Hillstone Networks Inc.

StoneOS 命令行用户手册

路由 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-ROU-5.5R6-CN-V1.0-Y18M07

目录

目录 3
关于本手册 1
手册约定 1
内容约定 1
CLI 约定 1
命令行接口（CLI） 2
CLI 介绍 2
命令模式和提示符 2
命令行错误信息提示 3
命令行的输入 3
命令行的编辑 4
过滤 CLI 输出信息 5
分页显示 CLI 输出信息 6
设置终端属性 6
设置连接超时时间 6
重定向输出 7
诊断命令 7
路由 8
开启/关闭静态路由查询 8
开启/关闭会话重匹配路由 9
VRouter 9
指定最大路由条目数 10
引入 VRouter 路由 10
取消直连路由优先 10
静态路由 10
配置静态路由 11
目的接口路由 12
添加目的接口路由条目 12
查看目的接口路由信息 13
查看目的接口路由的 FIB 信息 13
ISP 路由 13
配置 ISP 信息 14
配置 ISP 路由 14

查看 ISP 路由配置信息 15
上传 ISP 配置文件 15
删除已上传的预定义 ISP 配置文件 17
配置源路由 17
添加源路由条目 17
查看源路由条目信息 18
配置源接口路由 18
添加源接口路由条目 18
查看源接口路由条目信息 19
配置策略路由 19
创建 PBR 策略 19
创建 PBR 规则 19
编辑 PBR 策略规则 20
修改规则排列顺序 22
配置目的路由优先查找 22
应用 PBR 策略 23
配置 PBR 策略全局匹配顺序 23
显示 PBR 策略全局匹配顺序 23
策略路由规则支持配置 TTL 24
查看 PBR 策略规则信息 24
DNS 重定向 24
WAP 智能分流 26
动态路由 30
配置 RIP 30
配置 OSPF 35
配置 IS-IS 52
配置 BGP 61
等价多径路由（ECMP） 76
静态组播路由 77
开启/关闭组播路由功能 78
配置静态组播路由 78
显示组播路由信息 79
显示组播 FIB 信息 79
互联网组管理协议 79
IGMP Proxy 80
IGMP Snooping 81
BFD 83
BFD 工作模式 83
BFD Echo 功能 83

配置 BFD 基本功能 84
配置 BFD 与路由协议联动 85
显示 BFD 会话信息 87
路由配置举例 87
开启/关闭静态路由查询功能配置举例 87
多 VR 配置举例 88
静态组播路由配置举例 91
IGMP Proxy 配置举例 93
IGMP Snooping 配置举例 95
BFD 配置举例 97

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。

路由

路由是将数据包从一个网络转发到另一个网络中的目的地址的过程。路由器是处在两个网络之间转发数据包的设备。路由器根据路由表中储存的各种传输路径传输数据包，每一个传输路径即为一个路由条目。

StoneOS 具有三层路由功能，通过 VRouter，进行路由配置，对不同的数据包进行转发。StoneOS 支持静态路由（Static Routing）、ISP 路由、源路由（Source-Based Routing，简称 SBR）、源接口路由（Source-Interface-Based Routing，简称 SIBR）、目的接口路由（Destination-Interface-Based Routing，简称 DIBR）、策略路由（Policy-Based Routing，简称 PBR）、就近探测路由（Proximity Routing）、动态路由（包括 RIP、OSPF、IS-IS 和 BGP）和等价多径路由（Equal Cost MultiPath Routing，简称 ECMP）和静态组播路由（Static Multicast-routing）。

- 静态路由：手工配置的、根据目的 IP 地址确定下一跳的路由。
- 目的接口路由（DIBR）：根据数据包的目的 IP 地址和入接口，选择路由，进行转发。
- ISP 路由：根据不同的 ISP 确定下一跳。
- 源路由（SBR）：根据数据包的源 IP 地址，选择路由，进行转发。
- 源接口路由（SIBR）：根据数据包的源 IP 地址和入接口，选择路由，进行转发。
- 策略路由（PBR）：根据数据包的源地址、源用户、目的地址以及服务类型，选择路由，进行转发。
- 就近探测路由：根据出站就近探测的结果选择路由，进行转发。
- 动态路由：设备按照动态路由协议（RIP、OSPF 或者 BGP）自动生成的动态路由表项对数据包进行路由选择并转发。
- 等价多径路由（ECMP）：到达相同目的 IP 地址或网段的数据流量在多条相同管理距离的路径上进行负载均衡。
- 静态组播路由：手工配置的、将数据从一个组播源传送至组播组内各成员的路由。

当 Hillstone 设备对进入的数据包进行转发时，按照这样的顺序选路：策略路由→源接口路由→源路由→目的接口路由→目的路由/ISP 路由/就近探测路由/动态路由。

开启/关闭静态路由查询

对于策略路由、源接口路由和源路由，用户可以单独控制是否需要对它们进行查询（系统要求

必须进行目的路由查询)。默认情况下，策略路由、源接口路由和源路由查询为开启状态。开启/关闭策略路由、源接口路由和源路由查询，在全局配置模式下，使用以下命令(适用于所有 VRouter)：

- 开启：**route enable** {**pbr** | **sibr** | **sbr**}
- 关闭：**route disable** {**pbr** | **sibr** | **sbr**}

提示：关于开启/关闭静态路由查询的配置举例，请参阅“开启/关闭静态路由查询功能配置举例”。

开启/关闭会话重匹配路由

默认情况下，会话重匹配路由的功能是开启的。当用户添加、修改或者删除路由时，会话会重新匹配最优路由。在会话重新匹配路由的过程中，符合以下情况的会话会被删除：

- 当会话之前匹配的路由或者路由的出接口被删除时，该会话会被删除。
- 当会话之前匹配的路由不是最优路由，且重新匹配的路由的出接口发生变化时，该会话会被删除。

在某些情况下 (如添加或删除策略路由的应用类型)，会话可能会被大量删除，导致流量异常。此时，需要关闭会话重新匹配功能。

在 Flow 配置模式下，使用以下命令关闭或开启此功能：

- **session rematch route disable**
- **session rematch route enable**

VRouter

VRouter 的功能与路由器相同，并且拥有自己的路由表。系统有一个默认 VRouter，即 trust-vr，同时系统支持多 VRouter (多 VR) 功能。Hillstone 设备的所有路由配置都需要在相应的 VRouter 配置模式下进行。进入 VRouter 配置模式，在全局配置模式下使用以下命令：

ip vrouter *vrouter-name*

- *vrouter-name* – 指定 VRouter 的名称。

在 VRouter 配置模式下，用户可以配置静态路由条目、动态路由协议，也可以指定 VRouter 支持的最大路由条目数以及从其它 VRouter 引入路由。

使用多 VR 功能，需要先执行 **exec vrouter enable** 命令后再重启系统使多 VR 功能生效。

提示：关于多 VR 的配置举例，请参阅“多 VR 配置举例”。

指定最大路由条目数

指定 VRouter 允许的最大路由条目数（包含 VRouter 下的所有直连路由、静态路由和各种动态路由），在 VRouter 配置模式下，使用以下命令：

max-routes *number*

- *number* – 指定最大路由条目数。范围是 1 到 100000。

在 VRouter 配置模式下，使用该命令 no 的形式取消最大路由条目数的指定：

no max-routes

当路由条目数达到最大路由条目数，系统将会发出警告。

引入 VRouter 路由

用户可以把其它 VRouter 中的路由条目引入到当前 VRouter 进行使用。引入 VRouter 路由，在 VRouter 配置模式下使用以下命令：

import vrouter *vrouter-name* {**connected** | **static** | **rip** | **ospf** | **bgp**}

- *vrouter-name* – 指定被引入路由所属的 VRouter。
- **connected** | **static** | **rip** | **ospf** | **bgp** – 指定被引入路由的类型。

多次配置该命令引入多种类型路由。

注意：从其它 VRouter 引入的路由的优先级低于 VRouter 自身的路由。

取消直连路由优先

直连路由拥有最高路由优先级，在同时配置其他路由时，直连路由会被优先使用，使得其他路由不生效，因此，用户可以根据需要，取消直连路由优先，使其他路由优先使用。在 VRouter 配置模式下使用以下命令：

fib-lookup connect-first-disable

在 VRouter 配置模式下，使用该命令 no 的形式恢复直连路由优先：

no fib-lookup connect-first-disable

静态路由

静态路由是手工定义的路由条目，根据目的地址指定下一跳，因此也称作目的路由。对外连接较少或者内网连接相对比较稳定的网络通常使用静态路由。用户可以根据需要确定是否添加默认路由条目。

配置静态路由

用户可以添加目的路由条目并且显示目的路由信息。

添加目的路由条目

用户可以为 VRouter 添加目的路由条目。但是，添加目的路由条目之前，需要进入 VRouter 配置模式。请在全局配置模式下使用以下命令：

ip vrouter *vrouter-name*

- *vrouter-name* – 指定 VRouter 的名称。

进入到 VRouter 配置模式下后，用户可以添加目的路由条目。在 VRouter 配置模式下使用以下命令：

ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**tag** *tag-value*] [**description** *description*] [**schedule** *schedule-name*]

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定目的地址。Hillstone 设备支持两种方式，*A.B.C.D/M*或者 *A.B.C.D A.B.C.D*,例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- *A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name* – 指定下一跳。可以是网关地址（*A.B.C.D*）、接口（*interface-name*）或者 VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择隧道接口名称（当为多隧道接口时，用户必须使用 A.B.C.D 参数指定 IPSec VPN、GRE 或者 SCVPN 隧道的下一跳 IP 地址，并且此地址必须和该隧道接口绑定的相应隧道的下一跳 IP 地址相同）、Null0 接口或者 PPPoE 接口。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是 1 到 255，默认值是 1。
- **tag** *tag-value* – 指定目的路由的标记值。在 OSPF 引入路由时，如果此处配置的路由标记值匹配到路由映射表中的规则，那么将会引入该路由，从而实现对引入路由信息的过滤。取值范围是 1 到 4294967295。
- **description** *description* – 指定路由的描述信息。范围是 1 到 63 个字符。

- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

使用多条该命令添加多条静态路由条目。

使用以上命令 no 的形式删除指定的静态路由条目：

no ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*}[**description** *description*] [**schedule** *schedule-name*]

显示目的路由信息

用户可以在任何模式下使用以下命令查看目的路由信息：

show ip route static [**vrouter** *vrouter-name*]

- *vrouter-name* – 显示指定的 VRouter 的目的路由信息。

目的接口路由

目的接口路由（DIBR）根据数据包的目的 IP 地址和入接口，选择路由，进行转发。

添加目的接口路由条目

目的接口路由的配置也需要在 VRouter 配置模式下完成。进入 VRouter 配置模式，在全局配置模式下，使用以下命令：

ip vrouter *vrouter-name*

进入到 VRouter 配置模式下后，用户可以添加目的接口路由条目。在 VRouter 配置模式下使用以下命令：

ip route in-interface *interface-name* {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

- **in-interface** *interface-name* – 指定路由条目的入接口。
- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定目的地址。Hillstone 设备支持两种方式，*A.B.C.D/M*或者 *A.B.C.D A.B.C.D*,例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- *A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name* – 指定下一跳。可以是网关地址（*A.B.C.D*）、接口（*interface-name*）或者 VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择隧道接口名称（当为多隧道接口时，

用户必须使用A.B.C.D参数指定IPSec VPN、GRE或者SCVPN隧道的下一跳IP地址，并且此地址必须和该隧道接口绑定的相应隧道的下一跳 IP 地址相同)、Null0 接口或者PPPoE 接口。

- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是 1 到 255，默认值是 1。
- **description** *description* – 指定路由的描述信息。范围是 1 到 63 个字符。
- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表(最多 8 个)。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

使用多条该命令添加多条目的接口路由条目。

使用以上命令 no 的形式删除指定的目的接口路由条目：

no ip route in-interface *interface-name* {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* [*A.B.C.D*] | **vrouter** *vrouter-name*} [**description** *description*] [**schedule** *schedule-name*]

查看目的接口路由信息

用户可以在任何模式下使用以下命令查看目的接口路由信息：

show ip route in-interface *interface-name*

- **in-interface** *interface-name* – 显示指定入接口的目的接口路由信息。

查看目的接口路由的 FIB 信息

用户可以在任何模式下使用以下命令查看目的接口路由的 FIB 信息：

show ip fib in-interface *interface-name*

- **in-interface** *interface-name* – 显示指定入接口的目的接口路由的 FIB 信息。

ISP 路由

很多用户通常会申请多条线路进行流量负载均衡。然而，一般的均衡是不会根据流量的流向做均衡的，如果网通的服务器通过电信访问，网速就会很慢。Hillstone 设备针对该问题，提供 ISP

路由功能，使不同 ISP 流量走专有路由，从而提高网络速度。

配置 ISP 路由，用户首先需要将子网条目添加到一个 ISP，然后才可以配置以 ISP 名称为目的地的 ISP 路由。用户可以自定义 ISP 信息，也可以上传 ISP 包含不同 ISP 信息的配置文件。同时 StoneOS 提供一个预定义 ISP 配置文件，包含两个 ISP，分别是中国电信（China-telecom）和中国网通（China-netcom）。

配置 ISP 路由，用户需要进行的操作如下：

- 配置 ISP 信息
- 配置 ISP 路由
- 上传 ISP 配置文件
- 查看 ISP 路由配置信息
- 删除已上传的预定义 ISP 配置文件

配置 ISP 信息

在设备上配置 ISP 信息，首先需要进入 ISP 信息配置模式。在全局配置模式下，使用以下命令，创建 ISP 名称并且进入 ISP 信息配置模式：

isp-network *isp-name*

- *isp-name* – 指定 ISP 名称。

在全局配置模式下，使用该命令 no 的形式删除指定名称的 ISP：

no isp-network *isp-name*

为 ISP 添加子网条目，在 ISP 信息配置模式下，使用以下命令：

subnet *A.B.C.D/M*

- *A.B.C.D/M* – 为 ISP 指定子网，格式为 IP 地址/掩码，例如 1.1.1.0/24。

在 ISP 信息配置模式下配置多条该命令，为 ISP 添加多个子网。

在 ISP 信息配置模式下使用该命令 no 的形式删除指定的子网：

no subnet *A.B.C.D/M*

配置 ISP 路由

ISP 路由需要在 VRouter 配置模式下进行配置。进入 VRouter 配置模式，在全局配置模式下使用以下命令：

ip vrouter *vrouter-name*

- *vrouter-name* – 指定 VRouter 的名称。

在 VRouter 配置模式，使用以下命令配置 ISP 路由条目：

ip route *isp-name* {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

- *isp-name* – 指定系统中已存在的 ISP 名称作为路由的目的地址。
- *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* – 指定下一跳。可以是网关地址(*A.B.C.D*)、接口(*interface-name*)或者 VRouter(**vrouter** *vrouter-name*)。当下一跳为接口时，用户可以选择隧道接口名称、Null0 接口或者 PPPoE 接口。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的比重。范围是 1 到 255，默认值是 1。
- **description** *description* – 指定路由的描述信息。范围是 1 到 63 个字符。
- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

