hillstone 设备支持网络连接测试工具 Ping 和 Traceroute，当网络出现问题时，用户可以用这些工具对网络进行测试，查找故障原因。Hillstone 设备同时具有调试功能，供用户查阅与分析。

Ping 命令

Ping 命令主要用于检查网络连接状态以及主机是否可达。用户可以随时在任何 CLI 命令模式下使用 Ping 命令，检查网络连接状态及主机是否可达。其使用方法为：

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

- *ip-address* | *hostname* – 指定接受 Ping 报文的目的地址，可以是 IP 地址，也可以是主机名称。在双栈系统固件下，可以是 IPv6 地址。
- **count** *number* – 指定发送 Ping 包的个数。范围是 1 到 65535。默认情况下，系统不限制发送 Ping 包的个数。
- **size** *number* – 指定发送 Ping 包的大小。范围是 28 到 65500 字节（byte）。
- **source** *ip-address* – 指定发送 Ping 包的源地址，只能是接口名称。
- **timeout** *time* – 指定发送 Ping 包的超时时间。范围是 0 到 3600 秒。默认值是 0，即为没有超时时间限制。
- **vrouter** *vrouter-name* – 指定发送 Ping 包的出接口所属的 VRouter。默认为缺省 VR，

即 trust-vr。

命令输出结果包括以下两部分：

- 对每个 ping 报文的响应情况。如果在超时时间到后仍没有收到响应报文，则输出 Destination Host Not Responding 等，否则显示响应报文中报文序号、TTL 和响应时间；如果 ping 包没有到达目的路由或发送 ping 包的接口发生变化，则输出 Network is unreachable；如果接受 Ping 报文的目的地址无法解析时，则输出 unknown host *hostname*。
- 最后的统计信息，包括发送报文数、接收报文数、未响应报文百分比、命令执行时间和响应时间的最小、平均、最大和平均偏差值。

以下是 Ping 命令使用示例：

```
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
```

Traceroute 命令

Traceroute 用于测试数据包从发送主机到目的地所经过的网关。它主要用于检查网络连接是否可达，以及分析网络什么地方发生了故障。Traceroute 通常的执行过程是：首先发送一个 TTL 为 1 的数据包，因此第一跳发送回一个 ICMP 错误消息以指明此数据包不能被发送（因为 TTL 超时），之后此数据包被重新发送，TTL 为 2，同样第二跳返回 TTL 超时，这个过程不断进行，直到到达目的地。执行这些过程的目的是记录每一个 ICMP TTL 超时消息的源地址，以提供一个 IP 数据包到达目的地所经历的路径。

用户可以随时在任何 CLI 命令模式下使用 Traceroute 命令测试数据包经过的网关。其使用方法为：

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

- *ip-address* | *hostname* – 指定 traceroute 命令的目的地址，可以是 IP 地址，也可

以是主机名称。

- **numberic** - 指定用数字的方式显示地址，而不对地址进行解析。
- **port** *port-number* – 指定 UDP 端口号。范围是 1 到 65535。默认端口号为 33434。
- **probe** *probe-number* – 指定 traceroute 命令在每一跳发出的探测包的数目。范围是 1 到 65535。默认值是 3。
- **timeout** *time* – 指定发送下一个探测包的超时时间。范围是 1 到 3600 秒。默认值是 5 秒。
- **ttl** [*min-ttl*] [*max-ttl*] – *min-ttl* 用来指定最小 TTL 值，范围是 1 到 255，默认值是 1。*max-ttl* 用来指定最大 TTL 值，范围是 1 到 255，默认值是 30。指定 TTL 值，用来显示 *min-ttl* 跳到 *max-ttl* 跳的回显。
- **source** *interface* – 指定发送 traceroute 探测包的源地址，只可以是源接口名称。
- **use-icmp** – 指定使用 ICMP 包进行探测。如不配置该参数，系统将使用 UDP 包进行探测。
- **vrouter** *vrouter-name* – 指定发送 traceroute 探测包的出接口所属的 VRouter。默认为缺省 VRouter，即 trust-vr。

以下是使用 traceroute 命令分析网络情况的示例：

```
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  * * *
```

从以上示例结果中可以看出，从源主机到目的主机经过了哪些网关，以及哪些网关出现了故障。

系统调试功能

系统调试功能可以帮助用户对错误进行诊断和定位。Hillstone 设备的各种协议和功能基本上

都具有相应的调试功能。默认情况下，所有协议和功能的系统调试功能都是关闭的。用户只可以通过 CLI 对系统调试功能进行配置。开启 Hillstone 设备的系统调试功能，请在任何模式下输入以下命令：

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

- **all**– 开启 Hillstone 设备所有协议和功能的系统调试功能。
- *function-name* – 开启 Hillstone 设备指定协议或功能的系统调试功能。

在任何配置模式输入以下命令关闭所有或指定功能的系统调试功：

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

用户还可以通过双击“ESC”键关闭 debug 功能。由于部分信息被缓存，关闭过程可能会持续几分钟。

查看调试功能开启或者关闭状态，请在任何模式下输入以下命令：

show debug

注意：调试功能开启后，如果需要在终端输出 debug 信息，请开启系统的 debug 日志功能（执行 **logging debug on** 命令）。

收集并保存技术支持信息到文件

为了便于定位系统故障，系统支持收集 **show** 相关命令的显示信息，并保存成 tech-support 文件。收集并保存技术支持信息到文件，在任意模式下，使用以下命令：

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

- *cpu-number* –收集并保存指定 CPU 的技术支持信息到文件。该参数仅在多 CPU 系统中显示。
- **all** –收集并保存所有技术支持信息到文件。该参数仅在多 CPU 系统中显示。

注意：单 CPU 系统直接通过 **show tech-support** 命令收集并保存所有技术支持信息到文件。

显示技术支持信息

显示技术支持信息到 Console 口，在任意模式下，使用以下命令：

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

- *cpu-number* – 显示指定 CPU 的技术支持信息到 Console 口。该选项仅在多 CPU 系统中显示。
- **all** –显示所有技术支持信息到 Console 口。该选项仅在多 CPU 系统中显示。

注意：单 CPU 系统直接通过 **show tech-support toconsole** 命令显示技术支持信息到 Console 口。

自动收集技术支持信息

配置系统自动收集技术支持信息，在任意模式下，使用以下命令：

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

- *interval-time* - 指定自动收集技术支持信息的间隔时间。取值范围为 10 到 1440。单位为分钟。
- *count-time* – 指定自动收集信息技术支持信息的次数。取值范围为 1 到 10 次。

注意：

- 系统最多可以保存 10 个 tech-support 文件，当生成的文件个数超过 10 个时，新生成的文件会从头开始覆盖老的文件。
- 当配置完成并执行该命令时，如果再次配置自动收集技术支持信息，新的配置会覆盖之前的配置。

显示 nvramlog 或 watchdoglog 日志信息

显示 tech-support 文件中的 nvramlog 或者 watchdoglog 日志信息，在任意模式下，使用以下命令：

show tech-support *log-name*

- *log-name* - 指定需要显示的日志信息的名称。可以指定为 nvramlog 或者 watchdoglog。

删除自动收集技术支持信息功能

删除配置的自动收集技术支持信息的功能，在任意模式下，使用以下命令：

show tech-support-auto clear

配置系统重启

在 Hillstone 设备运行过程中，由于各种原因，如系统文件升级等，用户需要重启 Hillstone 设备。用户可以通过下电再重新上电重启 Hillstone 设备，也可以通过 CLI 或者 WebUI 重启 Hillstone 设备。

重启 Hillstone 设备，请在执行模式下使用 reboot 命令重启。请参阅以下示例：

```
hostname# reboot
System configuration has been modified. Save? [y]/n （键入字母“y”或者敲回车键，系统将保存配置；键入字母“n”，系统将不保存配置）
Building configuration..
```

```
Saving configuration is finished
System reboot, are you sure? y/[n]  (键入字母“y”，系统将重启；键入字母“n”或者敲回车键，系统将返回到执行模式)
```

执行 reboot 命令时，系统首先会提示用户是否保存先前所做的配置。请谨慎使用 reboot 命令，因为执行该命令会导致网络工作在短时间内中断。

StoneOS 版本升级

用户在使用 Hillstone 设备的过程中，有时需要升级 Hillstone 设备的系统固件 StoneOS 的版本。本节介绍 Hillstone 设备的启动系统以及 StoneOS 的升级方法。

启动系统介绍

Hillstone 设备的启动系统分为三个部分，分别是 Bootloader、Sysloader 和 StoneOS。它们各自的作用如下：

- Bootloader – Hillstone 设备上电后最先运行的程序。Bootloader 装载执行 StoneOS 或者 Sysloader。
- Sysloader - 升级 StoneOS。
- StoneOS – Hillstone 设备的操作系统软件。

系统启动后，Bootloader 尝试启动 StoneOS 或者 Sysloader。StoneOS 是 Hillstone 设备的操作系统软件。Sysloader 实现 StoneOS 的更新和选择，支持 FTP、TFTP 以及直接通过 USB Host 接口升级。Sysloader 本身的升级由 Bootloader 通过 TFTP 下载完成。

Bootloader 的工作模式

Bootloader 有两种工作模式，分别是**自动模式**和**交互模式**。

自动模式下 Bootloader 试图启动配置的 StoneOS，如果没有 StoneOS 或者 StoneOS 不合法，系统将终止运行，此时用户必须使用 Sysloader 升级 StoneOS。

用户在启动时根据提示按下“ESC”键后，Bootloader 进入交互模式。交互模式的主要功能是启动 Sysloader。在交互模式下，可以选择启动保存在 Flash 中的 Sysloader，也可以通过 TFTP 下载新的 Sysloader 然后启动。

通过网络迅速升级 StoneOS（TFTP）

Sysloader 可以从 TFTP 服务器获取 StoneOS，从而保证用户能够通过网络迅速升级 StoneOS。请按照以下步骤进行操作：

给设备上电并且进入 Sysloader。参照以下操作提示：

```
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  （5 秒倒计时结束前按“ESC”键）
Run on-board sysloader? [y]/n: y  （键入字母“y”或者敲回车键）
Loading: ##########################
```

从 Sysloader 的操作选择菜单选择通过 TFTP 升级 StoneOS。参照以下操作提示：

```
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  （在此处键入“1”并敲回车键）
```

依次配置 Sysloader 的 IP 地址、TFTP 服务器的 IP 地址、网关 IP 地址以及 StoneOS 名称。参照以下操作提示：

```
Local ip address     [     ]: 10.2.2.10/16（输入 Sysloader 的 IP 地址并敲回车键）
Server ip address    [     ]: 10.2.2.3（输入 TFTP 服务器的 IP 地址并敲回车键）
Gateway ip address   [     ]: 10.2.2.1（如果 Sysloader 与 TFTP 服务器的 IP 地址不属于同一个网段，输入网关的 IP 地址并敲回车键；否则直接敲回车键）
File name   : StoneOS-3.5R2（输入 StoneOS 名称并敲回车键，系统开始通过 TFTP 获取 StoneOS）
#################################################################
#################################################################
##########
```

保存 StoneOS。参照以下操作提示：

```
File total length 10482508
Checking the image...
Verified OK
Save this image? [y]/n: y（键入字母“y”或者敲回车键，保存获得的 StoneOS）
Saving ..........................................
Set StoneOS-3.5R2 as active boot image
```

重启。系统将使用新的 StoneOS 启动。参照以下操作提示：

```
Please reset board to boot this image
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（在此处键入“6”并敲回车键，系统开始重启）
```