使用多条该命令添加多条 ISP 路由条目。

使用以上命令 no 的形式删除指定的 ISP 路由条目：

no ip route *isp-name* {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* } [*distance-value*] [**weight** *weight-value*] [**description** *description*] [**schedule** *schedule-name*]

查看 ISP 路由配置信息

用户可以通过 show 命令查看 ISP 路由配置信息。

- 查看通过设备配置的 ISP 信息：

  show isp-network {**all** | *isp-name*}
- 查看 ISP 路由条目：

  show ip route isp [*isp-name* | **vrouter** *vrouter-name*]

上传 ISP 配置文件

ISP 配置文件的上传只能通过 WebUI 来完成。Hillstone 设备支持两种 ISP 配置文件，分别

是用户自定义 ISP 配置文件和系统预定义配置文件。

请按照下所示实例格式书写用户自定义配置文件，否则，即使文件上传成功，也不可以在系统中生效。预定义/用户自定义配置文件中包含的 ISP 的个数最多为 26 个，也就是作为索引值的 26 个英文字母的个数。

表 5：用户自定义 ISP 配置文件实例

```
# NOTICE: Keep the following comment lines intact!!!
E --- China-55
R --- China-66
# China-55
E:55.10.2.0/24
E:55.10.3.0/24
# China-66
R:66.20.2.0/24
R:66.20.3.0/24
```

上传预定义 ISP 配置文件

StoneOS 的预定义 ISP 配置文件为加密形式。Hillstone 更新预定义 ISP 配置文件后，用户需要重新上传新的预定义 ISP 配置文件。步骤如下：

1. 从页面左侧导航树选择并点击“配置➤网络➤路由”，进入路由页面。
2. 点击『ISP 信息』标签，进入 ISP 页面。
3. 点击 ISP 列表左上角的『上传』按钮，弹出<从 PC 上载 ISP 配置文件>对话框。
4. 选中<从电脑上传预定义的 ISP 配置文件>或<从电脑上传用户定义的 ISP 配置文件>的单选按钮。
5. 点击『浏览』按钮在电脑上选择需要的 ISP 配置文件，然后点击『上传』按钮上传所选择的 ISP 配置文件至设备。版本行显示了当前预定义 ISP 配置文件的版本号。

保存自定义 ISP 配置文件

用户还可以将在设备上配置的 ISP 信息保存到电脑。保存步骤如下：

1. 从页面左侧导航树选择并点击“配置➤网络➤路由”，进入路由页面。
2. 点击『ISP 信息』标签，进入 ISP 页面。
3. 点击 ISP 列表左上角的『保存』按钮，弹出<保存用户自定义 ISP 配置到 PC>对话框。
4. 在<ISP 名称>下拉菜单中选择需要保存的 ISP 的名称。
5. 点击『保存』按钮，保存相应的 ISP 配置文件到电脑的指定位置。

删除已上传的预定义 ISP 配置文件

如果已经上传过预定义 ISP 配置文件，用户可以在执行模式下，通过使用以下命令将上传的预定义 ISP 配置文件从系统中删除：

exec isp-network clear-predefine

执行该命令后，重启系统，系统将恢复使用原有的预定义 ISP 配置文件（出厂时系统自带的预定义 ISP 配置文件）。

配置源路由

源路由的配置需要在 VRouter 配置模式下完成。进入 VRouter 配置模式，在全局配置模式下，使用以下命令：

ip vrouter *vrouter-name*

添加源路由条目

在 VRouter 配置模式下，使用以下命令添加一条源路由条目：

ip route source {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**schedule** *schedule-name*]

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定源路由条目的网络地址。Hillstone 设备支持两种方式，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- *A.B.C.D* | *interface-name* – 指定下一跳。可以是网关地址（*A.B.C.D*）、接口（*interface-name*）或者 VRouter（**vrouter** *vrouter-name*）。当下一跳为接口时，用户可以选择隧道接口、Null0 接口或者 PPPoE 接口。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的权重。范围是 1 到 255，默认值是 1。
- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建

议用户不要配置时间重叠的时间表。

使用以上命令 no 的形式删除指定的源路由条目：

no ip route source { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name*}

查看源路由条目信息

用户可以在任何模式下通过 show 命令查看源路由条目信息。在任何模式下，使用以下命令：

源路由：**show ip route source** [**vrouter** *vrouter-name*]

- *vrouter-name* – 显示指定的 VRouter 的源路由信息。

配置源接口路由

源接口路由的配置也需要在 VRouter 配置模式下完成。进入 VRouter 配置模式，在全局配置模式下，使用以下命令：

ip vrouter *vrouter-name*

添加源接口路由条目

在 VRouter 配置模式下，使用以下命令添加一条源接口路由条目：

ip route source in-interface *interface-name* { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name*} [*distance-value*] [**weight** *weight-value*] [**schedule** *schedule-name*]

- *interface-name* – 指定路由条目的入接口。
- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定路由条目的源网络地址。Hillstone 设备支持两种方式，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- *A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* – 指定下一跳。可以是网关地址(*A.B.C.D*)、接口(*interface-name*)或者VRouter(**vrouter** *vrouter-name*)。当下一跳为接口时，用户可以选择隧道接口名称，也可以选择 Null0 接口（黑洞路由）。
- *distance-value* – 指定路由的管理距离大小。该参数设定路由的优先级，取值越小，优先级越高，而在有多条路由选择的时候，优先级高的路由会被优先使用。取值范围是 1 到 255，默认值为 1。当路由距离为 255 时，该路由无效。
- **weight** *weight-value* – 指定路由权值的大小。路由权值决定负载均衡中流量转发的权重。范围是 1 到 255，默认值是 1。

- **schedule** *schedule-name* – 指定时间表名称。该条配置将会在时间表指定的时间范围内生效。可配置多次该命令指定多个时间表（最多 8 个）。为避免产生不可预知的问题，建议用户不要配置时间重叠的时间表。

使用以上命令 no 的形式删除指定的源接口路由条目：

no ip route source in-interface *interface-name* { *A.B.C.D/M* | *A.B.C.D A.B.C.D*} {*A.B.C.D* | *interface-name* | **vrouter** *vrouter-name* }

查看源接口路由条目信息

用户可以在任何模式下通过 show 命令查看源接口路由条目信息。在任何模式下，使用以下命令：

源接口路由：**show ip route source in-interface** *interface-name*

配置策略路由

策略路由功能检查数据包的源 IP、目的 IP 和服务类型，对匹配策略的数据包的下一跳进行指定。

创建 PBR 策略

创建 PBR 策略，在全局配置模式下使用以下命令：

pbr-policy *name*

- *name* – 指定 PBR 策略名，名称范围是 1 到 31 个字符。如果该策略已经创建，则直接进入 PBR 策略配置模式。

使用 **no pbr-policy** *name* 删除指定的 PBR 策略。

创建 PBR 规则

进入 PBR 策略配置模式下，用户便可定义自己的 PBR 规则。在 CLI 中创建 PBR 规则的命令如下：

{**match** | **match-v6** } [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**] *src-addr dst-addr service-name* [*application-name*] **nexthop** {*interface-name* | *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} [**weight** *value*] [**track** *track-object-name*]

- **id** *rule-id* – 指定新建策略规则的 ID，取值范围为 1 到 255。如果不指定，系统将会

为 PBR 规则自动分配一个 ID。规则 ID 在该 PBR 策略中必须是唯一的。

- **before** *rule-id* | **after** *rule-id* | **top** – 指定 PBR 规则的位置，可以是某个规则之前(**before** *rule-id*)、某个规则之后(**after** *rule-id*)或者所有规则的首位(**top**)。默认情况下，系统会将新创建的策略规则放到所有规则的末尾。
- *src-addr* – 指定源地址，该地址为地址簿条目。
- *dst-addr* – 指定目的地址，该地址为地址簿条目。
- *service-name* – 指定服务名称。*service-name* 为服务簿中定义的服务。
- *application-name* – 指定应用名称。*application-name* 为应用簿中定义的应用。
- **nexthop** {*interface-name* | *A.B.C.D* | **vrouter** *vrouter-name* | **vsys** *vsys-name*} – 指定下一跳。*interface-name* 为出接口的名称，*A.B.C.D* 为下一跳的 IP 地址，**vrouter** *vrouter-name* 为 VRouter，**vsys** *vsys-name* 为虚拟系统。
- **weight** *value* – 指定下一跳的权重，取值范围是 1 到 255，默认值是 1。如果一条策略路由匹配多个下一跳，系统会按照权重值比例分配流量。
- **track** *track-object-name* – 指定下一跳的监测对象。如果监控对象失败，本条策略路由也会失败。关于如何配置监测对象，请参阅“系统管理“的“配置监测对象”部分。

使用该命令 no 的形式删除指定 ID 的规则。在 PBR 策略配置模式下，执行以下命令：

no match id *rule-id*

另外，用户还可以在 PBR 策略配置模式下使用以下命令，创建一个策略规则 ID，并且进入 PBR 策略规则配置模式，再进一步配置其它策略规则相关参数：

match [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]

- **id** *id* – 指定 PBR 策略规则的 ID。如果不指定，系统将会为策略规则自动分配一个 ID。规则 ID 在整个系统中必须是唯一的。策略规则的 ID 大小并不表示策略规则的匹配先后顺序。
- **top** | **before** *rule-id* | **after** *rule-id* – 指定策略规则的位置，可以是某个规则 ID 之前（**before** *id*）、某个规则 ID 之后（**after** *id*）或者所有规则的首位（**top**）。默认情况下，系统会将新创建的策略规则放到所有规则的末尾。

注意：关于如何配置其它策略相关参数，请参考下一节“编辑 PBR 策略规则”。

编辑 PBR 策略规则

创建好的 PBR 策略规则可以通过编辑来修改不合适的参数值，但是修改工作必须在 PBR 策略规则配置模式下才可以进行。在 CLI 中进入 PBR 策略规则配置模式，请输入以下命令：

- **match** [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]
- **match id** *rule-id* (该命令适用于规则 ID 已存在的情况，并且用该命令 no 的形式，可以删除该条规则，即 **no match id** *rule-id*)

进入 PBR 策略规则配置模式后，可使用的编辑策略规则的命令如下：

- 添加地址簿条目类型源地址：**src-addr** *src-addr*
- 删除地址簿条目类型源地址：**no src-addr** *src-addr*
- 添加 IP 成员类型源地址：**src-ip** {*ip/netmask* | *ip-address netmask*}
- 删除 IP 成员类型源地址：**no src-ip** {*ip/netmask* | *ip-address netmask*}
- 添加主机成员类型源地址：**src-host** *host-name*
- 删除主机成员类型源地址：**no src-host** *host-name*
- 添加 IP 地址范围类型源地址：**src-range** *min-ip max-ip*
- 删除 IP 地址范围类型源地址：**no src-range** *min-ip max-ip*
- 添加地址簿条目类型目的地址：**dst-addr** *dst-addr*
- 删除地址簿条目类型目的地址：**no dst-addr** *dst-addr*
- 添加 IP 成员类型目的地址：**dst-ip** *ip/netmask*
- 删除 IP 成员类型目的地址：**no dst-ip** *ip/netmask*
- 添加主机成员类型目的地址：**dst-host** *host-name*
- 删除主机成员类型目的地址：**no dst-host** *host-name*
- 添加 IP 地址范围类型目的地址：**dst-range** *min-ip* [*max-ip*]
- 删除 IP 地址范围类型目的地址：**no dst-range** *min-ip* [*max-ip*]
- 添加角色类型源用户：**role** *role-name*
- 删除角色类型源用户：**no role** *role-name*
- 添加用户类型源用户：**user** *aaa-server-name user-name*
- 删除用户类型源用户：**no user** *aaa-server-name user-name*
- 添加用户组类型源用户：**user-group** *aaa-server-name user-group-name*
- 删除用户组类型源用户：**no user-group** *aaa-server-name user-group-name*
- 添加服务类型：**service** *service-name*
- 删除服务类型：**no service** *service-name*
- 添加应用类型：**application** *application-name*
- 删除应用类型：**no application** *application-name*
- 指定下一跳：**nexthop** {*interface-name* | *A.B.C.D* | *vrouter-name* | **vsys**

vsys-name}

- 取消下一跳配置：**no nexthop**
- 配置时间表：**schedule** *schedule-name*
- 删除时间表：**no schedule**
- 添加规则描述：**description** *string*
- 删除规则描述：**no description**
- 开启日志记录功能：**log enable**
- 关闭日志记录功能：**no log enable**

启用/禁用 PBR 策略规则

默认情况下，配置好的 PBR 策略规则会在系统中立即生效。用户可以通过命令禁用某条策略规则，使其不对流量进行控制。禁用或者启用某条策略规则，在 PBR 策略规则配置模式下，使用以下命令：

- 禁用：**disable**
- 启用：**enable**

修改规则排列顺序

PBR 策略中的规则通过 ID 进行唯一标识。流量进入 Hillstone 设备时，Hillstone 设备对 PBR 策略规则进行顺序查找，然后按照查找到的相匹配的第一条规则对流量进行处理。但是，PBR 策略规则 ID 的大小顺序并不是规则查找时的匹配顺序。使用 **show pbr-policy** 命令列出的规则顺序才是规则匹配顺序（系统将由上到下进行查找匹配）。用户在创建 PBR 策略规则时可以指定该规则的排列位置，也可以在 PBR 策略配置模式下修改其位置。PBR 策略规则的排列位置可以是绝对位置，即处在首位（Top）或者处在末位（Bottom），也可以是相对位置，即位于某个 ID 之前或之后。修改规则排列顺序，在 PBR 策略配置模式下使用以下命令：

move *rule-id* {**top** | **bottom** | **before** *rule-id* | **after** *rule-id*}

配置目的路由优先查找

默认情况下，设备对进入的数据包进行转发时，按照这样的顺序选路：策略路由→源接口路由→源路由→目的路由，在某些情况下，用户需要使匹配 PBR 策略规则的数据包，转发时优先查找目的路由，即选路的顺序为：目的路由→策略路由。配置 PBR 策略规则的目的路由（DBR）优先

查找，在 PBR 策略规则配置模式下，使用以下命令：

fib-lookup dbr-first

使用以上命令 no 的形式取消 PBR 策略规则的目的路由（DBR）优先查找：**no fib-lookup dbr-first**

应用 PBR 策略

可以通过绑定 PBR 策略到接口、安全域或者 VRouter 来实现 PBR 策略的应用。在接口配置模式、安全域配置模式或 VRouter 配置模式下，使用以下命令：

bind pbr-policy *name*

- *name* – 绑定指定的 PBR 策略到接口、安全域或者 VRouter。

使用以上命令 no 的形式取消 PBR 策略在接口、安全域或者 VRouter 的绑定：

no bind pbr-policy

配置 PBR 策略全局匹配顺序

默认情况下，如果接口和其所在安全域或者 VRouter 绑定了 PBR 策略，流量匹配顺序为：接口->安全域->VRouter。用户可以根据需要自行配置 PBR 策略的全局匹配顺序，在全局配置模式下，使用以下命令：

pbr-match order *index*

- *index* –为 PBR 策略指定全局匹配顺序的排序指数。包括 1-6，顺序分别表示如下：
  - **1** – 接口->安全域->Vrouter。该排序指数为默认值。
  - **2** – 安全域->接口 ->Vrouter。
  - **3** – Vrouter ->安全域->接口。
  - **4** – 接口-> Vrouter ->安全域。
  - **5** – Vrouter ->接口->安全域。
  - **6** – 安全域-> Vrouter->接口。

使用 **no pbr-match** 恢复默认匹配顺序配置。

显示 PBR 策略全局匹配顺序

用户可以在任何模式下，通过 show 命令查看 PBR 策略规则的全局匹配顺序信息。具体命令以下：

show pbr-match order

策略路由规则支持配置 TTL

用户可以在 PBR 规则中配置报文的 TTL，符合条件的报文将被设备转发到特定的出口链路。配置 TTL，请先执行以下命令进入 PBR 策略规则配置模式：

- **match** [**id** *rule-id*] [**before** *rule-id* | **after** *rule-id* | **top**]
- **match id** *rule-id* (该命令适用于规则 ID 已存在的情况)

在 PBR 策略规则配置模式下，输入以下命令：

ttl-range *min-ttl max-ttl*

- *min-ttl max-ttl* – 指定策略路由规则中报文的生存时间范围。*min-ttl* 指定生存时间的最小值，取值范围为 1 到 255；*max-ttl* 指定生存时间的最大值，取值范围为 1 到 255。

在 PBR 策略规则配置模式下，执行 **no ttl-range** 命令取消 TTL 范围的配置。

查看 PBR 策略规则信息

用户可以在任何模式下，通过 show 命令查看 PBR 策略规则的具体信息。具体命令以下：

show pbr-policy [*name*]

- *name* – 显示指定 PBR 策略的详细信息。如果不指定名称则显示所有 PBR 策略的详细信息。

DNS 重定向

系统支持 DNS 重定向，即在用户向 DNS 服务器发出域名请求时，系统将 DNS 请求重定向到指定的 DNS 服务器地址。目前，DNS 重定向主要应用于视频引流。通过和 PBR 策略结合，系统可将 Web 视频网站的流量引流到指定的链路上，进而提升用户访问视频的体验。

在全局配置模式下,使用以下命令开启或关闭 DNS 重定向功能：

app cache dns-redirect {**enable** | **disable**}

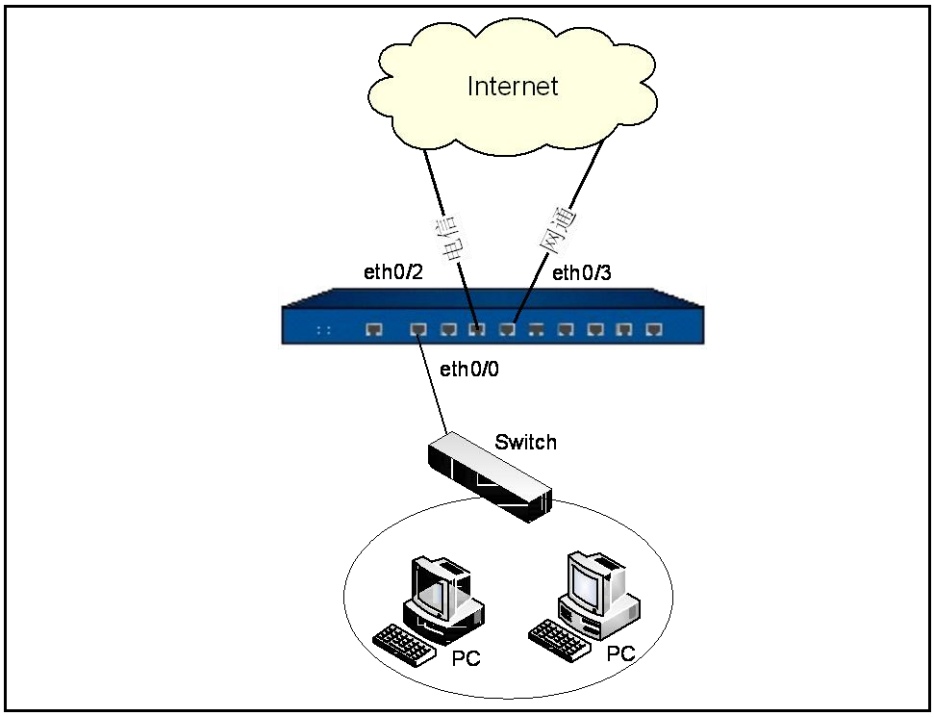
- **enable** – 开启 DNS 重定向功能。开启后，用户可根据系统提示指定 DNS 服务器地址，然后系统会将用户的 DNS 请求重定向到指定的 DNS 服务器上。
- **disable** – 关闭 DNS 重定向功能。默认情况下，系统关闭该功能。

在任何模式下，使用 **show dns-redirect** 命令查看 DNS 服务器和接口（该接口为 PBR 策略绑定的入接口）之间的绑定关系。

Web 视频引流配置案例

设备部署在互联网入口处，ethernet0/0 接口连接 PC，ethernet0/2 和 ethernet0/3 两个接口分别连接电信和网通的两条线路。配置 DNS 重定向和 PBR 策略之后，匹配到默认路由的流量将从 ethernet0/2 接口出去，匹配到策略路由的流量（如优酷）从 ethernet0/3 接口出去。组网图如下图所示：

图 1：Web 视频引流组网图



配置如下：

第一步：配置接口和安全域：

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 192.168.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone dmz
hostname(config-if-eth0/2)# ip address 10.180.41.52/20
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone dmz
hostname(config-if-eth0/3)# ip address 172.31.1.240/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

第二步：配置策略：

```
hostname(config)# rule id 1 from any to any service any permit
```

第三步：创建 SNAT：

```
hostname(config)# nat
hostname(config-nat)# snatrule from any to any service any trans-to eif-ip
mode dynamicport
```

第四步：配置默认路由：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 10.180.32.1
```

第五步：配置策略路由并绑定接口：

```
hostname(config)# pbr-policy test
hostname(config-pbr)# match top any any any YOUKU-DNS nexthop 172.31.1.1
        Match id 1 is created.
hostname(config-pbr)# match id 1
hostname(config-pbr-match)# application YOUKU
hostname(config-pbr-match)# application RTMFP
hostname(config-pbr-match)# exit
hostname(config-pbr)# exit
hostname(config)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# bind pbr-policy test
hostname(config-if-eth0/0)# exit
```

第六步：配置 ISP 路由：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route China-netcom 172.31.1.1
hostname(config-vrouter)# exit
```

第七步：升级 APP 特征库：

```
hostname(config)# exec app update professional
```

第八步：开启应用识别：

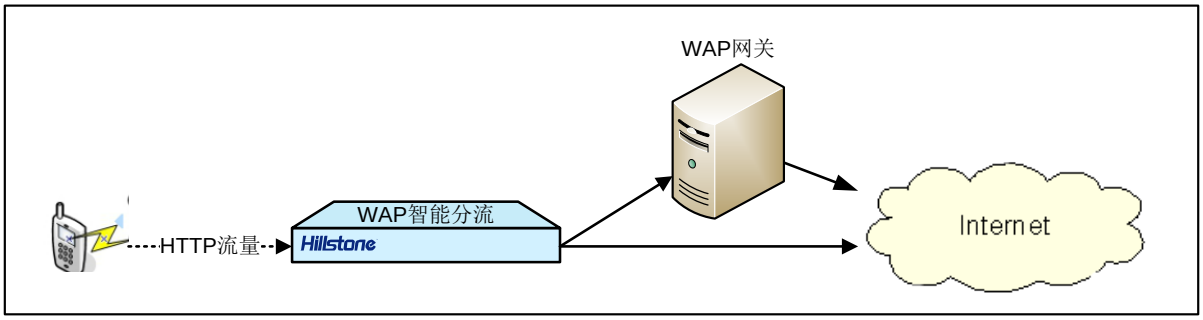
```
hostname(config)# zone trust
hostname(config-zone-trust)# application-identify
```

第九步：开启 DNS 重定向，并配置 DNS 服务器 IP 地址：

```
hostname(config)# app cache dns-redirect enable
Please specify the IP address for the DNS server
hostname(config)# ip name-server 58.240.57.33
```

WAP 智能分流

WAP 智能分流功能对流向 WAP 网关的 HTTP 流量进行分流，从而达到缓解 WAP 网关业务量的目的。下图为 Hillstone 设备用于 WAP 智能分流功能的典型部署图。



如上图所示，开启 WAP 智能分流功能的 Hillstone 设备工作在 WAP 服务器前端。当 HTTP 流量流向 Hillstone 设备时，系统对流量进行分析，并根据配置将流量分流到 WAP 网关或者外网。用户可选择将自营业务和 SP 业务分流到 WAP 网关进行处理，并把其他业务（浏览以及下载类业务）分流到外网。

WAP 智能分流功能主要基于策略路由规则实现分流。当流经接口的 HTTP 流量匹配策略路由规则时，系统会根据策略路由规则设置，将流量分流到指定的下一跳地址。对于分流到外网的流量，由于流量在分流之前的原始目的地为 WAP 网关地址，为保证正常访问，用户还需要开启 IP 替换功能，该功能能够将流量的原始目的地址（WAP 网关地址）替换为真实目的地址。

WAP 智能分流功能的配置包括：

- 启用 WAP 智能分流
- 配置 DNS 服务器
- 配置域名条目
- 配置策略路由规则
- 配置 SNAT 日志的记录方式

启用 WAP 智能分流

WAP 智能分流功能需配置在三层接口上，且只支持对 HTTP 流量进行分流。在指定接口上开启 WAP 智能分流功能并配置相关参数，请在接口配置模式下输入如下命令：

host-route http-dst-port *port-number1* [*port-number2*] [**dst-ip-replace** [**log-all** | **log-only-replace**]]

- **http-dst-port** *port-number1* [*port-number2*] – 指定 WAP 网关用于 HTTP 协议通讯的端口号。一般为 80 或 8080。
- **dst-ip-replace** [**log-all** | **log-only-replace**] – 开启目的 IP 替换功能并设置需要记录的日志信息。**log-all** 表示对所有流量记录日志；**log-only-replace** 表示对 IP 地址进行转换的流量记录日志。

用户可使用如下命令查看 WAP 智能分流的相关统计信息：

show host-route stat {**day** | **month**}

- **day** – 显示当天的统计信息。
- **month** – 显示当月的统计信息。

配置 DNS 服务器

DNS 服务器用来解析流量的真实目的地址。配置 DNS 服务器，请参阅“防火墙”的“网络参数”。由于一个域名可能对应多个 IP 地址，系统只支持保存解析后的第一个 IP 地址。

配置域名条目

用户可以给一个域名范围指定一个名称，在配置时，只需引用该名称。域名簿（Host book）就是 StoneOS 中用来存储域名范围与其名称的对应关系的数据库。域名簿中的域名与名称的对应关系条目被称作域名条目（Host entry）。

在使用 WAP 智能分流功能时，需配置域名条目并将其应用到策略路由规则中。根据流量是否匹配接口的策略路由规则设置以及是否命中域名条目，将流量分流到 WAP 网关或者外网。

注意：

- 域名条目个数的最大值为地址条目个数最大值的四分之一。
- 每条策略路由规则只可以配置一个域名条目。

用户可以通过 CLI 对域名簿进行以下配置：

- 添加或者删除域名条目
- 指定域名条目的域名范围
- 查看域名簿信息

添加或者删除域名条目

在全局配置模式，使用 **host-book** 命令向域名簿中添加一个域名条目，同时进入域名配置模式：

host-book *host-book-entry*

- *host-book-entry* – 指定要添加的域名条目的名称。

使用该命令 no 的形式将域名条目从域名簿中删除：

no host-book *host-book-entry*

指定域名条目的域名范围

在 StoneOS 系统中，域名条目的域名范围是其成员域名范围的总和。域名条目成员有以下几种：

- 域名：系统支持一级域名，例如：baidu.com。可使用通配符，例如：*baid*。
- IP 地址：指定 IP 地址，例如：61.155.169.229。

在域名配置模式下，使用 **host** 命令来为域名条目添加成员。

host *host-name*

- *host-name* – 指定域名或 IP 地址。

用该命令 no 的形式删除指定成员。

no host *host-name*

查看域名簿信息

用户可以在任何模式下使用以下命令查看域名簿的具体信息，包括域名簿内域名条目的名称、域名条目的成员数以及成员的具体内容。命令如下：

show host-book [*host-book-entry*]

- **show host-book** – 显示域名簿内所有域名条目的具体信息。
- *host-book-entry* – 显示指定域名条目的具体信息。

配置策略路由规则

在策略路由规则中引用域名条目，并将此策略路由规则绑定到开启 WAP 智能分流功能的接口，可以实现如下功能：根据流量是否匹配接口的策略路由规则设置以及是否命中域名条目，将流量分流到 WAP 网关或者外网。

在策略路由规则中引用域名条目，需要首先进入策略路由规则配置模式，再引用域名条目。在策略路由规则配置模式，输入如下命令引用域名条目：

host-book *host-book-entry*

- *host-book-entry* – 指定要引用的域名条目的名称。

关于如何绑定策略路由规则到接口，请参阅“配置策略路由”。

配置 SNAT 日志设置

当对分流到外网的流量进行 SNAT 并产生 SNAT 日志时，用户可选择在日志中记录流量的原始目的地址（即 WAP 网关地址）或记录真实目的地址（即 DNS 服务器解析出来的地址）。在全局配

置模式下，输入如下命令使 SNAT 日志中记录流量真实目的地址及端口号：

snat-log dst-using-translated

输入如下命令使 SNAT 日志中记录记录原始目的地址及端口号：

no snat-log

视频引流

通过视频引流功能，系统可将通过接口的 HTTP 视频流量引流到指定的链路上，进而提升用户访问视频的体验。使用视频引流功能，需要调整 WAP 智能分流的参数并结合应用识别功能。。