设备的 Flash 中最多可以储存两个 StoneOS。如果 Flash 中已经保存了两个 StoneOS，请根据提示对储存的 StoneOS 进行删除。

其它升级方式

通过网络从 TFTP 服务器获取 StoneOS 进行升级是最常用的升级方式，同时 Hillstone 设备还支持从 FTP 服务器获取 StoneOS。另外，用户还可以将 StoneOS 放入 U 盘，通过设备的 USB Host 接口进行升级。

通过 FTP 服务器获取 StoneOS

请按照以下步骤在 Sysloader 中通过 FTP 升级 StoneOS：

1. 进入 Sysloader 后，从 Sysloader 的操作选择菜单中选择“2”并敲回车键。
2. 配置 Sysloader 的 IP 地址。在“Local ip address [ ]:”后输入为 Sysloader 配置的 IP 地址。敲回车键。
3. 配置 FTP 服务器的 IP 地址。在“Server ip address [ ]:”后输入 FTP 服务器的 IP 地址。敲回车键。
4. 如果 Sysloader 与 FTP 服务器的 IP 地址不属于同一个网段，请配置 Sysloader 的网关 IP 地址。在“Gateway ip address [ ]:”后输入网关的 IP 地址。敲回车键。

5. 在“User Name [anonymous]:”后输入 FTP 用户名。敲回车键。
6. 在“Password :”后输入用户名对应的密码。敲回车键。
7. 在“File name :”后输入 StoneOS 文件名称。敲回车键。系统开始通过 FTP 获取指定的 StoneOS。
8. StoneOS 传输完成后，系统将会询问是否保存该 StoneOS。键入字母“y”，系统将把该 StoneOS 保存到设备的 Flash 中。
9. 保存成功后，系统再次出现 Sysloader 的操作选择菜单，选择“6”并敲回车键。系统开始使用新的 StoneOS 重新启动。

说明：对于匿名 FTP 服务器，在“User Name [anonymous]:”和“Password :”后直接敲回车键（第 5 步和第 6 步）。

通过 USB 口获取 StoneOS

请按照以下步骤在 Sysloader 中通过设备的 USB 接口升级 StoneOS。

将 StoneOS 拷贝到 U 盘的根目录下。

将 U 盘插入设备的 USB 接口中。

进入 Sysloader 后，从 Sysloader 操作选择菜单中选择“3”并敲回车键。

在正确的 StoneOS 后输入“y”，系统开始从 U 盘获取 StoneOS。

StoneOS 传输完成后，系统将会询问是否保存该 StoneOS。键入字母“y”，系统将把该 StoneOS 保存到设备的 Flash 中。

保存成功后，系统再次出现 Sysloader 的操作选择菜单，选择“6”并敲回车键。系统开始使用新的 StoneOS 重新启动。

Sysloader 菜单介绍

Sysloader 使用菜单提示的方式帮助用户完成指定的操作。本节介绍 Sysloader 中各菜单项的功能。关于 Sysloader 的菜单选项和功能，请参阅下表：

表 4：Sysloader 菜单选项与功能

菜单选项	功能
1 Load firmware via TFTP	通过 TFTP 升级 StoneOS。
2 Load firmware via FTP	通过 FTP 升级 StoneOS
3 Load firmware from USB disks	通过 U 盘升级 StoneOS。
4 Select backup firmware as active	选择系统中保存的备份 StoneOS 作为当前的

菜单选项	功能
	StoneOS 启动系统。
5 Show on-board firmware	显示系统中保存的 StoneOS 名称和状态。
6 Reset	重新启动系统。

在“Please select”提示后键入菜单选项相对应的数字，然后按回车键。按照提示进行操作。

通过 CLI 升级 StoneOS

除了可以在 Sysloader 中升级 StoneOS 以外，用户还可以在 CLI 中通过 FTP 服务器、TFTP 服务器或者 U 盘升级 StoneOS。

登录进入 CLI 后，在执行模式下，使用以下命令通过 FTP 服务器升级 StoneOS：

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

- *ip-address* – 指定 FTP 服务器的 IP 地址。
- **user** *user-name* **password** *password* – 指定 FTP 服务器的用户名和密码。
- *vrouter-name* – 通过指定的 VRouter 升级 StoneOS。
- *file-name* – 指定 StoneOS 名称。

登录进入 CLI 后，在执行模式下，使用以下命令通过 TFTP 服务器升级 StoneOS：

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

登录进入 CLI 后，在执行模式下，使用以下命令通过 U 盘升级 StoneOS：:

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

升级 StoneOS 成功后，重启系统使新的 StoneOS 生效。

备份与恢复配置

当系统升级时，为避免因升级失败而导致数据丢失，StoneOS 支持数据备份与恢复功能。该功能可在升级时将数据进行备份；当升级失败后，手动导入数据对其进行恢复，以保证系统的正常运行。目前仅支持将数据备份至指定的 FTP 服务器。仅 T 系列平台支持该功能。

在执行模式下，输入以下命令备份数据到指定的 FTP 服务器：

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

- *ip-address* – 指定 FTP 服务器的 IP 地址。
- **vrouter** *VR-name* – 通过指定的 VR 备份文件。
- **user** *username* **password** *password* – 指定 FTP 服务器的用户名和密码。
- *filename* – 指定导出数据文件的名称。如果不指定，则默认版本名称作为文件名。

在执行模式下，输入以下命令从 FTP 服务器恢复数据：

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

- *ip-address* – 指定 FTP 服务器的 IP 地址。
- **vrouter** *VR-name* – 通过指定的 VR 备份文件。
- **user** *username* **password** *password* – 指定 FTP 服务器的用户名和密码。
- *filename* – 指定导入的数据文件名称。

平滑关闭模块

作为多模块设备，部分 Hillstone 设备（SG-6000-X6150、SG-6000-X6180、SG-6000-X7180）支持对单个硬件模块进行平滑关闭（graceful-shutdown）操作。平滑关闭单个模块不会中断模块上的现有业务，可以保证整个系统的不间断运行。目前设备只支持 SSM 模块和 QSM 模块的平滑关闭。

执行平滑关闭的模块将首先停止接收新流量，在完成已有业务处理后，将状态自动更改为 offline（通过 **show module** 命令查看），此时平滑关闭完成。平滑关闭完成后，用户可以根据需要使用 **reboot slot** {*number*}命令启动模块，使其重新开始处理业务。

平滑关闭某个模块，在执行模式下，使用以下命令：

exec system graceful-shutdown slot {*number*}

- *number* – 指定 SSM/QSM 模块所在的槽位号。取值范围为 1-10。

执行该命令后，根据具体情况，系统会出现不同的提示信息。可能出现的提示信息如下表所示。用户可根据“说明”一栏的描述选择下一步操作。

表 5：平滑关闭的提示及说明

提示信息	说明
Only one SSM is available，the operation is not supported	系统只有一块 SSM，不能执行 SSM 模块升级。
The module is not SSM or QSM. Can’t do the operation	指定槽位的模块不是 SSM/QSM 模块，无法执行 ISSU 升级。
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	指定槽位的模块正在进行平滑关闭，关闭将持续一分钟，期间不要执行任何操作，但可以使用 show system graceful-shutdown status 命令查看状态信息。

重启启动模块，使用 **reboot slot** {number}命令。

提示：平滑关闭命令也适用于 SSM 模块或 QSM 模块的热插拔操作。执行热插拔操作时，用户可以使用该命令关闭模块，然后再拔出模块。

双主控 HA

部分 Hillstone 设备（SG-6000-X6150、SG-6000-X6180、SG-6000-X7180）支持双主控（SCM）HA 功能。当为设备配置两个 SCM 模块时，默认情况下，安装在 SC0 插槽的 SCM 模块为主用主控模块，工作在 Master 模式下，安装在 SC1 插槽的 SCM 模块为备用主控模块，工作在 Slave 模式下。如果设备当前只有一个 SCM 模块，则该 SCM 模块为主用主控模块，为设备安装新的 SCM 模块后，新安装的 SCM 模块为备用主控模块，此时模块的主备和其所在槽位无关。当主用主控模块发生故障时，备用主控模块会自动升级为主用主控模块，保证业务连续畅通。

使用双主控 HA，需要注意以下几点：

- 禁止在备用主控模块上做任何配置。
- 发生主备切换后，新的备用主控模块重启后仍工作在 Slave 模式下，不会进行抢占。
- 主备切换后，需要重新建立 Telnet、HTTP 等管理连接。
- 为保证能够同步许可证信息，安装某些许可证后，系统将会提示用户进行整机重启（断网重启）或者通过 ISSU 方式重启（运行中软件升级）。用户需要根据提示进行操作。

用户可以通过 **`show module`** 命令查看双主控状态。系统将在输出信息中为主用主控模块标注“M”，即 Master，为备用主控模块标注“B”，即 Backup（Slave）。

许可证管理

许可证（license）用来授权用户使用一些功能、服务，或者用来扩展性能。对于基于许可证的功能、服务和性能来说，如果没有购买和安装相应的许可证，该功能和服务就无法使用，或不能达到更高的性能。

系统的许可证的分类和规则如下表：

表 6：平滑关闭的提示及说明

平台许可证	说明	许可证过期
平台试用许可证（Platform Trial）	平台许可证是其他许可证运行的基础，如果平台许可证无效，其他许可证均不生效。设备出厂时已预装 15 天的试用许可证，支持	到期后， 已有的配置不能修改，若设备重启，系统恢复出厂配置。

	功能同正式许可证。	
平台正式许可证（Platform Base）	设备正式销售后，可以安装平台正式许可证。该许可证提供基础防火墙功能和 VPN 功能。	到期后，设备仍可正常使用，但不能升级到期后的 OS 版本。
功能许可证	**说明**	**许可证过期**
VSYS 许可证	授权 VSYS 的可用数量。	无过期。
SSL VPN 许可证	授权 SSL VPN 的最大接入数量。多个 SSL VPN 许可证可以叠加允许接入用户的最大数量。	无过期。
QoS/iQoS 许可证	开启流量管理功能。	到期后，无法使用 QoS/iQoS 的功能升级和维护服务。
WAP 分流许可证	提供 WAP 分流功能。	无过期。
国家商用密码 IPSec VPN 许可证	IPSec VPN 支持使用国家商用密码算法配置。 对于支持该算法的设备， 从 StoneOS 5.5R6 版本开始，系统不需安装国家商用密码 IPSec VPN 许可证即可使用国密算法。	无过期。
沙箱防护许可证	提供沙箱防护功能，授权每天允许上传到云沙箱的可疑文件样本数目，并且提供域名白名单的升级。 分为以下 3 种许可证： • Sandbox-300 许可证：每天允许上传 300 个文件。 • Sandbox-500 许可证：每天允许上传 500 个文件。 • Sandbox-1000 许可证：每天允许上传 1000 个文件。	有效期包括 1 年、2 年、3 年。 过期后，云端分析功能无法使用，不能升级域名白名单。 仅可根据本地数据库缓存结果使用沙箱防护功能，重启设备之后，功能不可用。
Twin-mode 许可证	提供孪生模式功能，控制系统孪生模式相关功能的可见性和可配置性。	过期后，无法使用孪生模式的功能升级和维护服务。
服务许可证	**说明**	**许可证过期**
病毒过滤（AV）许可证	提供病毒过滤功能和病毒特征库的升级。	过期后，不能升级病毒特征库，病毒过滤功能正常使用。
入侵防御（IPS）许可证	提供入侵防御功能和 IPS 特征库升级。	过期后，不能升级 IPS 特征库，入侵防御功能正常使用。
URL DB 许可证	提供 URL 分类库和 URL 分类库的在线查询	过期后，不能提供 URL 分类库