视频引流功能的配置包括：

1. 配置应用识别：根据数据流的应用类型对数据流进行相应的处理。
2. 开启视频引流：通过 **http-dst-port** *port-number1* [*port-number2*]命令开启 WAP 智能分流功能并指定视频网站用于 HTTP 协议通讯的端口号。使用视频引流功能不需要配置目的 IP 替换功能，即不需要配置 **dst-ip-replace** [**log-all** | **log-only-replace**] 参数。
3. 配置策略路由规则：配置策略路由规则并指定需要引流的应用/服务，并将该策略路由规则绑定到开启视频引流功能的接口。

动态路由

动态路由是根据网络系统的运行情况而自动调整的路由。Hillstone 设备根据路由协议自动调整动态路由表。StoneOS 支持 RIP、OSPF、IS-IS 和 BGP 三种动态路由协议。

配置 RIP

RIP（Routing Information Protocol）是路由信息协议。它是一种在路由器之间交换路由信息的内部网关路由协议。目前，RIP 有 RIP-1 和 RIP-2 两个版本，Hillstone 设备均支持。

对 RIP 协议的配置包括基本配置、引入路由、被动接口、邻居、网络和距离。另外，RIP 参数配置完成后，用户还需要在不同的接口上配置 RIP 参数，包括指定接口接收和发送更新的 RIP 版本号、水平分割以及接口的 RIP 认证。

基本配置

RIP 协议的基本配置包括指定 RIP 版本号、指定缺省度量、指定缺省距离、配置缺省信息发布

以及配置定时器（时间间隔、失效时间、保持时间和清除时间）。用户可以为不同的 VRouter 分别配置 RIP 协议。对 RIP 协议的基本配置需要在 RIP 路由模式下进行。进入 RIP 路由模式，请在全局配置模式下，使用以下命令：

ip vrouter *vrouter-name* （进入 VRouter 配置模式）

router rip（进入 RIP 路由模式，同时开启 Hillstone 设备的 RIP 功能）

在 VRouter 配置模式下，使用 **no router rip** 关闭 RIP 功能。

指定版本号

Hillstone 设备支持 RIP-1 和 RIP-2 两个版本。RIP-1 以广播方式传输报文；而 RIP-2 使用组播方式。指定 RIP 协议版本号，在 RIP 路由模式使用以下命令：

version *version-number*

- *version-number* – 指定版本号，1（RIP-1）或者 2（RIP-2）。默认为 2。

使用 **no version** 命令恢复默认版本配置。

指定缺省度量

RIP 协议使用跳数来衡量到达目的网络的距离，称为度量。路由器到与它直接相连网络的度量为 1，通过一个路由器可达的网络的度量为 2，依此类推，度量的最大值可以到 15，度量大于 15 的网络为不可达网络。缺省度量在引入路由时生效。指定 RIP 的缺省度量，在 RIP 路由配置模式下使用以下命令：

default-metric *value*

- *value* – 指定缺省度量值。范围是 1 到 15，默认值是 1。

使用 **no default-metric** 命令恢复缺省度量值。

指定缺省距离

指定 RIP 路由的缺省距离，在 RIP 路由配置模式下使用以下命令：

distance distance-*value*

- distance-*value* – 指定缺省管理距离。范围是 1 到 255，默认值是 120。

使用 **no distance** 命令恢复缺省距离值。

配置缺省信息发布

用户可以指定是否默认路由发布到其它使用 RIP 协议的路由器。默认情况下，RIP 协议不发送默认路由。配置缺省信息发布，在 RIP 路由配置模式下使用以下命令：

发送：**default-information originate**

不发送：**no default-information originate**

配置定时器

RIP 可配置的定时器分别是时间间隔(Interval)、失效时间(Invalid)、保持时间(Holddown)和清除时间（Flush)。具体描述如下：

- 时间间隔：每次向所有邻居发送全部 RIP 路由所间隔的时间。默认是 30 秒。
- 失效时间：如果一条路由在失效时间内一直没有被更新，该路由的度量就会被标记为 16，表示为不可达路由。默认的失效时间是 180 秒。
- 保持时间：如果一条更新后的路由的度量变大，例如，从 2 更新到 4，该路由会被赋予一个保持时间，路由在保持时间内，不接受任何更新。默认的保持时间是 180 秒。
- 清除时间：度量被标记为 16 的不可达路由会一直被发布到其它 RIP 协议路由，直到清除时间结束；如果该路由仍没有被更新，清除时间结束后，将会被从 RIP 路由信息数据库中删除。默认的清除时间是 240 秒。

用户可以修改以上四个定时器的时间值。配置定时器，在 RIP 路由配置模式下使用以下命令：

timers basic *interval-time invalid-time holddown-time flush-time*

- *interval-time* – 指定发送更新的时间间隔，单位为秒。范围是 0 到 16777215 秒。默认值是 30 秒。
- *invalid-time* – 指定路由的失效时间，单位为秒。范围是 1 到 16777215 秒。默认值是 180 秒。
- *holddown-time* – 指定路由的保持时间，单位为秒。范围是 1 到 16777215 秒。默认值是 180 秒。
- *flush-time* – 指定路由的清除时间，单位为秒。范围是 1 到 16777215 秒。默认值是 240 秒。

使用 **no timers basic** 命令恢复定时器的默认值。

引入路由

RIP 协议允许用户将设备上其它路由协议 (BGP、直连、静态和 OSPF) 的路由信息引入到 RIP 中，并向外发布。同时，用户可以设置被引入路由的度量。配置引入路由，在 RIP 路由配置模式下使用以下命令：

redistribute {**bgp** | **connected** | **static** | **ospf**} [**metric** *value*]

- **bgp** | **connected** | **static** | **ospf** – 指定引入路由的类型，可以是 BGP（**bgp**)、直连路由（**connected**)、静态路由（**static**）或者 OSPF（**ospf**)。
- **metric** *value* – 指定引入路由的度量。范围是 1 到 15。如果不指定该数值，系统会使

用 RIP 的缺省度量（通过 **default-metric** *value* 配置）。

用户可以配置多条该命令引入不同类型的路由。

使用 **no redistribute** {**bgp** | **connected** | **static** | **ospf**}命令取消指定类型路由的引入。

配置被动接口

用户可以将一些接口配置为只接收更新但是不发送，这种只接收更新的接口就是被动接口。配置被动接口，在 RIP 路由配置模式下使用以下命令：

passive-interface *interface-name*

- *interface-name* – 指定接口的名称作为被动接口。

用户可以配置多条该命令添加多个被动接口。

使用 **no passive-interface** *interface-name* 命令取消被动接口的配置。

配置邻居

用户可以指定一些邻居，使邻居和 Hillstone 设备之间能够允许点到点（非广播）的 RIP 信息交换。指定邻居，在 RIP 路由配置模式下使用以下命令：

neighbor *ip-address*

- *ip-address* – 指定邻居的 IP 地址。

用户可以配置多条该命令添加多个邻居。

使用 **no neighbor** *ip-address* 命令删除指定的邻居。

配置网络

用户需要配置一些网络，只有在指定网络中的接口才能接收和发送 RIP 更新。配置网络，在 RIP 路由配置模式下使用以下命令：

network *ip-address/netmask*

- *ip-address/netmask* – 指定网络的 IP 地址，例如 10.200.0.0/16。

用户可以配置多条该命令添加多个网络。

使用 **no network** *ip-address/netmask* 命令删除指定的网络。

配置距离

用户可以为从一些指定网络得到的路由指定管理距离。配置距离，在 RIP 路由配置模式下使用以下命令：

distance *distance-value ip-address/netmask*

- *distance-value* – 指定管理距离。范围是 1 到 255。用该命令指定的距离优先级高于 RIP 基本配置中的缺省距离（通过 **distance** *distance-value* 指定）。
- *ip-address/netmask* – 指定网络的 IP 地址，例如 10.200.0.0/16。

用户可以配置多条该命令为从不同的网络更新的路由指定距离。

使用 **no distance** *ip-address/netmask* 命令删除指定的管理距离。

RIP 数据库

Hillstone 设备运行 RIP 协议，就拥有一个 RIP 路由数据库，该数据库中储存了所有可达目的网络的路由条目。路由条目包含的信息有目的地址、下一跳、度量、来源以及定时器信息。用户可以在任何模式下，通过以下命令，随时查看 RIP 数据库的信息：

show ip rip database [*A.B.C.D/M*] [**vrouter** *vrouter-name*]

- *A.B.C.D/M* – 显示指定目的 IP 地址的 RIP 信息。
- **vrouter** *vrouter-name* – 显示指定 VRouter 的 RIP 信息。StoneOS 目前只支持 trust-vr 一个 VRouter。

配置接口的 RIP 功能

RIP 功能在 Hillstone 设备接口上的配置包括：认证方式、发送和接收的 RIP 版本号以及水分割功能。接口的 RIP 功能配置需要在接口配置模式下完成。

配置 RIP 报文认证

只有 RIP-2 支持 RIP 报文认证。认证方式有两种，分别是明文认证和 MD5 密文认证。明文认证不能提供安全保障。未加密的认证字随 RIP 报文一同传送，所以明文认证不能用于安全性要求较高的情况。默认为明文认证。用户需要配置 RIP 报文的认证方式和认证码。在接口配置模式下，使用以下命令：

- 方式：**ip rip authentication mode** {**md5** | **text**}
- 认证码：**ip rip authentication string** *string*

使用以上两个命令 no 的形式可以取消对认证方式和认证码的指定：

- **no ip rip authentication mode**
- **no ip rip authentication string**

配置发送和接收的 RIP 版本号

默认情况下，接口发送 RIP-2 信息。指定接口发送 RIP 信息的版本号，在接口配置模式下，使用以下命令：

ip rip send version [1][2]

- **1** – 指定只发送 RIP-1 的 RIP 信息。
- **2** – 指定只发送 RIP-2 的 RIP 信息。

使用 **no ip rip send version** 命令恢复默认版本号。

默认情况下，接口接收 RIP-2 信息。指定接口接收 RIP 信息的版本号，在接口配置模式下，使用以下命令：

ip rip receive version [1][2]

- **1** – 指定只接收 RIP-1 的 RIP 信息。
- **2** – 指定只接收 RIP-2 的 RIP 信息。

使用 **no ip rip receive version** 命令恢复默认版本号。

配置水平分割

水平分割是指不从本接口发送从该接口学到的路由。它可以在一定程度上避免产生路由环，保证路由的正确传播。配置水平分割功能，在接口配置模式下，使用以下命令：

开启水平分割：**ip rip split-horizon**

关闭水平分割：**no ip rip split-horizon**

显示系统 RIP 信息

用户可以通过 show 命令随时查看系统的 RIP 信息。查看 RIP 信息，在任何模式下使用以下命令：

show ip rip

配置 OSPF

OSPF 是开放式最短路径优先协议（Open Shortest Path First）的缩写。它是 IETF 组织开发的一个基于链路状态的内部网关协议。当前的 OSPF 版本为版本 2（RFC2328）。OSPF 适应各

种规模的网络，快速收敛特性能够在网络拓扑结构发生变化后立即发送更新报文，并且其算法本身决定了不会生成路由环路。OSPF 还具有以下特性：

- 区域划分：将自治系统的网络划分成区域来管理，从而减少了协议对 CPU 和内存的占用，提高性能。
- 无类路由：无类路由特性允许可变长子网掩码的使用。
- 等价路由：支持等价路由，提高多条路由的利用率。
- 组播发送：支持组播地址发送，减少对非 OSPF 设备的影响。
- 支持验证：支持基于接口的报文验证以保证路由计算的安全性。

说明：“自治系统”是处于一个管理机构控制之下的路由器和网络群组。一个自治系统中的所有路由器必须运行相同的路由协议。

OSPF 协议配置

用户可以为不同的 VRouter 分别配置 OSPF 协议。OSPF 协议配置包括以下各项：

- 配置 Router ID
- 配置区域认证
- 配置接口的网络类型
- 配置区域的路由聚合
- 配置区域的缺省花费
- 配置区域的虚拟链路
- 配置 stub 区域
- 配置 NSSA 区域
- 配置接口发送 OSPF 报文的缺省花费
- 配置缺省度量
- 配置缺省信息发布
- 配置缺省距离
- 配置 OSPF 定时器
- 指定运行 OSPF 协议的接口网络
- 引入路由
- 配置路由映射表
- 匹配多条路由匹配规则

- 修改引入路由属性
- 配置路由访问控制列表
- 配置距离
- 配置被动接口

OSPF 协议的基本配置需要在 OSPF 路由模式下进行。进入 OSPF 路由模式，请在 VRouter 配置模式下，使用以下命令：

ip vrouter *vrouter-name* （进入 VRouter 配置模式）

router ospf [*process-id*]（进入 OSPF 路由模式，同时开启 Hillstone 设备的 OSPF 功能）

- *process-id* – 指定 OSPF 的进程 ID。默认值是 1，取值范围是 1 到 65535。每个 OSPF 进程相互独立，有各自的链路状态数据库和对应的 OSPF 路由表信息。每一个 VRouter 支持最多 4 个 OSPF 进程，多个进程共同维护一个 VRouter 的路由表。

在指定 OSPF 进程 ID 时，注意如下事项：

- 每个 OSPF 进程中运行 OSPF 协议的接口网络不能重叠。
- 当多个 OSPF 进程中存在相同前缀的路由条目时，首先比较比较各个路由条目的管理距离，管理距离低的将被优先加入到 VRouter 的路由表中；管理距离相同时，，优先发现的的路由条目将被加入到 VRouter 的路由表中。
- 当其他路由协议引入 OSPF 路由时，将默认引入进程 ID 为 1 的 OSPF 路由信息。如果此进程不存在，将无法引入 OSPF 路由。

在 VRouter 配置模式下，使用 **no router ospf** [*process-id*]关闭 OSPF 功能。

配置 Router ID

每一台运行 OSPF 协议的路由器都必须拥有一个 Router ID。Router ID 是每个路由器在整个 OSPF 域中唯一标识，使用 IP 地址的形式表示。为 Hillstone 设备的 OSPF 协议配置 Router ID，在 OSPF 路由模式下，使用以下命令：

router-id *A.B.C.D* [**local**]

- *A.B.C.D* – 指定 OSPF 协议使用的 Router ID，为 IP 地址形式。
- **local** – 指定 OSPF 协议的 Router ID 为本地配置，该配置适用于 HA A/A 工作模式，并且不进行 HA 配置同步。默认情况下，Router ID 为非本地配置。

配置区域认证

用户可以配置区域的认证方式。默认情况下，区域是没有认证方式的。配置区域的认证方式，在 OSPF 路由模式下，使用以下命令：

area {*id* | *A.B.C.D*} **authentication** [**message-digest**]

- *id* | *A.B.C.D* – 指定区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- [**message-digest**] – 指定使用 MD5 认证方式。如果不使用该关键字，则为明文认证。

用该命令指定的认证类型必须与区域内其它的路由相同。同一网络中通过 OSPF 协议通信的路由器的认证密码必须相同。

使用 **no area** {*id* | *A.B.C.D*} **authentication** 命令取消对认证方式的指定。

配置接口的网络类型

OSPF 协议的接口的网路类型有以下三种：广播、点到点（Point-to-point）以及点到多点（Point-to-multipoint）网络类型。默认情况下，接口的网络类型为广播类型。配置接口的网络类型，在接口配置模式下，使用以下命令：

ip ospf network {point-to-point | point-to-multipoint}

- **point-to-point** – 指定接口网络类型为点到点网络类型。
- **point-to-multipoint** -指定接口网络类型为点到多点网络类型。

在隧道接口配置模式下，使用该命令 no 的形式恢复接口网络类型为广播类型：

no ip ospf network

配置区域的路由聚合

路由聚合是指将具有相同前缀的路由信息通过 ABR 聚合在一起，只发布一条路由到其它区域。一个区域可以配置多条聚合网段，这样 OSPF 可以对多个网段进行聚合。默认情况下，区域的路由聚合功能是关闭的。配置区域的路由聚合，在 OSPF 路由模式下，使用以下命令：

area {*id* | *A.B.C.D*} **range** {*A.B.C.D/M*} [**advertise** | **not-advertise**]

- *id* | *A.B.C.D* – 指定需要进行路由聚合的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- **range** {*A.B.C.D/M*} – 指定被聚合的网段。
- **advertise** – 指定将这一网段的路由聚合并通告聚合后的路由。
- **not-advertise** – 指定将这一网段的路由聚合且不通告聚合后的路由。

路由聚合功能仅对区域边界路由（连接骨干区域和非骨干区域的路由器，简称为 ABR）有效。

使用 **no area** {*id* | *A.B.C.D*} **range** {*A.B.C.D/M*} [**advertise** | **not-advertise**] 命令取消路由聚合的配置。

配置区域的缺省花费

区域的缺省花费是指将报文发送到 stub 区域的缺省路由花费。指定区域的缺省花费，在 OSPF 路由模式下，使用以下命令：

area {*id* | *A.B.C.D*} **default-cost** *cost-value*

- *id* | *A.B.C.D* – 指定需要指定缺省花费的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- *cost-value* – 指定花费值。默认值是 1。范围是 0 到 16777214。

使用 **no area** {*id* | *A.B.C.D*} **default-cost** 命令恢复缺省花费的配置。

注意：该命令仅对 NSSA 区域有效。

配置区域的虚拟链路

虚拟链路（Virtual Links）用来连接不连续的骨干区域，使他们能够保持逻辑上的连续性。配置虚拟链路以及定时器参数，在 OSPF 路由模式下，使用以下命令：

area {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* [**hello-interval** *interval-value*] [**retransmit-interval** *interval-value*] [**transmit-delay** *interval-value*] [**dead-interval** *interval-value*]

- *id* | *A.B.C.D* – 需要做虚拟链路进行连接的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- **virtual-link** *A.B.C.D* – 指定作为虚拟链路路由器的 Router ID。
- **hello-interval** *interval-value* – 指定接口发送 Hello 报文的时间间隔，单位为秒，默认值是 10 秒。范围是 1 到 65535 秒。
- **retransmit-interval** *interval-value* – 一台路由器向它的邻居发送一条 LSA 后需要获得对方的确认报文。若在指定的时间内没有收到对方的确认报文，就会向邻居重传这条 LSA。该参数用来指定邻接路由器之间重传 LSA 的时间间隔，单位为秒，默认值是 5 秒。范围是 3 到 65535 秒。
- **transmit-delay** *interval-value* – 指定更新包的延迟时间，单位为秒，默认值是 1 秒。范围是 1 到 65536 秒。
- **dead-interval** *interval-value* – 如果路由器在一定的时间内都没有收到对方的 Hello 报文，则认为对端路由器失效，这个一定的时间就是相邻路由器间的失效时间。该参数指定失效时间值，单位为秒，默认值是 40 秒。范围是 1 到 655635 秒。

使用 **no area** {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* [**hello-interval**] [**retransmit-interval**] [**transmit-delay**] [**dead-interval**]命令恢复定时器的默认

时间值。

用户可以配置虚拟链路的认证方式。在 OSPF 路由模式下，使用以下命令：

area {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest**] [**authentication-key** *string*] [**message-digest-key** *ID* **md5** *string*] [**null**]

- *id* | *A.B.C.D* – 需要做虚拟链路进行连接的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- **virtual-link** *A.B.C.D* – 指定作为虚拟链路路由器的 Router ID。
- **message-digest** – 指定使用 MD5 认证。
- **authentication-key** *string* – 指定明文认证的认证密码。
- **message-digest-key** *ID* **md5** *string* – 指定 MD5 认证的认证 ID 和密码。
- **null** – 不使用认证。

使用 **no area** {*id* | *A.B.C.D*} **virtual-link** *A.B.C.D* **authentication** [**message-digest**] [**authentication-key** *string*] [**message-digest-key** *ID*]命令取消认证配置。

配置 stub 区域

stub 区域是不收发 Type-5 的 LSA（AS-external-LSAs）区域。对于产生大量 Type-5 LSA 的网络，这种处理方式能够有效减小 stub 区域内路由器的 LSDB 规模，并缓解 SPF 计算对路由器资源的占用。stub 区域通常位于自治系统边界。配置 OSPF 的 stub 区域，在 OSPF 路由模式下，使用以下命令：

area {*id* | *A.B.C.D*} **stub** [**no-summary**]

- *id* | *A.B.C.D* – 指定 stub 区域的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。
- **no-summary** – 阻止 ABR 向 stub 区域发送 3 类或 4 类汇总 LSA。

使用 **no area** {*id* | *A.B.C.D*} **stub** [**no-summary**]命令取消 stub 区域的配置。

配置 NSSA 区域

Stub 区域不能引入外部路由，为了在允许将自治系统外部路由通告到 OSPF 路由域内部的同时，保持其余部分的 Stub 区域的特征，网络管理员可以将区域配置为 NSSA 区域。配置 OSPF 的 NSSA 区域，在 OSPF 路由模式下，使用以下命令：

area {*id* | *A.B.C.D*} **nssa** [**no-summary** | **no-redistribution** | **default-information-originate**]

- *id* | *A.B.C.D* – 指定 NSSA 区域的区域 ID。区域 ID 用 32 比特数来表示，可以是数字

形式，也可以是 IP 地址形式。

- **no-summary** | **no-redistribution** | **default-information-originate** – **no-summary** 参数只用于 NSSA 区域的 ABR，配置后，NSSA ABR 只通过 Type-3 的 Summary-LSA 向区域内发布一条缺省路由，不再向区域内发布任何其它 Summary-LSAs（这种区域又称为 Totally NSSA 区域）。**no-redistribution** 参数用于禁止将 AS 外部路由以 Type-7 LSA 的形式引入到 NSSA 区域中，这个参数通常只用在既是 NSSA 区域的 ABR，也是 OSPF 自治系统的 ASBR 的路由器上，以保证所有外部路由信息能正确地进入 OSPF 路由域。**default-information-originate** 参数只用于 NSSA 区域的 ABR 或 ASBR，配置后，对于 ABR，不论本地是否存在缺省路由，都将生成一条 Type-7 LSA 向区域内发布缺省路由；对于 ASBR，只有当本地存在缺省路由时，才产生 Type-7 LSA 向区域内发布缺省路由。

使用 **no area** {*id* | *A.B.C.D*} **nssa** [**no-summary** | **no-redistribution** | **default-information-originate**]命令取消 NSSA 区域的配置。

配置 OSPF 的引用带宽

OSPF 可以根据接口的带宽计算接口发送 OSPF 报文的花费。配置 OSPF 的引用带宽，在 OSPF 路由模式下，使用以下命令：

auto-cost reference-bandwidth *bandwidth*

- *bandwidth* – 指定带宽值，单位为 Mbps，默认值是 100。范围是 1 到 4294967。

使用 **no auto-cost reference-bandwidth** 命令使 OSFP 根据接口的类型计算接口发送 OSPF 报文的花费。

指定缺省度量

此处配置的 OSPF 协议的缺省度量在引入路由时生效。指定 OSPF 的缺省度量，在 OSPF 路由配置模式下使用以下命令：

default-metric *value*

- *value* – 指定缺省度量值。范围是 1 到 16777214。

使用 **no default-metric** 命令恢复缺省度量的默认值。

配置缺省信息发布

用户可以指定是否将默认路由发布到其它使用 OSPF 协议的路由器。默认情况下，是不发送默认路由的。配置缺省信息发布，在 OSPF 路由配置模式下使用以下命令：

default-information originate [**always**] [**type** {**1** | **2**}] [**metric** *value*]

- **always** – OSPF 无条件产生并发送默认路由。
- **type** {**1** | **2**} – 指定与发送到 OSPF 路由域的默认路由相关联的外部路由的类型。**1** 指 type1 外部路由，**2** 指 type2 外部路由。
- **metric** *value* – 指定发送默认路由的度量。如果不使用该命令配置度量并且也没有使用 **default-metric** *value*配置默认度量,其默认度量将会是 20。范围是 0 到 16777214。

使用 **no default-information originate** 命令恢复默认值。

指定缺省距离

指定 OSPF 路由的缺省距离，在 OSPF 路由配置模式下使用以下命令：

distance distance-*value*

- distance-*value* – 指定缺省管理距离。范围是 1 到 255，默认值是 110。

使用 **no distance** 命令恢复缺省距离的默认值。

配置 OSPF 定时器

用户可以指定以下两个 OSPF 协议的定时器：OSPF 收到更新后在多长时间内进行重新计算以及 OSPF 两次计算的时间间隔。配置 OSPF 定时器，在 OSPF 路由配置模式下使用以下命令：

timers spf *delay1 delay2*

- *delay1* – 收到更新后，在该指定时间内进行重新计算，单位为秒。范围是 0 到 65535，默认值是 5 秒。
- *delay2* – 指定两次计算的时间间隔，单位为秒。范围是 0 到 65535，默认值是 10 秒。

使用 **no timers spf** 命令恢复默认值。

指定运行 OSPF 协议的接口网络

指定运行 OSPF 协议的接口网络并且将网络配置到指定的区域中，在 OSPF 路由配置模式下使用以下命令：

network *A.B.C.D/M* **area** {*id* | *A.B.C.D*}

- *A.B.C.D/M* – 指定运行 OSPF 协议的接口网络。
- **area** {*id* | *A.B.C.D*} – 指定将网络添加到的区域 ID。区域 ID 用 32 比特数来表示，可以是数字形式，也可以是 IP 地址形式。

使用 **no network** *A.B.C.D/M* **area** {*id* | *A.B.C.D*}命令取消对网络的指定。

引入路由

OSPF 协议允许用户引入其他 OSPF 进程路由信息以及其它路由协议（BGP、IS-IS、直连、静态、RIP 和 VPN）的路由信息，并向外发布。用户可以设置被引入路由的度量以及外部路由的类

型，还可以引用路由映射表对路由信息进行过滤，仅允许引入或拒绝引入特定的路由信息。配置引入路由，在 OSPF 路由配置模式下使用以下命令：

redistribute {**bgp** | **connected** | **isis** | **ospf** *process-id* | **static** | **rip** | **vpn**} [**type** {**1** | **2**}] [**metric** *value*] [**route-map** *name*] [**tag** *tag-value*]

- **bgp** | **connected** | **isis** | **ospf** *process-id* | **static** | **rip** | **vpn**– 指定引入路由的类型，可以是 BGP（**bgp**）、ISIS(**isis**)、指定的 OSPF 进程（**ospf** *process-id*)、直连路由（**connected**)、静态路由（**static**)、RIP（**rip**）或者 VPN 路由（**vpn**)。
- **type** {**1** | **2**} – 指定外部路由的类型。**1** 指 type1 外部路由，**2** 指 type2 外部路由。
- **metric** *value* – 指定引入路由的度量。范围是 0 到 16777214。如果不指定该数值，系统会使用 OSPF 的缺省度量（通过 **default-metric** *value* 配置)。
- **route-map** *name* –指定用于过滤引入路由信息的路由映射表。有关路由映射表的更多信息，请参考 “配置路由映射表”。
- **tag** *tag-value* – 指定引入的路由的标记值。取值范围是 1 到 4294967295。

用户可以配置多条该命令引入不同类型的路由。

使用 **no redistribute** {**bgp** | **connected** | **static** | **rip**}命令取消指定类型路由的引入。

配置路由映射表

默认情况下系统会引入所有的路由信息。用户可以引用路由映射表对引入的路由信息进行过滤。路由映射表主要由路由匹配规则和匹配成功后所执行操作（允许或拒绝）两部分组成。如果引入的路由信息命中了任何路由匹配规则，系统就会执行对应的操作，允许或拒绝引入这些路由信息。

注意:

- 如果用户设置的操作是允许，匹配成功后系统仅允许引入匹配的路由信息，拒绝引入所有未匹配的路由信息。
- 如果用户设置的操作是拒绝，匹配成功后系统会拒绝引入匹配的路由信息，但仍允许引入未匹配的路由信息。

用户可通过以下步骤配置路由映射表，实现对引入路由信息的过滤：

1.创建路由映射表并在表中创建路由匹配规则。不同的匹配规则通过序列号区分。序列号越小，匹配优先级越高。默认情况下，引入的路由信息命中任何路由匹配规则，系统将不再继续匹配后续的规则；如果引入的路由信息没有命中任何匹配规则，系统将执行拒绝操作。

2.在路由匹配规则中配置匹配条件。匹配条件可以是引入路由的度量值、目的地址、下一跳地址或下一跳接口。一条路由匹配规则中可以包含多个匹配条件，这些匹配条件之间是与（AND）关

系，即引入的路由信息必须满足匹配规则中的所有匹配条件才会认定为命中了该条规则。

3.如果匹配条件为路由的目的地址或下一条地址，配置匹配时所引用的路由访问控制列表。有关路由访问控制列表的更多信息，请参考“配置路由访问控制列表”。

4.如有需要，设置系统在命中一条路由匹配规则后继续匹配其他规则。

5.如有需要，修改引入路由的部分属性后再对外发布

创建路由映射表并在表中配置路由匹配规则，在全局配置模式下，使用以下命令：

route-map *name* **{deny | permit}** *sequence*

- **route-map** *name* – 指定路由映射表名称，并进入路由映射表配置模式。取值范围是 1 到 31 个字符。如果该名称已经存在，则直接进入路由映射表配置模式。
- **deny | permit** – 指定对匹配的路由信息所执行的操作。deny 为拒绝，permit 为允许。
- *sequence* – 指定该路由映射表下路由匹配规则的序列号。取值范围是 1 到 65535。

使用该命令 no 的形式删除路由映射表：

no route-map *name* [*sequence*]