	功能。	的在线查询功能，自定义 URL 和 URL 过滤功能仍正常使用。
APP DB 许可证	提供 APP 库升级功能。APP DB 许可证不需要单独申请，随平台许可证一同发放，有效期也同平台许可证。	过期后不能升级 APP 特征库。
威胁防护（TP） 许可证	打包提供 AV、IPS 功能，和相应特征库的升级。	过期后，不能提供其包含的特征库的升级，功能仍可使用。
PTF 许可证	提供预定义黑名单的边界流量过滤（PTF）功能和 IP 信誉特征库升级。	到期后，系统会自动删除该 IP 信誉特征库，且预定义黑名单功能不能使用。
IP 信誉许可证	提供 IP 信誉的边界流量过滤（PTF）功能和 IP 信誉特征库升级。从 StoneOS 5.5R6 及以后版本，预定义黑名单边界流量过滤功能（由 PTF 许可证提供)升级为 IP 信誉边界流量过滤，用户可购买 IP 信誉许可证进行升级使用。	到期后，系统会自动删除 IP 信誉特征库，且 IP 信誉边界流量过滤功能将不能使用。
StoneShield 许可证	打包提供异常行为检测（ABD）、高级威胁检测（ATD）功能，和相应特征库的升级。	过期后，不能提供其包含的特征库的升级，功能仍可使用。
扩展增强许可证	**说明**	**许可证过期**
AEL 许可证	提高并发会话数量（session）和处理能力（performance）的最大值。	无过期。

申请许可证

请遵循以下流程申请许可证：

生成申请许可证所需的许可证请求。在任何模式使用 **exec license apply applicant** *string* 命令生成许可证请求。具体命令描述，请参考“许可证命令”。

将生成的请求发送给 Hillstone 代理商。

安装许可证

许可证为一串字符串。获得许可证后，用户需要将许可证安装到相应的设备。

在 CLI 中安装许可证，在任何模式下使用 **exec license install** *license-string* 命令。具体命令描述，请参考“许可证命令”。许可证正确安装完后，用户需重启设备以使许可证生效。

注意：StoneOS 允许用户卸载已安装的许可证。但是强烈建议用户**不要**对许可证进行卸载。

连接云·界许可证服务器

云·界产品安装许可证后，需连接到许可证服务器，进行合法性校验，以防止许可证被克隆盗版。目前系统支持两种校验方式，分别是通过互联网连接到公网许可证服务器校验和通过局域网连接到内网 vLMS(虚拟许可证管理系统)校验，用户可根据需要选择其中的一种方式。

通过公网服务器的方式适用于小型私有云或行业云场景。虚拟防火墙连接到公网服务器后，服务器将提供许可证的合法性校验（目前公网服务器暂不提供许可证的分发和管理）。若发现克隆许可证的行为或虚拟防火墙未连接服务器进行校验，虚拟防火墙将会在 30 天后重启。

通过局域网 vLMS 的方式多适用于大型公有云场景。虚拟防火墙连接到 vLMS 后，vLMS 不仅提供许可证的校验，还提供许可证的自动分发和管理。若发现克隆许可证的行为，服务器将回收克隆或被克隆的其中一台虚拟防火墙的全部许可证并重启该虚拟防火墙；若虚拟防火墙不连接服务器进行校验，虚拟防火墙将会在 30 天后重启。

连接许可证服务器，在任何模式下使用以下命令：

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

具体命令描述，请参考“许可证命令”。 安装许可证并连接到许可证服务器后，用户需重启系统以使许可证生效。

提示：关于 vLMS（虚拟许可证管理系统）的更多资料，请参阅云·界《vLMS 虚拟许可证管理系统使用手册》。

许可证命令

本节具体描述申请、安装和卸载许可证所需的命令。

生成许可证请求

生成申请许可证所需的许可证请求，请在任何模式下使用以下命令：

exec license apply applicant *string*

- *string* – 申请人名称。

安装/卸载许可证

获得许可证后，用户可在任何模式下通过使用以下命令安装许可证：

exec license install *license-string*

- *license-string* – 要安装的许可证字符串。

卸载许可证，在任何模式下使用以下命令：

exec license uninstall *license-name*

- *license-name* – 要卸载的许可证名称。

安装许可证后，输入命令 **reboot** 使系统重启。许可证将在重启后生效。

连接云·界许可证服务器

云·界安装许可证后，需要用户连接云.界许可证服务器进行合法性验证，在任何模式下使用以下命令：

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

- **public-server** –指定云·界的许可证服务器为公网服务器。
- **license-server** *A.B.C.D* – 指定云·界的许可证服务器为局域网 vLMS，并指定其 IP 地址。
- **ssl-port** *port-number* – 指定局域网 vLMS 的连接的端口号，取值范围为 1 到 65535。

连接许可证服务器成功后，输入命令 **reboot** 使系统重启。许可证将在重启后生效。

注意：通过公网服务器进行许可证验证时，请保证连接公网服务器的接口在 trust-vr 安全域内并且通过 trust-vr 安全域可以访问互联网。

显示云·界许可证服务器信息

在任意模式下，使用以下命令云·界许可证服务器信息：

show connected license-server

许可证灌装介绍

许可证灌装方法适用于需要给大批设备安装许可证的情况。使用许可证灌装可以简化大批量设备安装许可证的操作步骤，减少错误的发生。

许可证灌装操作

许可证灌装操作步骤如下：

1. 拥有大批量设备的用户提供设备序列号以及需要的许可证类型。具体许可证信息请咨询当地代理商。
2. Hillstone 山石网科获得许可证信息后，生成相应的许可证文件，并将许可证文件通过适当的方式发送给客户，例如通过邮件。
3. 用户获得许可证文件后，将许可证文件拷贝到格式为 FAT32 的 U 盘中，拷贝路径为“\license”。目录名称“license”区分大小写（必须为全部小写）且不可更改。拷贝许可证文件时不可修改许可证书写格式，否则将无法安装许可证。
4. 用户利用存有许可证文件的 U 盘为所有设备安装许可证。具体安装步骤请参考下节内容。

许可证安装

用户将许可证文件拷贝到 U 盘的正确位置后，将 U 盘插入设备的 USB 口，设备将自动扫描 U 盘并安装许可证。用户可以根据指示灯状态判断许可证安装状态。具体步骤如下：

启动设备，进入运行状态（出现“login”提示符）。

将存有许可证文件的 U 盘插入设备的 USB 口。

设备扫描 U 盘信息，寻找与其序列号相同的许可证，找到后自动安装相应的许可证。通过设备的 ALM 指示灯可判断许可证安装状态，指示灯闪烁方式以及含义如下表所示：

表 7：指示灯含义

设备说明	ALM 指示灯状态
设备从 U 盘的“license”目录下中发现匹配的许可证	绿色闪烁持续到许可证安装完成
许可证安装完成	恢复之前状态
设备未从 U 盘的“license”目录下中发现匹配的许可证	红色闪烁保持 10 秒后恢复之前状态
设备未从 U 盘中找到“license”目录	保证原状态不变

许可证安装完毕取出 U 盘，然后用同样的方法为其他设备安装许可证。

U 盘中所有和设备相匹配的许可证都会被自动安装到设备上，同时已经安装的许可证将被自动移动到 U 盘的“license_installed”目录（自动创建）下，避免重新插入 U 盘后再次扫描并安装重复的许可证。

重启设备，使许可证生效。

简单网络管理协议（SNMP）

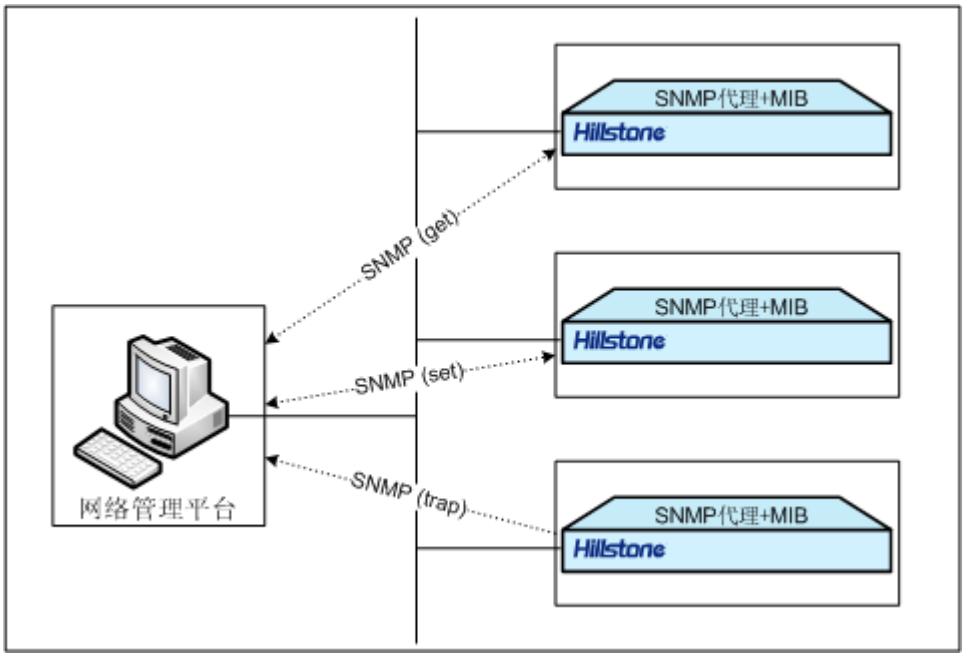
简单网络管理协议（SNMP， Simple Network Management Protocol）是应用层协议，它通过标准框架、公共语言和相对应的安全机制来监控和管理网络设备。SNMP 的体系结构包括网络管理平台、SNMP 代理、网络管理协议和管理信息库(MIB，Management Information Base)四部分。

- 网络管理平台：是一个通过网络管理软件（如 adventnet、solarwinds 等）向 SNMP 代理发出 Get 和 Set 报文并接收代理的应答，以达到管理和监控网络设备目的的系统。
- SNMP 代理：是运行在被管理网络设备上的一个软件模块，用来维护被管理设备的信息数据并在需要时把管理数据发送给网络管理平台。
- 网络管理协议：网络管理平台和 SNMP 代理之间是通过网络管理协议连接的，通过 SNMP 报文的形式来交换信息。协议主要支持 Get、Set 和 Trap 三种功能，Get 用于管理平台获取代理的 MIB 对象值，Set 用于管理平台去设置代理的 MIB 对象值，Trap 用于代理向管理平台通告重要事件。
- 管理信息库（MIB）：是由 SNMP 代理维护的有关网络设备的信息数据库，信息库里的内容可供网络管理平台查询或设置其中变量的值。

Hillstone 设备的 SNMP 功能

Hillstone 设备拥有 SNMP 代理功能，该 SNMP 代理功能能够接受网络管理平台的操作请求并反馈网络和设备的相应信息。下图为 SNMP 管理框架在 Hillstone 设备中实现的示意图：

图 2：SNMP 管理框架在 Hillstone 设备中的实现



SNMP 版本

Hillstone 设备支持以下版本的 SNMP：

- SNMPv1 协议，具体描述请参阅 RFC-1157，A Simple Network Management Protocol。
- SNMPv2 协议，具体描述请参阅 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 协议，具体描述请参阅 RFC2263，SNMPv3 Applications；RFC2264，User-based Security Model (USM) for version 3 of the Simple Network Management Protocol (SNMPv3)；RFC2265，View-based Access Control Model (VACM) for the Simple Network Management Protocol (SNMP)。

SNMPv1 和 SNMPv2c 都使用了团体字的认证方式，可以限制网络管理平台获取设备信息。SNMPv3 引入了基于用户的安全模型用于保证消息安全及基于视图的访问控制模型用于访问控制。