- *sequence* – 仅删除路由映射表中指定的匹配规则。

配置路由匹配规则中的匹配条件，在路由映射表配置模式下，使用以下命令：

match {**as-path** *access-list-number* | **community** {*community-list-name* | *community-list-number*} [exact-match] | **metric** *metric-value* | **interface** *interface-name* | **ip address** *access-list* | **ip next-hop** *access-list* | **tag** *tag-value* }

- **as-path** *access-list-number* – 匹配路由的 AS 路径。*access-list-number* 为用户配置的 AS 路径访问控制列表号。如果路由的 AS 路径匹配该访问控制列表中允许的 AS 路径，则认为匹配成功。有关 AS 路径访问控制列表配置的更多信息，请参考“配置 AS 路径访问控制列表 ”。
- **community** {*community-list-name* | *community-list-number*} [exact-match] – 匹配路由的团体属性。*community-list-name* 为团体属性列表名称；*community-list-number* 为团体属性列表号；exact-match 指定对团体属性进行精确匹配。有关团体属性列表列表配置的更多信息，请参考“配置团体属性列表 ”。
- **metric** *metric-value* – 匹配路由的度量值。取值范围是 0 到 4294967295。
- **interface** *interface-name* – 匹配路由的下一跳接口。
- **ip address** *access-list* – 匹配路由的目的地址。*access-list* 为用户配置的路由访问控制列表。如果路由的目的地址属于该访问控制列表中允许的地址，则认为匹配成功。有关访问控制列表配置的更多信息，请参考“配置路由访问控制列表”。
- **ip next-hop** *access-list* – 匹配路由的下一跳地址。*access-list* 为用户配置的

路由访问控制列表。如果路由的下一跳地址属于该访问控制列表中允许的地址，则认为匹配成功。有关访问控制列表配置的更多信息，请参考“配置路由访问控制列表”。

- **tag** *tag-value* – 匹配 OSPF 协议的路由的标记值。如果此处配置的路由的标记值匹配静态路由中的标记值，则认为匹配成功。取值范围是 1 到 4294967295。

重复以上命令向路由匹配规则中添加多个匹配条件。使用该命令 no 的形式删除匹配条件：

no match {**metric** | **interface** | **ip address** | **ip next-hop**}

注意：如果用户仅创建了路由映射表但没有在映射表中配置任何路由匹配规则，系统默认会认为引入的路由信息匹配成功。

例如，设置 OSPF 协议仅引入 BGP 协议中下一跳接口为 eth0/1 且度量值为 50 的路由信息，命令行如下：

```
hostname(config)# route-map test permit 10
hostname(config-route-map)# match interface ethernet0/1
hostname(config-route-map)# match metric 50
hostname(config-route-map)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

匹配多条路由匹配规则

默认情况下，如果引入的路由信息命中任何路由匹配规则，系统将不再继续匹配后续的规则。用户可以要求系统在命中一条规则后仍继续匹配其他规则，以实现更精细的控制。设置系统在匹配成功后继续匹配其他规则，在路由映射表配置模式下，使用以下命令：

continue [*sequence*]

- *sequence* – 指定继续匹配的规则序列号。取值范围是 1 到 65535。该序列号必须大于当前规则的序列号。如果没有指定此参数，系统在当前规则匹配成功后会继续匹配下一条规则。

使用该命令 no 的形式取消继续匹配其他规则：

no continue

例如，也可以通过以下命令行设置 OSPF 协议仅引入 BGP 协议中下一跳接口为 eth0/1 且度量值为 50 的路由信息：

```
hostname(config)# route-map test permit 10
hostname(config-route-map)# match interface ethernet0/1
hostname(config-route-map)# continue 20
hostname(config-route-map)# exit
hostname(config)# route-map test permit 20
hostname(config-route-map)# match metric 50
```

```
hostname(config-route-map)# exit
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

修改引入路由属性

对于满足匹配条件的引入路由，用户可以在修改路由的部分属性后再对外发布。修改引入路由的属性，在路由映射表配置模式下，使用以下命令：

set {**metric** *metric-value* | **metric-type** {**type-1** | **type-2**}| **tag** *tag-value*}

- **metric** *metric-value* – 修改引入路由的度量值。取值范围是取值范围是 0 到 4294967295。
- **metric-type** {**type-1** | **type-2**} – 修改外部路由的度量类型。**type-1** 指 type1 类型外部路由度量，**type-2** 指 type2 类型外部路由度量。
- **tag** *tag-value* – 指定 OSPF 协议的引入路由的标记值。取值范围是 1 到 4294967295。

使用该命令 no 的形式取消对路由属性的修改并还原到引入路由时的设置：

no set {**metric** | **metric-type | tag** }

配置路由访问控制列表

路由匹配规则中的目的地址和下一跳地址匹配是通过引用路由访问控制列表实现的。路由访问控制列表主要由 IP 地址匹配规则和匹配成功后所执行操作（允许或拒绝）两部分组成。如果目的地址或下一跳地址匹配指定的 IP 地址，系统会继续执行指定的操作。一个路由访问控制列表中可以包含多条 IP 地址匹配规则，系统按照添加时间顺序依次匹配，命中任何一条规则会立即结束匹配；如果匹配失败，系统会执行拒绝操作。

配置路由访问控制列表，在全局配置模式下，执行以下命令：

access-list route *name* {**deny** | **permit**} {*A.B.C.D/M* [**exact-match**] | **any**}

- *name* – 指定路由访问控制列表的名称并进入路由访问控制列表配置模式。取值范围是 1 到 31 个字符。如果该名称已经存在，则直接进入路由访问控制列表配置模式。
- **deny | permit** – 指定对匹配的 IP 地址所执行的操作。deny 为拒绝，permit 为允许。
- *A.B.C.D/M* – 指定需要匹配的 IP 地址或 IP 地址前缀（不包括掩码）。
- **exact-match** – 对 IP 地址前缀进行精确匹配（包括掩码）。
- **any** – 匹配任意 IP 地址。

使用该命令 no 的形式删除路由访问控制列表：

no access-list route *name* [{**deny** | **permit**} {*A.B.C.D/M* [**exact-match**] | **any**}]

如果指定了具体的 IP 地址匹配规则，该命令只从路由访问控制列表中删除对应的规则而不会删除

整个访问控制列表。

对路由访问控制列表添加描述信息，在全局配置模式下，使用以下命令：

access-list route *name* **description** *description*

- *name* – 指定路由访问控制列表的名称。取值范围是 1 到 31 个字符。
- *description* – 指定描述信息。取值范围是 1 到 31 个字符。

使用该命令 no 的形式删除描述信息：

no access-list route *name* **description**

例如，设置 OSPF 协议拒绝引入 BGP 协议中下一跳地址为 192.168.1.1 和 192.168.2.0 网段中 IP 地址和的路由信息，命令行如下：

```
hostname(config)# route-map test deny 10
hostname(config-route-map)# match ip next-hop access_list
hostname(config-route-map)# exit
hostname(config)# access-list route access_list permit 192.168.1.1/32
hostname(config)# access-list route access_list permit 192.168.2.0/24
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# redistribute bgp route-map test
hostname(config-router)# end
```

配置距离

用户可以根据路由类型指定管理距离。配置距离，在 OSPF 路由配置模式下使用以下命令：

distance ospf {**intra-area** *distance-value* | **inter-area** *distance-value* | **external** *distance-value*}

- **intra-area** *distance-value* – 指定区域内路由的管理距离。默认值是 110。范围是 1 到 255。
- **inter-area** *distance-value* – 指定区域间路由的管理距离。默认值是 110。范围是 1 到 255。
- **external** *distance-value* – 指定外部 type5 类型路由的管理距离。默认值是 110。范围是 1 到 255。

使用 **no distance ospf** 命令恢复距离的默认值。

配置被动接口

用户可以将一些接口配置为只接收更新但是不发送，这种只接收更新的接口就是被动接口。配置被动接口，在 OSPF 路由配置模式下使用以下命令：

passive-interface *interface-name*

- *interface-name* – 指定接口的名称作为被动接口。

用户可以配置多条该命令添加多个被动接口。

使用 **no passive-interface** *interface-name* 命令取消被动接口的配置。

配置基于路由访问控制列表的路由过滤

OSFP 协议支持通过路由访问控制列表对引入的路由进行过滤。配置基于路由访问控制列表的路由过滤，在 OSPF 路由配置模式下，使用以下命令：

distribute-list *access-list-name* **in** [*interface-name*]

- *access-list-name* – 指定路由访问控制列表的名称。关于路由访问控制列表的更多信息，请参考“配置路由访问控制列表”。
- **in** – 指定对引入的路由（**in**）进行过滤。
- *interface-name* – 指定接口名称。指定后，将过滤从指定接口学习到的 OSPF 路由。如果不指定接口名称，系统将过滤所有 OSPF 路由。

使用该命令 no 的形式取消基于路由访问控制列表的路由过滤的配置：

no distribute-list *access-list-name* **in** [*interface-name*]

配置接口 OSPF 功能

接口的 OSPF 功能配置需要在接口配置模式下完成。OSPF 协议在 Hillstone 设备接口上的配置包括：

- 配置接口的 OSPF 认证
- 指定接口的链路花费
- 配置接口定时器
- 指定接口路由器优先级
- 配置接口的网络类型

配置接口的 OSPF 认证

接口的 OSPF 认证优先于区域 OSPF 认证。Hillstone 设备支持明文认证和 MD5 认证。默认情况下，接口的 OSFP 认证是关闭的。开启或者关闭接口的 OSPF 认证功能，在接口配置模式下使用以下命令：

ip ospf authentication
no ip ospf authentication

配置明文认证的认证密码，在接口配置模式下，使用以下命令：

ip ospf authentication-key *string*

- *string* – 指定认证密码（最多为 8 个字符）。

使用 **no ip ospf authentication-key** 命令取消密码配置。

配置 MD5 认证 ID 和密码，在接口配置模式下，使用以下命令：

ip ospf message-digest-key *ID* **md5** *string*

- *ID* – 指定认证 ID。
- *string* – 指定认证密码。

使用 **no ip ospf message-digest-key** *ID* 命令取消密码配置。

指定接口的链路花费

指定接口的链路花费，在接口配置模式下，使用以下命令：

ip ospf cost *cost-value* [**local**]

- *cost-value* – 指定接口的链路花费。取值范围是 1 到 65535。
- **local** – 指定接口的链路花费为 **local**。当设备处于 HA AA 模式时，配置此参数，该接口的链路花费值将不会同步到备份设备，从而使两台设备具有不同的链路花费值，避免出现非对称 OSPF 路由。

使用 **no ip ospf cost** [**local**]命令取消对所需花费的指定。

配置接口定时器

接口的定时器有以下四个：接口发送 Hello 包的时间间隔、接口相邻路由器的失效时间、接口重传 LSA 的时间间隔以及接口更新包的延迟时间。

指定接口发送 Hello 包的时间间隔，在接口配置模式下，使用以下命令：

ip ospf hello-interval *interval*

- *interval* – 指定接口发送 Hello 包的时间间隔，单位为秒。默认值是 10 秒。范围是 1 到 65535 秒。

使用 **no ip ospf hello-interval** 恢复默认时间间隔。

如果接口在一定的时间内都没有收到对方的 Hello 报文，则认为对端路由器失效，这个一定的时间就是相邻路由器间的失效时间。指定接口的相邻路由失效时间，在接口配置模式下，使用以下命令：

ip ospf dead-interval *interval*

- *interval* – 指定接口的相邻路由失效时间，单位为秒。默认值是 40 秒（发送 Hello 包时间间隔的 4 倍)。范围是 1 到 65535 秒。

使用 **no ip ospf dead-interval** 恢复默认失效时间。

指定接口重传 LSA 的时间间隔，在接口配置模式下，使用以下命令：

ip ospf retransmit-interval *interval*

- *interval* – 指定接口重传 LSA 的时间间隔，单位为秒。默认值是 5 秒。范围是 3 到 65535 秒。

使用 **no ip ospf retransmit-interval** 恢复默认时间间隔。

指定接口更新包的延迟时间，在接口配置模式下，使用以下命令：

ip ospf transmit-delay *interval*

- *interval* – 指定接口更新包的延迟时间，单位为秒。默认值是 1 秒。范围是 1 到 65535 秒。

使用 **no ip ospf transmit-delay** 恢复默认延迟时间。

指定接口路由器优先级

路由器的优先级用来决定使用哪个路由器作为指定路由器。指定路由器用来接收网络中所有其它路由器的链路信息，并将收到的链路信息广播出去。指定接口路由器的优先级，在接口配置模式下，使用以下命令：

ip ospf priority *level*

- *level* – 指定路由器的优先级。默认值是 1。范围是 0 到 255。优先级为 0 的路由器不会被选中作为指定路由器。当同一个网络的两个路由器都可作为指定路由器时，优先级高的路由器会被选中；如果优先级也相同，Router ID 高的会被选中。

使用 **no ip ospf priority** 命令恢复默认优先级。

配置接口的网络类型

OSPF 协议的接口的网路类型有以下三种：广播、点到点（Point-to-point）以及点到多点（Point-to-multipoint）网络类型。默认情况下，接口的网络类型为广播类型。配置接口的网络类型，在接口配置模式下，使用以下命令：

ip ospf network {point-to-point | point-to-multipoint}

- **point-to-point** – 指定接口网络类型为点到点网络类型。
- **point-to-multipoint** -指定接口网络类型为点到多点网络类型。

在隧道接口配置模式下，使用该命令 no 的形式恢复接口网络类型为广播类型：

no ip ospf network

显示 OSPF 信息

显示 OSPF 路由信息，在任何模式下使用以下命令：

show ip route ospf [**vrouter** *vrouter-name*]

- *vrouter-name* – 显示指定的 VRouter 的 OSPF 路由信息。

显示防火墙的 OSPF 信息，在任何模式下使用以下命令：

show ip ospf [**vrouter** *vrouter-name*] [**process** *process-id*]

- *vrouter-name* – 指定 VRouter 名称。

- **process** *process-id* – 指定 OSPF 进程 ID。

显示防火墙 OSPF 协议的数据库信息，在任何模式下使用以下命令：

show ip ospf database {**asbr-summary** | **external** | **nssa-external** | **network** | **router** | **summary**} [*A.B.C.D*] [{**adv-router** *A.B.C.D*} | **self-originate**] [**vrouter** *vrouter-name*] [**process** *process-id*]

- **asbr-summary** – 显示自制系统边界路由 LSAs。
- **external** – 显示外部路由 LSAs。
- **nssa-external** - 显示 NSSA 的外部 LSA 的有关信息。
- **network** – 显示网络 LSAs。
- **router** – 显示路由 LSAs。
- **summary** – 显示汇总 LSAs。
- *A.B.C.D* – 链路状态 ID，以 IP 地址形式表示。
- **adv-router** *A.B.C.D* – 显示指定路由器的 LSAs。
- **self-originate** - 只显示自己产生的 LSA（从本地路由器）。
- *vrouter-name* – 指定 VRouter 名称。
- **process** *process-id* – 指定 OSPF 进程 ID。

show ip ospf database [**max-age** | **self-originate**] [**vrouter** *vrouter-name*] [**process** *process-id*]

- **max-age** - 指定最大老化时间。
- **self-originate** - 只显示自己产生的 LSA（从本地路由器）。
- *vrouter-name* – 指定 VRouter 名称。
- **process** *process-id* – 指定 OSPF 进程 ID。

显示 OSPF 接口信息，在任何模式下使用以下命令：

show ip ospf interface [*interface-name*] [**vrouter** *vrouter-name*] [**process** *process-id*]

显示 OSPF 虚拟链路信息，在任何模式下使用以下命令：

show ip ospf virtual-links [**vrouter** *vrouter-name*] [**process** *process-id*]

显示 OSPF 邻居信息，在任何模式下使用以下命令：

show ip ospf neighbor [*A.B.C.D* | **detail**] [**vrouter** *vrouter-name*] [**process** *process-id*]

显示 OSPF 路由信息，在任何模式下使用以下命令：

show ip ospf route [*A.B.C.D*] [**vrouter** *vrouter-name*] [**process** *process-id*]

显示路由映射表信息，在任何模式使用以下命令：

show route-map [*name*]

显示路由访问控制列表信息，在任何模式使用以下命令：

show access-list route [*name*]

显示 OSPF 路由过滤信息，在任何模式下使用以下命令：

show ip ospf distribute-list [**vrouter** *vrouter-name*] [**process** *process-id*]

配置 IS-IS

IS-IS （Intermediate System-to-Intermediate System）最初是 ISO 为 CLNP（Connection-Less Network Protocol) 设计的一种动态路由协议。为了提供对 IP 的路由支持，IETF（Internet Engineering Task Force）在 RFC 1195 中对 IS-IS 进行了扩充和修改，使它能够同时应用在 TCP/IP 和 OSI 环境中,称为集成化 IS-IS（Integrated IS-IS 或 Dual IS-IS)。IS-IS 属于 IGP (Interior Gateway Protocol)，用于自治系统内部。IS-IS 是一种链路状态协议，使用 SPF（Shortest Path First）算法进行路由计算。

StoneOS 支持应用在 TCP/IP 网络环境中的 IS-IS 动态路由协议。

用户可以为不同的 VRouter 分别配置 IS-IS 动态路由协议。IS-IS 协议配置包括以下各项：

- 指定路由器类型
- 使能接口 IS-IS
- 配置接口 IS-IS 类型
- 配置网络类型为点对点类型
- 配置 NET 地址
- 配置管理距离
- 配置度量类型
- 配置接口度量值
- 引入路由
- 发布缺省路由
- 配置 Hello 报文发送时间间隔
- 配置 Hello 报文失效乘数
- 配置 Hello 报文填充功能
- 配置被动接口
- 配置 DIS 选举优先级
- 配置 LSP 生成时间间隔
- 配置 LSP 最大生存时间
- 配置 LSP 刷新时间

- 配置 SPF 计算时间间隔
- 配置过载标志位
- 配置主机名映射
- 配置认证
- 配置接口认证模式

IS-IS 基本配置

IS-IS 动态路由协议的基本配置需要在 IS-IS 路由配置模式下进行。进入 IS-IS 路由配置模式，依次使用以下命令：

ip vrouter *vrouter-name* – 在全局配置模式下执行此命令，进入 VRouter 配置模式。

router isis – 进入 IS-IS 路由配置模式，同时在此 VRouter 创建一个 IS-IS 进程。每个 VRouter 的 IS-IS 进程之间相互独立。

需要关闭 IS-IS 进程时，在 VRouter 配置模式下，使用 **no router isis**。

指定路由器类型

路由器类型包括：Level-1 路由器，Level-2 路由器，以及 Level-1-2 路由器。指定路由器类型，在 IS-IS 路由配置模式下，使用如下命令：

is-type [level-1 | level-1-2 | level-2-only]

- **level-1 | level-1-2 | level-2-only** – 指定路由器类型为 Level-1 路由器（**level-1**），Level-2 路由器(**level-2**), Level-1-2 路由器（**level-1-2**）。路由器默认类型为 Level-1-2 类型。只有当路由器类型为 Level-1-2 时，用户可对接口的类型进行指定。

取消路由器类型配置，在 IS-IS 路由配置模式下，使用 **no is-type** 命令。

使能接口 IS-IS

默认情况下，IS-IS 功能在接口上处于关闭状态。在当前路由器上创建 IS-IS 进程后，需要在接口上使能 IS-IS。在接口配置模式下，使用如下命令：

isis enable

使用 **no isis enable** 命令在接口上关闭 IS-IS 功能。

配置接口 IS-IS 类型

当路由器类型是 Level-1 时，接口的邻接类型只能为 Level-1；当路由器类型是 Level-2 时，

接口的邻接类型只能为 Level-2;当路由器类型是 Level-1-2 时,接口的邻接类型默认为 level-1-2 类型。配置接口的邻接类型，在接口配置模式下，使用如下命令:

isis circuit-type [level-1 | level-1-2 | level-2-only]

- **level-1 | level-1-2 | level-2-only** – 指定接口类型为 level-1 邻接类型接口（level-1），level-2 邻接类型接口（level-2-only）或者 level-1-2 邻接类型接口（level-1-2）。

配置网络类型为点对点类型

当只有两台设备接入到广播网络时，可以配置接口所在链路的类型为点对点链路类型。对于点对点链路类型，IS-IS 不进行 DIS 选举和 CSNP 泛洪。在接口配置模式下，使用如下命令:

isis network point-to-point

使用 **no isis network point-to-point** 命令取消点对点链路类型设置。

IS-IS 路由信息配置

配置 NET 地址

NET（Network Entity Title，网络实体名称）指示的是 IS 本身的网络层信息，不包括传输层信息，可以看作是一类特殊的 NSAP，即 SEL 为 0 的 NSAP 地址。NET 地址用来标识开启 IS-IS 进程的设备。一个 IS-IS 进程的设备最多可以配置 3 个 NET 地址。这三个 NET 地址的区域地址可以不同，但是 System ID 必须相同。指定设备的 NET 地址，在 IS-IS 路由配置模式下，使用如下命令:

net *net*

- *net* – 指定 NET 地址。在建立 Level-1 邻居时，区域地址必须相同，否则无法建立邻居。在建立 Level-2 邻居时，不检查区域地址是否相同。

使用 **no net** *net* 命令取消对 NET 地址的设置。

配置管理距离

指定 IS-IS 路由的管理距离，在 IS-IS 路由配置模式下，使用以下命令:

distance *distance-value*

- *distance-valeu* – 为 IS-IS 路由指定管理距离。范围是 1 到 255，默认值是 115。

使用 **no distance** 命令恢复缺省管理距离。

配置度量类型

当度量类型为 narrow 时，路由器只生成和接收 metric field 的类型为 narrow 类型的报文。

接口度量值的取值范围为 0 到 63。对于大型网络，路由的最大度量值为 1023。当路由度量值大于 1023 时，认为目标不可达。当度量类型为 wide 时，路由器仅生成和接收 metric field 的类型为 wide 类型的报文。接口度量值的取值范围为 0 到 16777215。当度量类型为 transition 时，路由器既可以接收/发送 narrow 类型的报文，也可以接收/发送 wide 类型的报文。配置度量类型，在 IS-IS 路由配置模式下，使用如下命令：

metric-style {wide | narrow | transition}

- **wide** – 路由器仅生成和接收 metric field 的类型为 wide 类型的报文。
- **narrow** – 路由器只生成和接收 metric field 的类型为 narrow 类型的报文。默认为 narrow。
- **transition** – 路由器既可以接收/发送 narrow 类型的报文，也可以接收/发送 wide 类型的报文。

使用 **no metric-style** 恢复默认度量类型。

配置接口度量值

度量值用来计算经过此链路到达网络目的地址的链路开销。配置接口所在链路的度量值，在接口配置模式下，使用如下命令：

isis metric *value* **[level-1 | level-2]**

- *value* – 指定接口所在链路的度量值。取值范围为 1 到 16777214。默认值为 10。当接口的度量类型为 narrow 时，度量值不能超过 63。
- **level-1 | level-2** – 使用 **level-1** 参数指定 Level-1 路由信息的度量值。使用 **level-2** 参数指定 Level-2 路由信息的度量值。不指定 **level-1** 和 **level-2** 参数时，设置的度量值将会同时对 Level-1 和 Level-2 路由信息生效。

使用 **no isis metric** 命令恢复接口度量值的默认值。

引入路由

IS-IS 协议允许用户将设备上其它路由协议（直连、静态、OSPF、BGP 和 RIP）的路由信息引入到 IS-IS 中，并向外发布。同时，用户可以设置被引入路由的度量。配置引入路由，在 IS-IS 路由配置模式下使用以下命令：

redistribute {connected | static | ospf | bgp | rip} [level-1 | level-1-2 | level-2] [metric *value***] [metric-type {external | internal}]**

- **connected | static | ospf | bgp | rip** – 指定引入路由的类型，可以是直连路由（**connected**）、静态路由（**static**）、OSPF（**ospf**），BGP（**bgp**）或者 RIP（**rip**）。
- **level-1 | level-1-2 | level-2** – 指定引入路由的级别，可以作为 Level-1 路由

（**level-1**）、Level-2 路由（**level-2**）或者同时作为 Level-1 和 Level-2 路由（**level-1-2**）。默认值为 **level-2**。

- **metric** *value* – 指定引入路由的度量。范围是 0 到 4294967295。默认值为 0。当路由器的度量类型为 narrow 时，引入路由的度量值不能超过 63。
- **metric-type {external | internal}** – 当指定 metric 类型为 **external** 时，metric 值为使用命令 **metric** *value* 中配置的值加 64；当指定 metric 类型为 **internal** 时，metric 值为命令 **metric** *value* 中配置的数值。默认类型为 **internal**。

使用 **no redistribute {connected | static | ospf | bgp | rip} [level-1 | level-1-2 | level-2]** 命令取消指定类型路由的引入。

发布缺省路由

对于引入其他协议的路由信息时所存在的缺省路由，不会被路由器引入并使用。如果需要在路由域中发布缺省路由，在 IS-IS 路由配置模式下使用以下命令：

default-information originate

当配置了此命令的路由器的路由表中存在一条缺省路由，IS-IS 将只通过 Level-2 LSP 通告此路由。

使用 **no default-information originate** 命令取消发布缺省路由。

IS-IS 网络优化

配置 Hello 报文发送时间间隔

配置接口发送 Hello 报文的时间间隔，在接口配置模式下，使用如下命令：

isis hello-interval *value* **[level-1 | level-2]**

- *value* – 接口发送 Hello 报文的时间间隔。取值范围为 1 到 600。单位为秒。默认值为 3 秒。
- **level-1 | level-2** – 使用 **level-1** 参数指定 Level-1 Hello 报文的发送时间间隔。使用 **level-2** 参数指定 Level-2 Hello 报文的发送时间间隔。默认为 Level-2 和 Level-1Hello 报文。

使用 **no isis hello-interval** 命令将 Hello 报文发送时间间隔恢复为默认值。

配置 Hello 报文失效乘数

在指定抑制时间内，如果路由器没有收到来自邻居的 Hello 报文，将宣告邻居失效。抑制时间等于 Hello 报文失效乘数与 Hello 报文发送时间间隔的乘积，。配置 Hello 报文失效乘数，在接口

配置模式下，使用如下命令：

isis hello-multiplier *value* **[level-1 | level-2]**

- *value* – 指定 Hello 报文失效乘数。取值范围为 2 到 100。默认值为 10。
- **level-1 | level-2** – 使用 **level-1** 参数指定 Level-1 Hello 报文的失效乘数。使用 **level-2** 参数指定 Level-2 Hello 报文的失效乘数。默认为 Level-1 和 Level-2 Hello 报文。

使用 **no isis hello-multiplier** 命令恢复报文失效乘数的默认值。

配置 Hello 报文填充功能

使用 Hello 报文填充功能将 Hello 报文填充到接口 MTU 大小。配置 Hello 报文填充功能，在接口配置模式下，使用如下命令：

isis hello padding

使用 **no isis hello padding** 命令取消 Hello 报文填充功能。

配置 DIS 选举优先级

在广播类型网络中，通过指定接口的 DIS(Designated IS)优先级，影响 DIS 选举结果。在 DIS 选举中，接口的 DIS 优先级高的 IS 被选举为 DIS。当 DIS 优先级相同时，则 MAC 地址最大的接口所属的 IS 被选举为 DIS。配置接口的 DIS 选举优先级，在接口配置模式下，使用如下命令：

isis priority *value* **[level-1 | level-2]**

- *value* – 指定 DIS 选举优先级。取值范围为 0 到 127。默认值为 64。
- **level-1 | level-2** – 使用 **level-1** 参数指定 Level-1 接口的 DIS 选举优先级。使用 **level-2** 参数指定 Level-2 接口的 DIS 选举优先级。默认为 Level-1 和 Level-2 接口设置相同的 DIS 选举优先级。

使用 **no isis priority [level-1 | level-2]**命令恢复指定级别接口的 DIS 选举优先级。

配置被动接口

如果把接口配置为被动接口，则此被动接口不向外发送和接受 IS-IS 报文，并且此接口不与相邻路由器建立邻居关系。但仍然可以把该接口直连网络的路由信息放在 LSP 中从其他接口宣告出去。配置被动接口，在接口配置模式下，使用如下命令：

isis passive

使用 **no isis passive** 命令取消被动接口设置。

配置 LSP 生成时间间隔

为了防止网络拓扑频繁变化而导致 LSP 频繁重新生成，用户可配置 LSP 生成时间间隔，以抑制网络变化频繁导致占用过多的带宽资源和路由器资源。配置 LSP 生成时间间隔，在 IS-IS 路由配置模式下，使用如下命令：

lsp-gen-interval *value* **[level-1 | level-2]**

- *value* – 指定 LSP 生成时间间隔。取值范围为 1 到 120。默认值为 30。单位为秒。
- **level-1 | level-2** – 选择 **level-1** 仅为 Level-1 LSPs 指定生成时间间隔；选择 **level-2** 仅为 level-2 LSPs 指定生成时间间隔。不指定参数时，配置的生成时间间隔适用于 Level-1 LSP 和 Level-2 LSP。