MIB 信息库

Hillstone 设备支持 RFC-1213 中定义的所有相关的管理信息库组（Management Information Base for Network Management of TCP/IP-based Internets: MIB-II）和 RFC-2233 中定义的使用 SMIv2 的接口组 MIB（The Interfaces Group MIB using SMIv2：

IF-MIB)。此外，StoneOS 提供一个私有 MIB 库，MIB 库中包含 Hillstone 设备的系统信息、IPSec VPN 信息以及系统统计信息，用户可以将其导入到管理主机的 MIB 浏览器，进行使用。

Trap 报文信息

Hillstone 设备的 SNMP 代理功能在设备发生异常情况时，会主动向网络管理平台发送 Trap 报文报告所发生的事件。Hillstone 设备的 SNMP 代理可以生成以下各种 trap 信息：

- 热启动 trap
- SNMP 验证失败 trap
- 端口状态改变 trap
- VPN SA 协商状态改变 trap
- HA 状态改变 trap
- 系统状态改变 trap，如 CPU 使用率超过 80%的 trap、风扇状态改变 trap、内存过低 trap 等
- 网络攻击 trap，如 ARP 欺骗攻击 trap、IP 地址欺骗攻击 trap、SYN Flood 攻击 trap 等
- 配置改变 trap

配置 SNMP

Hillstone 设备的 SNMP 的配置包括以下各项：

- 开启或者关闭 SNMP 代理功能
- 配置 SNMP 代理设备端口号
- 配置 SNMP 引擎 ID
- 创建 SNMPv3 用户组
- 创建 SNMPv3 用户
- 配置管理主机地址
- 配置 trap 报文目标主机地址
- 配置管理员的标识及联系方法
- 配置 Hillstone 设备位置
- 指定启用 SNMP 功能的虚拟路由器

开启或者关闭SNMP 代理功能

默认情况下，系统的 SNMP 代理功能是关闭的。开启 Hillstone 设备的 SNMP 代理功能，请在全局配置模式下使用以下命令。用该命令 no 的形式关闭 SNMP 代理功能。

- **snmp-server manager**
- **no snmp-server manager**

配置SNMP 代理设备端口号

配置 SNMP 代理设备端口号，在全局配置模式下，使用以下命令：

snmp-server port *port-number*

- *port-number* – 指定 SNMP 代理设备的端口号。范围为 1 到 65535。默认值为 161。

配置SNMP 引擎ID

SNMP 引擎 ID 唯一标识一个引擎，SNMP 引擎是 SNMP 实体（网络管理平台或者被管理网络设备）的重要组成部分，完成 SNMP 消息的收发、验证、提取 PDU、组装消息与 SNMP 应用程序通信等功能。配置本地设备的 SNMP 引擎 ID，在全局配置模式下使用以下命令：

snmp-server engineID *string*

- *string* – 指定引擎 ID 号。取值范围为 1 到 23 个字符。

创建SNMPv3 用户组

配置 SNMPv3 用户组，请在全局配置模式下使用以下命令：

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

- *group-name* – 指定用户组的名称。取值范围为 1 到 31 个字符。
- **noauth** | **auth** | **auth-enc** – 指定用户组的安全级别。可以为 noAuth、Auth 或者 Auth-Enc。安全级别决定了在处理一个 SNMP 数据包时所采用的安全机制。noAuth 即无认证和加密；Auth 提供基于 MD5 或 SHA 算法的认证；Auth-Enc 提供基于 MD5 或 SHA 算法的认证和基于 AES 和 DES 的报文加密。
- **read-view** *read-view* – 指定该用户组的只读 MIB 视图名。如不指定该参数，系统默认为空。
- **write-view** *writeview* –指定该用户组的可写 MIB 视图名。如不指定该参数，系统默认为空。

系统最多允许配置 5 个用户组，且每个用户组最多可包含 5 个用户。在全局配置模式下使用 **no snmp-server group** *group-name* 命令删除指定的用户组。

创建 SNMPv3 用户

配置 SNMPv3 用户，请在全局配置模式下使用以下命令：

snmp-server user *user-name* **group** *group-name* **v3 remote** *A.B.C.D/M* [**auth-protocol** {**md5** | **sha**} *auth-pass* [**enc-protocol** {**des** | **aes**} *enc-pass*]]

- **user** *user-name* – 指定用户名称。取值范围为 1 到 31 个字符。
- **group** *group-name* – 为所创建的用户指定已经配置好的用户组。
- **remote** *A.B.C.D/M* – 指定远程管理主机的 IP 地址以及掩码。
- **auth-protocol** {**md5** | **sha**} – 指定用户安全级别为需要认证且认证协议可以为 MD5 或 SHA 算法。如不输入此参数，则默认是无认证，无加密模式。
- *auth-pass* – 指定认证密码。取值范围为 8 到 40 个字符。
- **enc-protocol** {**des** | **aes**} – 指定用户安全级别为加密且加密协议为 DES 或者 AES。
- *enc-pass* – 指定加密密码。取值范围为 8 到 40 个字符。

系统最多允许配置 25 个用户。在全局配置模式下使用 **no snmp-server user** *user-name* 命令删除指定的用户。

配置管理主机地址

配置管理主机地址，请在全局配置模式下使用以下命令：

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* – 指定管理主机的 IP 地址或 IP 地址范围。
- **version** [*1* | *2c*] – 指定 SNMP 的版本为 SNMPv1 或者 SNMPv2C。
- **community** *string* –团体字是管理进程和代理进程之间的口令，因此与 Hillstone 设备认可的团体字不符的 SNMP 报文将被丢弃。该参数指定主机的团体字，取值范围为一个最多 31 位的字符串，且仅当 SNMP 为 v1 和 v2C 版本时有效。
- **ro** | **rw** – 指定该团体字的读写权限。ro 为只读，此类团体字只可读取 MIB 中的信息；rw 为可读可写，此类团体字不仅可以读取 MIB 中的信息，还可以对信息进行修改。此项为可选，默认情况下，团体字的访问权限为只读。

- **version** *3* –指定 SNMP 的版本为 SNMPv3。

全局配置模式下使用 **no snmp-server host** {*host-name* | *ip-address* | *ip-address/mask* | **range** *start-ip end-ip*}命令删除指定的管理主机。

配置 trap 报文目标主机地址

用户可以配置接收 SNMP trap 报文的主机。配置 SNMP trap 报文目标主机地址，请在全局配置模式下使用以下命令：

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

- *host-ip* – 指定 trap 报文目标主机的 IP 地址。
- **port** *port-number* – 指定接收 trap 报文的目标主机端口号。取值范围为 1 到 65535，默认值为 162。
- **version** {*1* | *2c*} – 指定使用 SNMPv1 或者 SNMPv2C 发送 trap 报文。
- **community** *string* – 指定 SNMPv1 或者 SNMPv2C 的团体字。
- **version** *3* – 指定使用 SNMPv3 发送 trap 报文。
- **user** *string* – 指定已配置的 SNMPv3 用户名。
- **engineID** *string* – 指定 trap 报文目标主机的引擎 ID 号。
- **port** *port-number* – 指定接收 trap 报文的目标主机端口号。取值范围为 1 到 65535，默认值为 162。

在全局配置模式下使用 **no snmp-server trap-host** {*host-name* | *ip-address*}命令删除指定的 trap 报文目标主机。

配置管理员的标识及联系方法

sysContact 即系统联络，是 MIB II 中系统组的一个管理变量，内容为被管理设备（此处为 Hillstone 设备）相关人员的标识及联系方法。用户可以通过配置此参数，将重要信息存储在 Hillstone 设备中，以便出现紧急问题时查询使用。配置管理员的标识及联系方法，请在全局配置模式下使用以下命令：

snmp-server contact *string*

- *string* – 描述系统联络信息的字符串。取值范围为 1 到 255 个字符。

在全局配置模式下使用 **no snmp-server contact** 命令该系统联系信息。

配置 Hillstone 设备位置

sysLocation 是 MIB 中系统组的一个管理变量，用于表示被管理设备(此处为 Hillstone 设备)的位置。指定 Hillstone 设备的位置，请在全局配置模式下使用以下命令：

snmp-server location *string*

- *string* – 描述 Hillstone 设备位置的字符串。取值范围为 1 到 255 个字符。

在全局配置模式下使用 **no snmp-server location** 命令删除系统位置信息。

指定启用 SNMP 功能的 VRouter

用户可以指定启用 SNMP 功能的 VRouter。指定启用 SNMP 功能的 VRouter，请在全局配置模式下使用以下命令：

snmp-server vrouter *vrouter-name*

- *vrouter-name* –指定 VRouter 的名称。

在全局配置模式下使用 **no snmp-server vrouter** 命令关闭指定 VRouter 的 SNMP 功能。

配置 SNMP 服务器

用户可以配置 SNMP 服务器，从而通过 SNMP 协议来获取相关的 ARP 信息。配置 SNMP 服务器，在全局配置模式下，使用以下命令：

arp-mib-query server *ip-address* **community** *string* [**vrouter** *vrouter-name*] [**source** *interface-name*] [**port** *port-number*] [**interval** *value*]

- *ip-address* – 指定 SNMP 服务器的 IP 地址。
- **community** *string* – 指定 SNMPv1 或者 SNMPv2C 的团体字，取值范围为一个最多 31 位的字符串。
- **vrouter** *vrouter-name* – 指定 VRouter 的名称。
- **source** *interface-name* – 指定 SNMP 服务器上用来接收 ARP 信息的源接口名称。
- **port** *port-number* – 指定 SNMP 服务器的端口号。范围为 1 到 65535。默认值为 161。
- **interval** *value* – 指定 SNMP 服务器上接收 ARP 信息的时间间隔，单位为秒，范围是 5 到 1800 秒，默认值是 60 秒。

在全局配置模式下使用 **no arp-mib-query server** *ip-address* 命令删除指定的 SNMP 服务器。

清除 SNMP 服务器的 ARP 表项信息

用户可以在任何模式下通过以下命令清除 SNMP 服务器的 ARP 表项信息：

clear arp-mib-query

显示 SNMP 信息

用户可以在任何模式下通过以下命令查看 SNMP 的相关配置信息：

- 显示 Hillstone 设备的 SNMP 配置信息：**show snmp-server**
- 显示 Hillstone 设备的 SNMPv3 用户组信息：**show snmp-group**
- 显示 Hillstone 设备的 SNMPv3 用户信息：**show snmp-user**

显示 SNMP 服务器信息

用户可以在任何模式下通过以下命令查看 SNMP 服务器的相关信息：

- 显示 SNMP 服务器状态信息：**show arp-mib-query status**
- 显示 SNMP 服务器的 ARP 表项信息：**show arp-mib-query table** [*ip-address*]
- 显示 SNMP 服务器配置信息：**show configuration arp-mib-query**

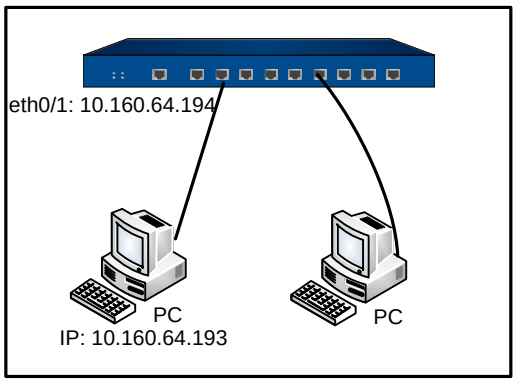
SNMP 配置示例

为方便用户更好的理解和使用 Hillstone 设备的 SNMP 功能，本节介绍两个典型的 SNMP 配置示例。

组网要求

网络管理平台与 Hillstone 设备通过以太网相连，网络管理平台的 IP 地址为 10.160.64.193，Hillstone 设备以太网口 IP 地址为 10.160.64.194。请看以下示意图：

图 3：SNMP 组网图



- 示例一:通过 SNMPv2C 实现 IP 地址为 10.160.64.193 的 PC 对 Hillstone 设备的管理，使用团体字 public。另外，允许向网络管理平台 10.160.64.193 发送 trap 报文，使用团体字 private。
- 示例二：通过 SNMPv3 实现 IP 地址为 10.160.64.193 的 PC 对 Hillstone 设备的管理。安全级别为需要认证和加密，指定认证协议为 MD5、认证密码为 password1，指定加密协议为 DES、加密密码为 password2。同时，PC 只能读取 MIB-II 信息库的内容并且只能对 usm 信息库的内容进行设置。另外，允许向 Hillstone 设备发送 trap 报文。

示例一配置步骤

第一步：配置 Hillstone 设备：

进入全局配置模式

```
hostname# configure
```

启动 Hillstone 设备接口的 SNMP 功能

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# manage snmp
```

启动 SNMP 功能

```
hostname(config)# snmp-server manager
```

配置团体字和访问权限

```
hostname(config)# snmp-server host 10.160.64.193 version 2c community public
ro
```

配置管理员标识、联系方法以及 Hillstone 设备物理位置

```
hostname(config)# snmp-server contact cindy-Tel:218
hostname(config)# snmp-server location Hostname-Network
```

允许向网络管理平台 10.160.64.193 发送 trap 报文，使用的团体字为 private

```
hostname(config)# snmp-server trap-host 10.160.64.193 version 2c community private
```

第二步：配置网络管理平台。

示例二配置步骤

第一步：配置 Hillstone 设备：

进入全局配置模式

```
hostname# configure
```

启动 Hillstone 设备接口的 SNMP 功能

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# manage snmp
```

启动 SNMP 功能

```
hostname(config)# snmp-server manager
```

配置本地引擎 ID

```
hostname(config)# snmp-server engineID hillstone
```

配置用户组，网络管理平台只能读取 MIB-II 信息库的内容并且可以对 usm 信息库的内容进行设置

```
hostname(config)# snmp-server group group1 v3 auth-enc read-view mib2 write-view usm
```

配置用户，认证协议为 MD5，密码为 password1；加密协议为 DES，密码为 password2

```
hostname(config)# snmp-server user user1 group group1 v3 remote 10.160.64.193 auth md5 password1 enc des password2
```

配置管理主机地址

```
hostname(config)# snmp-server host 10.160.64.193 version 3
```

配置 trap 报文目标主机地址，允许向网络管理平台 10.160.64.193 发送 trap 报文

```
hostname(config)# snmp-server trap-host 10.160.64.193 version 3 user user1 engineID remote-engineid
```

配置管理员标识、联系方法以及 Hillstone 设备物理位置

```
hostname(config)# snmp-server contact cindy-Tel:218
hostname(config)# snmp-server location Hostname-Network
```

第二步：配置网络管理平台。

HSM 代理

Hillstone Security Management™，简称为 HSM，是山石网科自主研发的集中网络安全管理系统，能够对网络中的多台 Hillstone 安全设备进行集中控制和管理。HSM 系统分为三部分，即 HSM 代理、HSM 服务器和 HSM 客户端。将这三部分合理部署到网络中，并且实现安全连接后，用户可以通过客户端程序，查看被管理安全设备的日志信息、统计信息、设备属性等，实时监控被管理设备的运行状态和流量信息。

每台 Hillstone 安全设备运行的 StoneOS 都包含 HSM 代理模块，在设备上正确配置了 HSM 代理功能后，就可以实现设备与 HSM 服务器的连接，进而实现服务器对设备的管理与控制。

用户可以通过命令行接口（CLI）和 Web 界面（WebUI）两种方式为 Hillstone 安全设备配置 HSM 代理功能（Hillstone SR 系列安全路由器只支持 WebUI 配置方式）。Hillstone 设备的 HSM 代理功能配置主要包括以下各项：

- 配置 HSM 服务器管理参数
- 指定信任域
- 开启/关闭 HSM 代理功能
- 显示 HSM 代理配置

提示：关于 HSM 的详细信息，请参阅《Hillstone Security Management™ 用户手册》。

配置 HSM 服务器管理参数

为实现设备与 HSM 服务器的连接，使服务器能够对设备进行管理，用户需要在设备上配置服务器的 IP 地址、连接端口号、连接出接口、设备注册模式、访问密码及启用 HSM 代理功能的 VRouter。

配置 HSM 服务器的 IP 地址，在全局配置模式下，使用以下命令：

network-manager host *ip-address*

- *ip-address* – 指定 HSM 服务器的 IP 地址。此 IP 地址不能为“0.0.0.0”、“255.255.255.255”以及组播地址。

配置 HSM 服务器的连接端口号，在全局配置模式下，使用以下命令：

network-manager host port *port-number*

- *port-number* – 指定 HSM 服务器的连接端口号。范围是 1 到 65535。默认值是 9091。

配置 HSM 服务器的连接出接口，在全局配置模式下，使用以下命令：

network-manager host source *interface-name*

- **source** *interface-name* – 指定 HSM 服务器的连接出接口。

指定 HSM 服务器的设备注册模式为普通模式（即非加密模式），在全局配置模式下，使用以下命令：

network-manager host plain

在全局配置模式下，用该命令 no 的形式指定为加密模式：

no network-manager host plain

配置 HSM 服务器的访问密码，在全局配置模式下，使用以下命令：

network-manager host password *password*

- *password* – 指定 HSM 服务器的访问密码。服务器通过该密码对设备进行认证。范围是 1 到 31 个字符。

配置启用 HSM 代理功能的 VRouter，在全局配置模式下，使用以下命令：

network-manager host vrouter *vrouter-name*

- *vrouter-name* –指定 VRouter 的名称。

在全局配置模式下，使用以下命令取消对 HSM 服务器管理参数的配置：

no network-manager host

为保证设备与 HSM 服务器在 NAT 环境下能够正常通信，系统支持用户在设备上配置 FTP 服务器和日志服务器的 IP 地址和端口号。默认情况下，FTP 服务器的 IP 地址为 HSM 服务器的 IP 地址，端口号为 21；日志服务器的 IP 地址为 HSM 服务器的 IP 地址，端口号为 514。

配置 FTP 服务器的 IP 地址和端口号，在全局配置模式下，使用以下命令：

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

- *ip-address* – 指定 FTP 服务器的 IP 地址。
- *port-number* – 指定 FTP 服务器的端口号。

在全局配置模式下，使用以下命令恢复 FTP 服务器默认 IP 地址和端口号：

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

配置日志服务器的 IP 地址和端口号，在全局配置模式下，使用以下命令：

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

- *ip-address* – 指定日志服务器的 IP 地址。
- **secure-tcp** – 指定该参数后，安全设备和 HSM 服务器在日志传输时，日志信息将被加密传输。
- *port-number* – 指定日志服务器的端口号。

在全局配置模式下，使用以下命令恢复日志服务器默认 IP 地址和端口号：

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

开启/关闭 HSM 代理功能

HSM 服务器管理参数以及信任域配置完成以后，用户需要开启设备的 HSM 代理功能以实现设备与服务器的正常连接。默认情况下，设备的 HSM 代理功能是关闭的，启用此功能，在全局配置模式下，使用以下命令：

network-manager enable

在全局配置模式下，用该命令 no 的形式关闭此功能：

no network-manager enable

显示 HSM 代理配置

用户可以在任何模式下使用 show 命令查看设备上 HSM 代理的配置信息：

show network-manager

网络时间协议（NTP）

网络时间协议（Network Time Protocol），简称为 NTP。NTP 为整个网络传递统一、标准的时间。实现方法是在网络上指定若干时钟源，为用户提供授时服务，并且这些时钟服务器间能够相互对比以提高准确度。NTP 协议采用 UDP 传输协议格式，使用专用端口 123。

提示：关于 NTP 确保时钟同步的精确性的算法，请参阅 RFC1305 规范。

Hillstone 设备的时间影响到设备的许多功能模块，例如 VPN 隧道的建立、时间表功能的实现以及自签名证书的使用等，因此系统时间的精确性十分重要。为保证 Hillstone 设备系统能够一直保持精确时间，Hillstone 设备允许用户通过 NTP 来使系统时间与网络上的 NTP 服务器同步。Hillstone 设备支持两种设置时间的方式，分别是手动设置和通过 NTP 与服务器同步。

注意：为保证自签名证书时间的正确性，避免证书使用错误，初次使用设备时，请务必将设备时间与 PC 时间同步。

手动配置时间

手动配置系统的时间，在全局配置模式下，使用以下命令：

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

- *HH:MM:SS Month Day Year* – 指定系统时间。HH、MM 和 SS 分别表示小时、分钟和秒，Month、Day 和 Year 分别表示月、日和年。

手动配置时区

系统提供多个预定义时区，同时，为实现更精确的时区配置，系统支持自定义时区配置，并且，用户可以为自定义时区指定夏令时。

系统的默认时区是东 8 区。为系统指定时区，在全局配置模式下，使用以下命令：

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

- *timezone-name* – 指定预定义时区名称。
- *cus-timezone-name* – 指定自定义时区名称，范围是 1 到 6 个字符。
- *hours minutes* – 为自定义时区指定相对 UTC（Universal Time Coordinated，协调世界时）时间的偏移量。hours 的取值范围是-13 到 12；minutes 的取值范围是 0 到 59。

例如：

自定义时区为 test，其相对 UTC 的偏移量是 6 小时 30 分：

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

配置夏令时

夏令时（summer-time）是为节约能源而人为规定的地方时间制度。按国家法令，在夏季及其前后实施。一般在天亮早的夏季人为将时间提前一小时，夏季结束再将时间调回一小时。用户可以为系统自定义时区指定夏令时的绝对时间段和循环时间段。

为系统指定夏令时的绝对时间段，在全局配置模式下，使用以下命令：

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

- *cus-timezone-name* – 指定自定义时区名称，范围是 1 到 6 个字符。
- **date** – 指定夏令时的绝对时间段。
- *start-date* – 指定夏令时起始日期。书写格式为“月/日/年”，例如 7/20/2011。
- *start-time* – 指定夏令时起始时间。书写格式为“小时：分钟”，例如 10:30。
- *end-date* – 指定夏令时终止日期。书写格式为“月/日/年”，例如 7/20/2011。
- *end-time* – 指定夏令时终止时间。书写格式为“小时：分钟”，例如 10:30。
- *compensation-time* – 指定夏令时生效时的时间补偿，默认值为 0。例如夏令时开始时，某些地区时间须调快 1 小时 30 分；夏令时结束时，时间须调慢 1 小时 30 分。“1 小时 30 分”即为夏令时生效时的时间补偿。书写格式为“小时：分钟”，例如 1:30。

例如：

自定义时区 test 的夏令时从 6/22/2011 的 10:30 开始，到 9/23/2011 的 10:00 结束。夏令时期间的时间将比非夏令时期间的时间快 2 小时 30：

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

为系统指定夏令时的循环时间段，即在每年的指定时间段内，执行夏令时。在全局配置模式下，使用以下命令：

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* – 指定自定义时区名称，范围是 1 到 6 个字符。
- **recurring** – 指定夏令时的循环时间段。
- **{ [Mon] |[…] | [Sun] }{after | before}***start-day start-month start-time* – 指定夏令时循环时间段的起始时间。例如命令关键字为 **Mon before 22 6 10:30**，即夏令时起始时间为每年 6 月 22 日前的第一个周一的 10:30。
- **{ [Mon] |[…] |[Sun]} {after | before}***end-day end-month end-time*– 指定夏令时循环时间段的终止时间。例如命令关键字为 **Fri after 23 9 10:00**，即夏令时终止时间为每年 9 月 23 日后的第一个周五的 10:00。
- *compensation-time* – 指定夏令时生效时的时间补偿，默认值为 0。例如夏令时开始时，某些地区时间须调快 1 小时 30 分；夏令时结束时，时间须调慢 1 小时 30 分。“1 小时 30 分”即为夏令时生效时的时间补偿。书写格式为“小时：分钟”，例如 1:30。

例如：

自定义时区 test 的夏令时在从每年的 6 月 22 日前的第一个周一的 10:30 开始，到 9 月 23 日后的第一个周五的 10:00 结束。夏令时期间的时间将比非夏令时期间的时间快 2 小时 30：

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

注意：夏令时的配置会对日志和基于时间的功能模块产生影响。例如，当 9/23/2011 的 10:00 夏令时结束时，系统时间将自动调慢 2 小时 30 分，恢复为非夏令时期间的 7:30。这样，9/23/2011 的 7:30 到 10:00 在这一天会出现两次。

使用 **no clock summer-time** *cus-timezone-name* **date** 命令取消夏令时的配置。

查看系统时间配置信息

在 CLI 任何命令模式下使用 **show clock** 命令，查看当前的时区配置信息。

在 CLI 任何命令模式下使用 **show config** 命令，查看当前的夏令时配置信息。

配置 NTP 功能

通过 NTP 配置，可以使 Hillstone 设备的系统时间与时钟服务器同步。在 Hillstone 设备上可以做的 NTP 配置有以下各项：

- 开启/关闭 NTP 功能
- 配置 NTP 服务器
- 配置最大调整时间
- 配置查询间隔
- 开启/关闭身份验证功能
- 配置 NTP 身份验证功能

开启/关闭 NTP 功能

默认情况下，系统的 NTP 功能是关闭的。在 Hillstone 设备上开启或者关闭 NTP 功能，在全局配置模式下使用以下命令：

- 启用：**ntp enable**
- 禁用：**no ntp enable**

配置 NTP 时钟服务器

用户最多可以指定 3 个时钟服务器，同时可以使用 prefer 关键字指定主时钟服务器（Hillstone 设备首先与主服务器进行时间同步）；如果没有为服务器指定 prefer 关键字，Hillstone 设备会使用户最先配置的服务器做时间同步。配置 NTP 时钟服务器，请在全局配置模式下输入以下命令：

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

- *ip-address* | *host-name* – 指定时钟服务器的 IP 地址或主机名称。主机名称取值范围为 1 到 127 个字符。
- **key** *number* – 指定可以通过该服务器的验证密钥。如果要在配置的时钟服务器上使用 NTP 身份验证功能，用户必须指定 key 参数值。
- **source** *interface-name* – 指定 Hillstone 设备上发送和接收 NTP 包的接口。
- **prefer** – 如果指定了多个时钟服务器，该关键字用来指定该服务器为主时钟服务器。

Hillstone 设备首先与主服务器进行时间同步，如果失败，再查找下一个时钟服务器。

- *vrouter-name* – 为指定的 VRouter 指定时钟服务器。

使用 **no ntp server** {*ip-address* | *host-name*}命令取消指定时钟服务器的配置。

以下是时钟服务器配置示例：

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

配置最大调整时间

如果 Hillstone 设备和 NTP 时钟服务器的时间差在最大调整时间之内，就能成功进行时间同步，否则同步不成功。配置最大调整时间，在全局配置模式下，输入以下命令：

ntp max-adjustment *time-value*

- *time-value* – 最大调整时间值。范围是 0 到 3600 秒，0 表示没有时间限制。默认值是 10 秒。

使用 **no ntp max-adjustment** 命令恢复最大调整时间的默认值。

配置查询间隔

Hillstone 设备每隔一个查询间隔就与时钟服务器做一次同步，保证 Hillstone 设备系统时间的准确。配置查询间隔，在全局配置模式下，输入以下命令：

ntp query-interval *time-interval*

- *time-interval* – 查询间隔值。范围是 1 到 60 分钟。默认值是 5 分钟。

使用 **no ntp query-interval** 命令恢复查询间隔的默认值。

开启/关闭身份验证功能

默认情况下，系统的 NTP 身份验证功能是关闭的。在 Hillstone 设备上开启或者关闭 NTP 身份验证功能，在全局配置模式下使用以下命令：

- 启用：**ntp authentication**
- 禁用：**no ntp authentication**

配置 NTP 身份验证功能

使用 NTP 身份验证功能，用户需要配置 MD5 身份验证密钥 ID 和密钥。启动该功能后，Hillstone 设备只会与通过验证的服务器进行同步。配置 NTP 验证密钥 ID 和密钥，请在全局配置

模式下，输入以下命令：

ntp authentication-key *number* **md5** *string*

- *number* - 验证密钥 ID，范围是从 1 到 65535；
- *string* - MD5 验证密钥，范围是 1 到 31 个字符。

在全局配置模式下，使用 **no ntp authentication-key** *number* 命令取消验证密钥的配置。

查看 NTP 状态

NTP 配置完成后，在任何模式下运行 **show ntp status** 命令可以查看当前的 NTP 配置信息和 NTP 状态。

NTP 配置示例

NTP 服务器的 IP 地址是 10.10.10.10；身份验证密钥 ID 和 MD5 验证密钥分别是 1 和 aaaa；查询间隔为 3 分钟；最大调整时间为 5 秒。配置完成后开启 Hillstone 设备的 NTP 身份验证功能和 NTP 功能。最后查看 NTP 配置信息和状态。请参考以下配置命令：

```
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
```

配置时间表功能

Hillstone 设备支持时间表（Schedule）功能。时间表功能可以使策略规则在指定的时间生效，也可以控制 PPPoE 接口与因特网的连接时间。时间表包含绝对计划和周期计划。周期计划通过周期条目指定时间表的时间点或者时间段；而绝对计划决定周期计划的生效时间。每个周期计划最多可以拥有 16 条周期条目。

创建时间表

创建一个时间表，在全局配置模式下，使用以下命令：

schedule *schedule-name*

- *schedule-name* – 指定时间表的名称。范围是 1 到 31 个字符。

执行该命令后，系统创建指定名称的时间表并且进入时间表配置模式；如果指定的名称已存在，则直接进入时间表配置模式。在时间表配置模式下，用户可以配置时间表的周期和绝对时间。

使用 **no schedule** *schedule-name* 命令删除指定的时间表。删除时间表之前，请从其它模块中取消对该时间表的引用。

指定绝对计划

绝对计划是一个时间范围，指定的周期计划会在绝对计划的时间范围内生效。同时，用户也可以不启用绝对计划功能，此时周期计划会在被应用到系统中某项功能上时，立即生效。指定绝对计划，在时间表配置模式下，使用以下命令：

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

- **start** *start-date start-time* – 指定绝对计划的开始时间点，包括日期和具体时间。start-date 为开始的日期，书写格式为“月/日/年”，例如 10/23/2007；start-time 为开始的具体时间，书写格式为“小时：分钟”，例如 15：30。如果不指定该参数的值，开始时间为当前时间。
- **end** *end-date end-time* – 指定绝对计划的结束时间点，包括日期和具体时间。end-date 为结束的日期，书写格式为“月/日/年”，例如 11/05/2007；end-time 为结束的具体时间，书写格式为“小时：分钟”，例如 09：00。如果不指定该参数的值，则无结束时间，周期会从开始时间起，一直有效。

使用 **no absolute** 命令关闭绝对计划功能，使周期计划能够即时生效。

指定周期计划

周期计划的时间是该周期计划中周期条目的总和。一个周期计划中最多可以添加 16 个条周期条目。用户可以配置三种类型的周期条目：

- 每天：每天的指定时间。例如每天的 9：00 到 18：00。
- 每周的某几天：一周中指定天的指定时间。例如每周一、周二和周六的 9：00 到 13：30。
- 每周一段时间：一周中的一个连续时间段。例如从周一早上 9：30 到周三下午 15：00。

指定“每天”或者“每周的某几天”类型周期条目，在时间表配置模式下，使用以下命令：

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

- **daily** – 每一天（周一到周日）。
- **weekdays** – 工作日（周一到周五）。
- **weekend** – 周末（周六到周日）。
- [**monday**] […] [**sunday**] – 选择需要的日期。例如选择周二、周三和周六，命令关键字为 **tuesday wednesday saturday**。
- *start-time* – 开始时间。书写格式为“小时：分钟”，例如 09：00。
- *end-time* – 结束时间。书写格式为“小时：分钟”，例如 16：30。

使用多条该命令添加多个“每天”或者“每周的某几天”类型周期条目。

使用 **no periodic** {**daily** | **weekdays** | **weekend** | [**monday**] […] [**sunday**]} *start-time* **to** *end-time* 命令删除指定的周期条目。

指定“每周一段时间”类型周期条目，在时间表配置模式下，使用以下命令：

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

- [**monday**] | […] | [**sunday**] – 开始日期，可以是周一到周日的任意一天。
- *start-time* – 开始时间。书写格式为“小时：分钟”，例如 09：00。
- [**monday**] | […] | [**sunday**] – 结束日期，与开始日期相同或者晚于开始日期。
- *end-time* – 结束时间。书写格式为“小时：分钟”，例如 16：30。

使用多条该命令添加多条“每周一段时间”类型周期条目。

使用 no periodic {[monday] | […] | [sunday]} *start-time* to {[monday] | […] | [sunday]} *end-time* 命令删除指定的周期条目。

配置监测对象

系统的监测功能能够监测指定的目标（IP 地址或者主机）是否可达或者接口的链路是否连通，以及监测目标或接口链路是否出现拥塞。如果监测目标不可达或接口链路没有连通，系统会直接判断监测失败；如果监测目标可达或接口链路连通，系统可以继续根据报文延时和接口流量判断监测目标或链路是否出现拥塞。监测功能主要用在 HA、策略路由、链路负载均衡等场景，用户可以通过配置监控功能确保系统始终选择相对健康的链路。

注意：

- 监测失败后，系统会断开到监测对象的所有会话。
- 出现拥塞后，系统仍会保留到监测对象的所有会话，但不允许新建会话。

配置监测功能，首先需配置监测对象，在全局配置模式下，使用以下命令：

track *track-object-name* **[local]**

- *track-object-name* – 指定监测对象名称。范围是 1 到 31 个字符。
- **local** – 若指定该参数，系统将不向备份设备同步该监测对象的相关配置信息。默认情况下，不指定该参数。

执行该命令后，系统创建指定名称的监测对象，并且进入监测对象配置模式；如果指定的名称已存在，则直接进入监测对象的配置模式。使用该命令 no 的形式删除指定的监测对象：

no track *track-object-name*

系统支持通过 Ping 报文、HTTP 报文、ARP 报文、DNS 报文和 TCP 报文五种方式对目标进行主动监测，还支持通过统计指定接口的流量信息对目标进行被动监测。

Ping 报文监测

通过 Ping 报文对目标进行监测，在监测对象配置模式下使用以下命令：

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* – 指定监测目标的 IP 地址或者主机名称。主机名称范围是 1 到 63 个字符。
- **interface** *interface-name* – 指定发送 Ping 检测报文的出接口。
- **interval** *value* – 指定发送 Ping 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **src-interface** *interface-name* – 指定 Ping 检测报文的源接口。
- **prior-used-srcip** – 若源接口上已配置多个 IP，将其中一个 IP 指定为 prior-used-srcip 后，系统将使用此 IP 发送 track 报文；若没有指定该参数，则使用默认的源接口主 IP 发送 track 报文。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。
- **delay high-watermark** *value* **low-watermark** *value* – 指定监测目标响应 Ping 报文延时的高水位线和低水位线，单位为毫秒。取值范围是 1 到 65535 毫秒。延时小于指定的高水位线，系统会判断链路为正常状态；延时大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在延时小于或等于指定的低水位线后系统才会判

断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。

- **delay-weight** *value* – 指定该条监测出现链路拥塞对整个监测对象出现链路拥塞所贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

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

HTTP 报文监测

通过 HTTP 报文对目标进行监测，在监测对象配置模式下使用以下命令：

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* – 指定监测目标的 IP 地址或者主机名称。主机名称范围是 1 到 63 个字符。
- **interface** *interface-name* – 指定发送 HTTP 检测报文的出接口。
- **interval** *value* – 指定发送 HTTP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **src-interface** *interface-name* – 指定 HTTP 检测报文的源接口。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。
- **delay high-watermark** *value* **low-watermark** *value* – 指定监测目标响应 HTTP 报文延时高水位线和低水位线，单位为毫秒。取值范围是 1 到 65535 毫秒。延时小于指定的高水位线，系统会判断链路为正常状态；延时大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在延时小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。
- **delay-weight** *value* –指定该条监测出现链路拥塞对整个监测对象出现链路拥塞所贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监

测条目：

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

ARP 报文监测

通过 ARP 报文对目标进行监测，在监测对象配置模式下使用以下命令：

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

- *A.B.C.D* – 指定监测目标的 IP 地址。
- **interface** *interface-name* – 指定发送 ARP 检测报文的出接口。
- **interval** *value* – 指定发送 ARP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

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

DNS 报文监测

通过 DNS 报文对目标进行监测，在监测对象配置模式下使用以下命令：

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* – 指定监测目标的 IP 地址。
- **interface** *interface-name* – 指定发送 DNS 检测报文的出接口。
- **interval** *value* – 指定发送 DNS 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。

- **src-interface** *interface-name* – 指定 DNS 检测报文的源接口。
- **delay high-watermark** *value* **low-watermark** *value* – 指定监测目标响应 DNS 报文延时高水位线和低水位线，单位为毫秒。取值范围是 1 到 65535 毫秒。延时小于指定的高水位线，系统会判断链路为正常状态；延时大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在延时小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。
- **delay-weight** *value* –指定该条监测出现链路拥塞对整个监测对象出现链路拥塞所贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

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

TCP 报文监测

通过 TCP 报文对目标端口进行监测，在监测对象配置模式下使用以下命令：

tcp {*A.B.C.D* | **host** *host-name*} **port** *port-number* **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* – 指定监测目标的 IP 地址或者主机名称。主机名称范围是 1 到 63 个字符。
- **port** *port-number* – 指定监测目标的目的端口号。取值范围为 0 到 65535。
- **interface** *interface-name* – 指定发送 TCP 检测报文的出接口。
- **interval** *value* – 指定发送 TCP 报文的时间间隔，单位为秒。范围是 1 到 255 秒。默认值是 3 秒。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续未收到该参数指定个数的响应报文，就判断为监测失败，即目标不可达。取值范围是 1 到 255。默认值是 3。
- **src-interface** *interface-name* – 指定 TCP 检测报文的源接口。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。
- **delay high-watermark** *value* **low-watermark** *value* – 指定监测目标响应 TCP 报文延时的高水位线和低水位线，单位为毫秒。取值范围是 1 到 65535 毫秒。延时小于指

定的高水位线，系统会判断链路为正常状态；延时大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在延时小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。

- **delay-weight** *value* – 指定该条监测出现链路拥塞对整个监测对象出现链路拥塞所贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。对于同一个监测对象，不能同时配置对同一目标主机的 HTTP 监测和对端口 80（**port** 80）的 TCP 监测。使用该命令 no 的形式删除指定的监测条目：

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

接口链路状态监测

配置监测接口的链路状态，在监测对象配置模式下使用以下命令：

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

- *interface-name* – 指定被监测接口的名称。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no interface *interface-name*

接口带宽监测

配置监测接口带宽，在监测对象配置模式下使用以下命令：

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

- *interface-name* – 指定被监测接口的名称。
- **direction** {**in** | **out** | **both**} – 指定监测的流量方向。**in** 指流入方向，**out** 指流出方向，**both** 指双方向。默认为流出方向（**out**）。
- **high-watermark** *value* **low-watermark** *value* – 指定接口流量的高水位线和低水位线，单位为 kbps。取值范围是 1 到 100000000kbps。接口流量小于指定的高水位线，

系统会判断链路为正常状态；接口流量大于或等于指定的高水位下，系统会判断出现链路拥塞；出现链路拥塞后，只有在接口流量小于或等于指定的低水位线后系统才会判断链路恢复正常状态。这种高低水位线的设计可以有效的防范链路在正常与拥塞状态之间频繁切换。

- **interval** *value* – 指定监控接口流量的间隔时间，单位为秒。取值范围是 1 到 255 秒。默认值是 1 秒。
- **threshold** *value* – 指定判断该条监测出现拥塞的警戒值。如果系统连续检测到参数指定次数的链路过载情况，就判断该条监测出现拥塞。取值范围是 1 到 255。默认值是 3。
- **weight** *value* – 指定该条监测出现拥塞对整个监测对象出现拥塞贡献的权重值。取值范围是 1 到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no bandwidth interface *interface-name*

接口链路质量监测

通过统计指定接口的采样流量信息，系统可以监测该接口的链路状态。配置接口链路对象监测，在监测对象配置模式下使用以下命令：

traffic-condition interface *interface-name* [**condition-threshold** *low-watermark high-watermark*] [**interval** *value*] [**threshold** *value*] [**weight** *value*]

- *interface-name* – 指定被监测接口的名称。
- **condition-threshold** *low-watermark high-watermark* – 指定每个监测周期的新建会话成功率阈值。默认情况下，失败界定阈值为 30，成功界定阈值为 50。取值范围是 0 到 100。在某个监测周期内，当新建会话成功率小于指定的失败界定阈值时，判断为监测失败；当新建会话成功率大于指定的成功界定阈值时，判断为监测成功；当新建会话成功率大于等于失败界定阈值且小于等于成功界定阈值时，系统保持原来的监测状态。
- **interval** *value* – 指定每个监测周期的持续时间，单位为秒。取值范围是 1 到 255 秒。默认值是 3 秒。每个监测周期结束后，系统会重置探测到的新建会话相关数值。
- **threshold** *value* – 指定判断监测失败的警戒值。如果系统连续检测到参数指定次数的监测失败情况，就判断该条监测失败。取值范围是 1 到 255。默认值是 3。
- **weight** *value* – 指定该条监测失败对整个监测对象失败贡献的权重值。取值范围是 1

到 255。默认值是 255。

用户可以配置多条该命令为监测对象指定多个监测条目。使用该命令 no 的形式删除指定的监测条目：

no traffic-condition interface *interface-name*

配置警戒值

警戒值用于判断整个监测对象失败或出现拥塞。当监测对象中同类型监测条目的权重值总和大于等于对应的警戒值时，系统会判断整个监测对象失败或出现拥塞。用户可以针对监测对象失败、报文超时导致的监测对象拥塞和接口流量过载导致的监测对象拥塞三种情况分别设置不同类型的警戒值：监测对象警戒值、报文超时警戒值和接口流量警戒值。

监测对象警戒值

当监测对象中失败的监测条目的权重值的总和大于等于一定值，系统就判断整个监测对象失败。该值即为监测对象的警戒值。指定监测对象的警戒值，在监测对象配置模式下使用以下命令：

threshold *value*

- *value* – 指定监测对象警戒值的大小。范围是 1 到 255。默认值是 255。

在监测对象配置模式使用该命令 no 的形式恢复警戒值的默认值：

no threshold

报文延时警戒值

当监测对象中报文延时所导致链路拥塞的权重值的总和大于等于一定值，系统就判断整个监测对象出现拥塞。该值即为报文延时的警戒值。指定报文延时的警戒值，在监测对象配置模式下使用以下命令：

delay-threshold *value*

- *value* – 指定报文延时警戒值的大小。范围是 1 到 255。默认值是 255。

在监测对象配置模式使用该命令 no 的形式恢复警戒值的默认值：

no delay-threshold

例如，配置监测对象如下：

```
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
```

完成该配置后，如果监测目标 1.1.1.1 和 1.1.1.2 均出现链路拥塞（即 DNS 报文延时均超过 100 毫秒），则 **delay-weight**=50+220=270>250，系统判定监测对象 **delay-test** 出现拥塞。

接口流量警戒值

当监测对象中接口流量过载所导致链路拥塞的权重值的总和大于等于一定值，系统就判断整个监测对象出现拥塞。该值即为接口流量的警戒值。指定接口流量的警戒值，在监测对象配置模式下使用以下命令：

bandwidth-threshold *value*

- *value* – 指定接口流量警戒值的大小。范围是 1 到 255。默认值是 255。

在监测对象配置模式使用该命令 no 的形式恢复警戒值的默认值：

no bandwidth-threshold

例如，配置监测对象如下：

```
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
```

完成该配置后，如果监测目标接口 eth0/1 和 eth0/2 均出现链路过载（即上述接口上均出现过 5 次或 5 次以上流量超过 20kbps 的情况），则 **bandwidth-threshold** =50+220=270>250，系统判定监测对象 **bandwidth-test** 出现拥塞。

当被监控接口的监测对象失败或出现拥塞后，系统会自动禁止这些接口的相关路由（静态路由、动态路由、策略路由等）参与流量转发，即正常的流量转发不再匹配到这些接口的路由，但当系统只有一条出口默认路由时，此规则无效。

用户可以在任何模式下使用 show 命令查看监测对象的配置信息：

show track *tack-object-name*

应用层强制检查

系统支持应用层强制检查功能。开启该功能后，系统将对应用层入侵防御、病毒过滤、内容过滤以及网页关键字过滤、应用层行为控制进行强制检查。若关闭该功能，当系统资源过低（例如设备的 CPU 使用率过高、内存、数据包缓存剩余容量不足）时，系统将对数据包放行处理，来控制

应用层功能对设备的资源利用，从而不会影响到其他功能模块。默认情况下，该功能为关闭状态。

开启/关闭应用层强制检查功能

用户可在全局配置模式下，使用以下命令开启应用层强制检查：

fail-close enable

在全局配置模式下，使用该命令 no 的形式关闭该功能：

no fail-close enable

注意：不支持应用层强制检查功能有：FTP 的应用行为控制、Web surfing、IPS 的 MSRPC/SUNRPC/DNS(UDP) 检测。

查看应用层强制检查启用状态

在任何模式下运行 **show fail-close** 命令可以查看当前的应用层强制检查功能的启用状态。

系统监控报警

StoneOS 的系统监控报警功能能够监控系统资源的使用状况，并根据配置发出报警信息。当前版本支持的报警方式为日志信息和 SNMP Trap 信息。

配置系统监控报警功能，首先要进入监控配置模式。进入监控配置模式，在全局配置模式下，使用以下命令：

monitor

进入监控配置模式后，用户可以根据需要监控的系统资源对象，设置相应的监控规则：

{**cpu** | **memory utilization** | **interface-bandwidth** *interface-name* **utilization** | **log-buffer** { **config** | **event** | ips | **network** | **security** | **traffic{session** | **nat** | **urlfilter**}} **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** | **urlfilter**}} **utilization** | **policy utilization** | **session utilization | snat-resource utilization** – 指定监控对象，可以为系统 CPU（**cpu**）、内存（**memory**）、接口带宽（**interface-bandwidth**）、日志容量（**log-buffer**）、策略数（**policy**）、会话（**session**）和 SNAT 转换后的 IP 地址端口资源（**snat-resource**）。当用户设备为 X

平台时，选择 CPU 监控对象后，需要继续选择对应的板卡。

- *interface-name* – 指定监控的接口名称。
- **config** | **event** | **ips** | **network** | **security** | **traffic {session** | **nat** | **urlfilter**} – 指定具体的日志类型。
- **utilization** – 指定监控值为各对象的利用率。CPU (cpu) 的监控值默认为利用率，不需要指定。

♦ **interval** *interval-value* – 指定监控间隔，即系统在报警计算时间段（**sample-period** *period-value*）内，每次取值后等待的时间间隔。取值范围为 3 到 10 秒。

♦ **absolute** – 指定监控值为绝对值。

♦ **rising-threshold** *threshold-value* – 指定上升阈值，即实际监控值超过该阈值满足报警条件的百分比。取值范围为 1 到 99。

sample-period *period-value* – 指定报警计算时间段。取值范围为 30 到 3600 秒。

count *count-value* – 指定在报警计算时间段（**sample-period**）内，监控对象的实际监控数值超过阈值（**rising-threshold**）的次数。取值范围为 1 到 1000。如果配置该参数，在监控时间段内，若监控对象值超过阈值的次数大于该 **count** 值，则发出警告；如果不配置该参数，在监控时间段内，若监控对象值的平均值大于阈值（**rising-threshold**），则发出警告。

♦ **log** [**snmp-trap**] | **snmp-trap** – 指定报警方式。可以使用日志（**log**）或者 SNMP Trap 报文（**snmp-trap**），也可以同时使用这两种报警方式。

例如：

配置 CPU 峰值监控：

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

完成该配置后，在 600 秒内，如果 CPU 利用率超过了阈值 65%，且发生过最少 50 次，则发出报警日志

配置会话均值监控：

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

完成该配置后，在 600 秒内，如果会话平均利用率超过了阈值 90%，则发出报警日志

在监控配置模式下使用该命令 no 的形式删除指定的监控规则：

no {**cpu** | **memory utilization** | **interface-bandwidth** *interface-name*

utilization | log-buffer { config | event | ips | network | security | traffic {session | nat | urlfilter}} utilization | policy utilization | session utilization | snat-resource utilization}

注意:

- 不支持对 SNAT 转换后地址为出接口 IP 地址（**eif-ip**）的端口资源的监控报警；
- 对于每种监控对象，只有最后配置的一条监控规则生效。

查看系统监控报警配置，在任意模式下，使用以下命令：

show monitor

系统监控报警功能的日志信息类别为事件（Event），严重等级为严重（Critical）。用户可以查看系统事件日志信息，或者配置事件日志 email 提醒功能将日志信息发送到管理员邮件。关于如何配置系统日志的详细信息，请参阅《监控》的“日志”。

查看系统监控严重等级为严重（Critical）以上的事件日志，在任意模式下，使用以下命令：

show logging alarm [**severity** *severity-level*]

系统最大并发连接数变化

在 Hillstone 设备部分平台上开启多 VR、病毒过滤、入侵防御、URL 特征库功能后，或者使用 IPv6 版本系统软件，系统的最大并发连接数会发生变化。下表列出 Hillstone 设备平台型号、系统文件版本以及相应的系统最大并发连接数的变化情况。

表 8：系统最大并发连接数变化列表

平台	系统文件	最大并发连接数变化
SG-6000-M8860 SG-6000-M8260 SG-6000-M7260 SG-6000-M7860	StoneOS IPv4 版本	开启多 VR、病毒过滤、入侵防御、URL 特征库功能后，系统最大并发连接数无变化。
	StoneOS IPv6 版本	系统最大并发连接数无变化。 IPv6 版本不支持多 VR、病毒过滤、入侵防御以及 URL 特征库功能。
SG-6000-X7180 SG-6000-X6180 SG-6000-X6150	StoneOS IPv4 版本	开启多 VR：最大并发连接数减少 15%。 计算公式为“实际最大并发连接数=原始最大并发连接数*(1-0.15)” 不支持病毒过滤、入侵防御、URL 特征库功能。
	StoneOS IPv6 版本	系统最大并发连接数为 IPv4 版本的 50%。 不支持多 VR、病毒过滤、入侵防御以及 URL 特征库功能。
除以上 7 个平台外的	StoneOS IPv4 版本	• 开启多 VR：最大并发连接数减少 15%。

平台	系统文件	最大并发连接数变化
其它平台		计算公式为“实际最大并发连接数=原始最大并发连接数*(1-0.15)”； • 开启病毒过滤/入侵防御/URL 特征库中的一个或者多个：最大并发连接数减少 50%。 计算公式为“实际最大并发连接数=原始最大并发连接数*(1-0.5)”； • 开启多 VR 的同时开启病毒过滤/入侵防御/URL 特征库中的一个或者多个：最大并发连接数在已经减少的基础上再减少 50%。 计算公式为“实际最大并发连接数=原始最大并发连接数*(1-0.15)*(1-0.5)”。
	StoneOS IPv6 版本	系统最大并发连接数为 IPv4 版本的 50%。 IPv6 版本不支持多 VR、病毒过滤、入侵防御以及 URL 特征库功能。

连接山石云·景

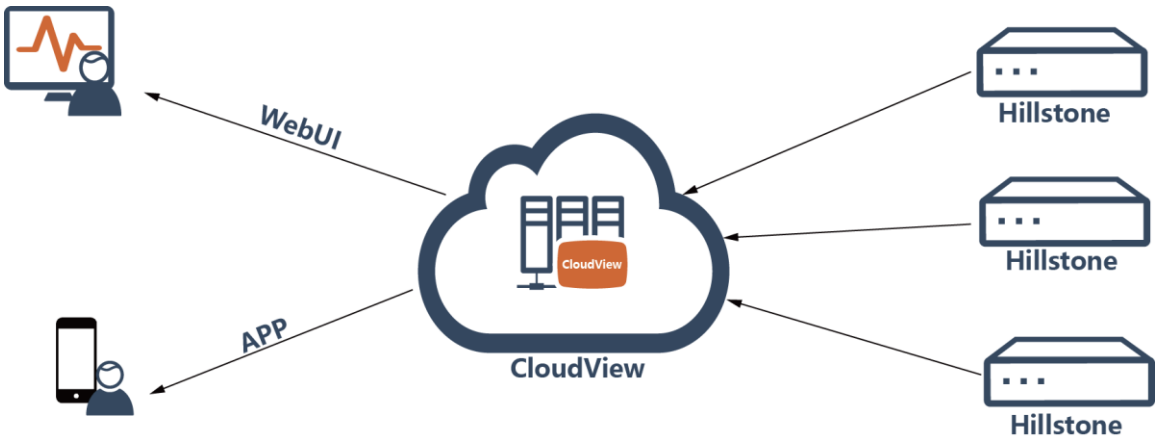
云·景 (CloudView) 是一款安全领域的 SaaS 产品，是移动互联时代的云安全服务平台。云·景部署在公有云上，为用户提供在线按需服务。用户可以通过互联网、手机端获得便捷、高质量以及低成本的增值安全服务，得到更好的安全体验。

在 Hillstone 设备上正确配置了连接云·景功能后，就可以实现设备注册到公有云以及与云·景的连接，进而实现云·景对设备的远程监控。

云·景典型应用场景

云·景的主要应用场景描述如下：

Hillstone 设备注册到云·景，将设备信息、流量数据、威胁事件、系统日志等上传到云端，云端提供可视化的展示。用户通过 Web 方式或者手机 APP 方式进行远程监控设备状态信息、获取报表、威胁分析等。



Hillstone 设备端配置

在 Hillstone 设备端，配置包括以下内容：

- 配置云·景服务器
- 启用云·景
- 开启流量数据上传
- 开启系统日志上传
- 开启威胁事件上传
- 显示云·景服务器配置

配置云·景服务器

在连接云·景之前，用户需要配置云·景服务器地址、用户名、密码，当用户名密码验证通过后，将下发云·景服务器的配置信息。配置云·景服务器，在全局配置模式下，使用以下命令：

cloud server address *A.B.C.D |domain* [**username** *user-name* **password** *pass-word*]

- *A.B.C.D/domain* – 指定云·景服务器地址或域名，系统默认地址为 http://cloud.hillstonenet.com.cn。
- **username** *user-name* – 指定云·景的注册用户名称，即可将设备注册到公有云指定的用户名下。
- **password** *pass-word* – 指定对应用户的密码。

使用 **no cloud server address** 恢复云·景服务器默认配置。

启用云·景

在全局配置模式下使用 **cloud server enable** 命令启用云·景功能。

开启流量数据上传

设备支持将设备的监控数据上传到云·景，在全局配置模式下，使用如下命令：

cloud server upload-type traffic

使用 **no cloud server upload-type traffic** 关闭流量数据上传功能。

开启系统日志上传

设备支持将事件日志上传到云·景，上传间隔默认为 10 分钟。在全局配置模式下，使用如下命令：

cloud server upload-type log-event

使用 **no cloud server upload-type log-event** 关闭事件日志上传功能。

说明：开启该功能前，请先确保设备已开启事件日志功能（**logging event on**） 以及云·景服务器状态为已连接。

开启会话数据上传

设备支持将设备的会话数据上传到云·景，在全局配置模式下，使用如下命令：

cloud server upload-type session

使用 **no cloud server upload-type session** 关闭会话数据上传功能。

注意：对于部分 Hillstone 设备（X 系列、T 系列），不支持上传会话数据到云·景。

开启 URL 数据上传

设备支持将设备的 URL 数据上传到云·景，在全局配置模式下，使用如下命令：

cloud server upload-type url

使用 **no cloud server upload-type url** 关闭 URL 数据上传功能。

注意：对于部分 Hillstone 设备（X 系列、T 系列），不支持上传 URL 数据到云·景。

开启威胁事件上传

设备支持将设备检测的所有威胁事件上传到云·景，传间隔默认为 10 分钟。在全局配置模式下，使用如下命令：

```
cloud server upload-type threat-event
```

使用 `no cloud server upload-type threat-event` 关闭威胁事件上传功能。

说明：关于威胁检测的配置，请参阅具体威胁防护功能配置章节。

开启所有类型数据上传

上传上述所有类型数据，在全局配置模式下，使用如下命令：

```
cloud server upload-type all
```

使用 `no cloud server upload-type all` 关闭所有类型数据上传功能。

开启威胁防护数据上传

在用户开启并使用此功能时，基于该功能本身的要求，威胁数据将会被上传到云端，被用于内部的数据研究以减少用户设备的误报并实现更好的防护效果。开启威胁防护数据上传，在全局配置模式下，使用如下命令：

```
cloud server upload-type hcsp
```

取消威胁防护数据上传，使用 `no cloud server upload-type hcsp` 命令

启用云巡检

云巡检功能能够实现在云端对 Hillstone 设备进行远程集中的监控和运维管理。在 Hillstone 设备端启用云巡检功能后，系统能够接收并执行云端的巡检指令，并且将收集的巡检数据信息上传到云·景。

启用云巡检功能，在全局配置模式下，使用如下命令：

```
cloud server upload-type inspection
```

禁用云巡检功能，使用 `no cloud server upload-type inspection` 命令。

显示云·景服务器配置

显示云·景服务器的配置，在任意模式下，使用如下命令：

```
show cloud server
```