使用 **no lsp-gen-interval** 命令恢复默认值。

配置 LSP 最大生存时间

为 LSP 配置最大生存时间。当 LSP 的最大生存时间递减为 0 时，IS-IS 协议将在 LSDB 中把此 LSP 继续保持 60 秒。若还未收到此 LSP 的更新，则删除此 LSP。配置 LSP 最大生存时间，在 IS-IS 路由配置模式下，使用如下命令：

max-lsp-lifetime *value*

- *value* – 指定 LSP 的最大生存时间。取值范围为 350 到 65535。默认值为 1200。单位为秒。

使用 **no max-lsp-lifetime** 命令恢复默认值。

配置 LSP 刷新时间

每一个 LSP 都有一个最大生存时间，因此每个路由器必须定时刷新自己生成的 LSP，以防止 LSP 的最大生存时间减小至 0。用户可对 LSP 的刷新周期进行配置。配置 LSP 刷新时间，在 IS-IS 路由配置模式下，使用如下命令：

lsp-refresh-interval *value*

- *value* – 指定 LSP 的刷新时间。取值范围为 1 到 65535。默认值为 900。单位为秒。需要确保刷新时间比 LSP 最大生存时间少 300 秒以上，使刷新后的 LSP 可以在原 LSP 过期前到达区域内的设备。

使用 **no lsp-refresh-interval** 命令恢复默认值。

配置 SPF 计算时间间隔

当 LSDB 发生变化时需要进行路由计算。计算 SPF 的时间间隔可以由用户根据需要进行配置。配置 SPF 计算时间间隔，在 IS-IS 路由配置模式下，使用如下命令：

spf-interval *value* **[level-1 | level-2]**

- *value* – 指定计算 SPF 的时间间隔。取值范围为 1 到 120。默认值为 10。单位为秒。
- **level-1 | level-2** – 选择 **level-1** 仅为 Level-1 SPF 指定计算时间间隔；选择 **level-2** 仅为 level-2 SPF 指定计算时间间隔。不指定参数时，配置的计算时间间隔适用于 Level-1 SPF 和 Level-2 SPF 的计算。

使用 **no spf-interval** 命令恢复默认值。

配置过载标志位

当路由器因资源不足而导致 LSDB 不完整或不准确时，会在通告的 LSPs 中设置过载标志位。其它路由器在收到此类型 LSPs 后，就不会再利用这台路由器转发需要经过它传送的数据，但到此路由器直连地址的报文仍然可以被转发给此路由器。为路由器手工配制过载标志位，在 IS-IS 路由配置模式下，使用如下命令：

set-overload-bit

使用 **no set-overload-bit** 命令取消配置过载标志位。

配置主机名映射

在 IS-IS 路由域中，System ID 作为 NET 地址的一部分，用来在区域内唯一标识主机或路由器。主机名映射可以将 System ID 映射到主机名。IS-IS 的路由器维护一个主机名到 System ID 的映射关系表。配置主机名映射，在 IS-IS 路由配置模式下，使用如下命令：

hostname dynamic

使用 **no hostname dynamic** 取消主机名映射配置。

IS-IS 网络安全性

配置认证

对路由器之间所发送的 LSP 报文，CSNP 报文，PSNP 报文进行认证配置。认证配置只影响路由信息的学习，不影响邻居的建立。认证证方式有两种，分别是明文认证和 MD5 密文认证。明文认证不能提供安全保障。未加密的认证字随报文一同传送。默认为明文认证。配置验证方式，在 IS-IS 路由配置模式下，使用如下命令：**authentication {md5 | text} [level-1 | level-2]**

- **md5 | text** – 使用 MD5 认证方式（**md5**）或明文认证（text）。
- **level-1 | level-2** – 使用 **level-1** 参数为 Level-1 路由器之间的报文指定认证方式。使用 **level-2** 参数为 Level-2 路由器之间的报文指定认证方式。通过配置 Level-1 路由器之间的认证，可以防止将从不可信任的路由器学习到的路由信息加入到 Level-1 的 LSDB

中。同一区域内的 Level-1 路由器必须配置相同的认证方式和认证密码。通过配置 Level-2 路由器间的认证，可以防止将不可信的路由信息注入 Level-2 路由器。同一路由域中所有 Level-2 路由器必须配置相同的认证方式和认证密码。

取消认证配置，在 IS-IS 路由配置模式下，使用 **no authentication mode**。

指定认证方式后，需要继续指定认证所使用的秘钥。为 Level-1 路由器之间报文的认证方式指定秘钥，使用如下命令：

area-password *word*

- *word* – 指定认证所使用的秘钥。秘钥的最大长度为 32 字符。

删除指定的密钥，使用 **no area-password** 命令。

为 Level-2 路由器之间报文的认证方式指定秘钥，使用如下命令：

domain-password *word*

- *word* – 指定认证所使用的秘钥。秘钥的最大长度为 32 字符。

删除指定的密钥，使用 **no domain-password** 命令。

配置接口认证模式

接口认证用来确认邻居的合法性，防止与无法信任的路由器形成邻居。配置接口认证后，认证密码将会封装到 Hello 报文中。通过检查才会形成邻居关系，否则将不会形成邻居关系。两台路由器要形成邻居关系必须配置相同的认证模式和认证密码。配置接口认证模式，在接口配置模式下，使用如下命令：

isis authentication {md5 | text} [level-1 | level-2]

- **md5 | text** – 使用 MD5 认证方式（**md5**）或明文认证（text）。
- **level-1 | level-2** – 使用 **level-1** 参数为 Level-1 路由器之间的 Hello 报文指定认证方式。使用 **level-2** 参数为 Level-2 路由器之间的 Hello 报文指定认证方式。

使用 **no isis authentication** 命令取消接口认证。

配置接口认证模式后，需要继续指定认证所使用的秘钥。在接口配置模式下，使用如下命令：

isis password *word* **[level-1 | level-2]**

- *word* – 指定认证所使用的秘钥。秘钥的最大长度为 32 字符。
- **level-1 | level-2** – 使用 **level-1** 参数为 Level-1 路由器之间的 Hello 报文认证指定密码。使用 **level-2** 参数为 Level-2 路由器之间的 Hello 报文认证指定密码。

使用 **no isis password** 命令取消指定的密钥。

查看 IS-IS 信息

显示 IS-IS 进程信息及相关配置，在任何模式下使用以下命令：

show isis [vrouter *vrouter-name*]

- *vrouter-name* – 显示指定的 VRouter 的 IS-IS 进程信息及相关配置。

显示 IS-IS 链路状态数据库，任何模式下使用以下命令：

show isis database [detail] [vrouter *vrouter-name***]**

- **detail** – 显示链路状态数据库的详细信息。
- *vrouter-name* – 显示指定的 VRouter 的链路状态数据库信息。

显示 IS-IS 接口信息，在任何模式下使用以下命令：

show isis interface [*interface-name***]**

显示 IS-IS 邻居信息，在任何模式下使用以下命令：

show isis neighbor [detail] [vrouter *vrouter-name***]**

显示动态主机名配置，在任何模式下使用以下命令：

show isis hostname [vrouter *vrouter-name***]**

显示 IS-IS 路由信息，在任何模式下使用以下命令：

show isis route [*A.B.C.D/M***] [vrouter** *vrouter-name***]**

显示路由引入信息，在任何模式下使用以下命令：

show isis route redistribute [level-1 | level-2] [*A.B.C.D/M***] [vrouter** *vrouter-name***]**

配置 BGP

BGP 是边界网关协议（Border Gateway Protocol）的缩写。它是在自治系统（“自治系统”是处于一个管理机构控制之下的路由器和网络群组。一个自治系统中的所有路由器必须运行相同的路由协议）之间动态交换路由信息的路由协议，也是 ISP 之间使用的协议。BGP 使用 TCP 传输协议，端口号为 179，并且支持无类别域间选路（CIDR）。BGP 有两种运行方式：当 BGP 运行在自治系统之间时，为 EBGP，而当 BGP 运行在自治系统之内时，为 IBGP。BGP 具有以下特点：

- 首次建立 TCP 连接后，BGP 邻居之间交换整个 BGP 路由表，之后仅交换更新路由信息。
- 周期性发送 KEEPALIVE 报文校验 TCP 的连通性。
- BGP 路由器仅选择最优路径发布到 BGP 邻居。
- BGP 是一种距离矢量的路由协议，从设计上避免了环路的发生。

发送 BGP 消息的路由器称为 BGP 发言人，它接收或产生新的路由信息，并发布给其它 BGP 发言人。当 BGP 发言人收到来自其它自治系统的新路由时，如果该路由比当前已知路由更优、或

者当前还没有该路由，它就把这条路由发布给所有其它 BGP 发言人。相互交换消息的 BGP 发言人之间互称对等体（peer），多个相关的对等体可以构成对等体组（peer group）。对等体组的作用是简化配置，不影响实际的对等体关系的建立与路由的传递。

BGP 有 4 种类型的报文，分别为 OPEN、UPDATE、NOTIFICATION 和 KEEPALIVE。BGP 对等体间通过发送 OPEN 报文来交换各自的版本、自治系统号、保持时间、BGP 标识符等信息，进行协商。OPEN 报文主要用于建立邻居（BGP 对等体）关系，它是 BGP 路由器之间的初始握手消息，应该发生在任何通告消息之前。对等体在收到 OPEN 消息之后，即以 KEEPALIVE 消息作为响应。一旦握手成功，则这些 BGP 邻居就可以进行 UPDATE（更新）、KEEPALIVE（保持激活）以及 NOTIFICATION（通知）等消息的交换操作。UPDATE 报文携带的是路由更新信息，其中包括撤销路由信息和可达路由信息及其路径属性。当 BGP 检测到差错（连接中断、协商出错、报文差错等）时，发送 NOTIFICATION 报文，关闭同对等体的连接。KEEPALIVE 报文在 BGP 对等体间周期性发送，以确保连接有效。

BGP 协议配置

用户可以为不同的 VRouter 分别配置 BGP 协议。BGP 协议配置包括以下各项：

- 进入 BGP 配置模式
- 指定 Router ID
- 创建聚合路由
- 添加静态 BGP 路由
- 配置定时器
- 指定 BGP 路由管理距离
- 指定缺省度量
- 创建 BGP 对等体组
- 添加 BGP 对等体到对等体组
- 配置 BGP 对等体
- 配置 BGP MD5 认证
- 激活 BGP 连接
- 配置缺省信息发布
- 配置描述信息
- 配置 BGP 对等体定时器

- 配置下一跳为自身
- 配置 EBGP 多跳
- 关闭对等体或者对等体组
- 重置 BGP 连接
- 配置 AS 路径访问控制列表
- 配置团体属性列表
- 引入路由
- 配置路由映射表
- 修改引入路由属性
- 配置基于 AS 路径访问控制列表的路由过滤
- 配置向对等体或者对等体组发送团体属性
- 配置基于路由映射表的路由过滤
- 等价负载均衡

进入 BGP 配置模式

对 BGP 协议的配置需要在 BGP 路由模式下进行。进入 BGP 路由模式，在 VRouter 配置模式下，使用以下命令：

ip vrouter *vrouter-name* （从全局模式进入 VRouter 配置模式）
router bgp *number*

- *number* – 指定自治系统的编号。范围是 1 到 4294967295。

运行该命令后，系统的 BGP 路由功能被开启，为指定的自治系统创建 BGP 实例，并且进入 BGP 实例配置模式。

在 VRouter 配置模式下，使用 **no router bgp** *number* 删除 BGP 实例。

指定 Router ID

每一台运行 BGP 协议的路由器都必须拥有一个 Router ID。Router ID 是每个路由器在整个 BGP 域中的唯一标识，使用 IP 地址的形式表示。如果不指定 Router ID，系统会将设备上回环接口的最大 IP 地址设置为 Router ID，如果没有回环接口或者回环接口未配置 IP 地址，则选择其他接口的最大 IP 作为 Router ID。指定 Router ID，在 BGP 实例配置模式下，使用以下命令：

router-id *A.B.C.D*

- *A.B.C.D* – 指定 BGP 协议使用的 Router ID，为 IP 地址形式。

在 BGP 实例配置模式下，使用该命令 no 的形式取消 Router ID 的指定：

no router-id

创建聚合路由

用户可以将 BGP 路由表内的路由条目进行聚合。创建聚合路由，在 BGP 实例配置模式下，使用以下命令：

aggregate-address {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} [**as-set**] [**summary-only**]

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定聚合网络地址。Hillstone 设备支持两种方式，*A.B.C.D/M*或者 *A.B.C.D A.B.C.D*,例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- **as-set** – 如果指定该参数，系统会将被聚合路由的路径信息作为自己的路径信息发布给其它路由器。
- **summary-only** – 如果指定该参数，系统将只发布聚合路由。

在 BGP 实例配置模式下，使用该命令 no 的形式取消聚合路由的指定：

no aggregate-address {*A.B.C.D/M* | *A.B.C.D A.B.C.D*}

添加静态 BGP 路由

向 BGP 路由表中添加静态 BGP 路由条目，在 BGP 实例配置模式下，使用以下命令：

network {*A.B.C.D/M* | *A.B.C.D A.B.C.D*}

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定 BGP 静态路由条目信息。Hillstone 设备支持两种方式，*A.B.C.D/M* 或者 *A.B.C.D A.B.C.D*，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。

在 BGP 实例配置模式下使用该命令 no 的形式删除指定的静态路由条目：

no network {*A.B.C.D/M* | *A.B.C.D A.B.C.D*}

配置定时器

用户可以配置两个 BGP 定时器，分别是 KEEPALIVE（保持激活）和 HOLDDOWN（保持时间），描述如下：

- KEEPALIVE（保持激活）：StoneOS 向 BGP 对等体发送保持激活信息的频率。默认为每隔 60 秒发送一次。
- HOLDDOWN（保持时间）：如果本地路由器在保持时间结束后仍没有收到某对等体的保持激活信息，则判断为该对等体老化。默认为 180 秒。

配置定时器，在 BGP 实例配置模式下，使用以下命令：

timers *keepalive holddown*

- *keepalive* – 指定发送保持激活信息的频率，单位为秒。默认是 60 秒。取值范围是 0 到 65535，且小于或者等于 HOLDDOWN/3 的值，如果大于 HOLDDOWN/3，实际生效的

时间将为 HOLDDOWN/3。参数值为 0 表示不发送 KEEPALIVE 信息。

- *holddown* – 指定保持时间，单位为秒。默认是 180 秒。取值范围是 0 或者 3 到 65535。参数值为 0 表示不检查保持时间。

在 BGP 实例配置模式下使用该命令 no 的形式恢复定时器的默认值：

no timers

指定 BGP 路由管理距离

用户可以为从其它对等体获得的 BGP 路由以及本地 BGP 路由指定管理距离。指定 BGP 路由管理距离，在 BGP 实例配置模式下，使用以下命令：

distance *ebgp-distance ibgp-distance local-distance*

- *ebgp-distance* – 指定 EBGP 路由管理距离。默认值为 20。取值范围是 1 到 255 的整数。
- *ibgp-distance* – 指定 IBGP 路由管理距离。默认值为 200。取值范围是 1 到 255 的整数。
- *local-distance* – 指定本地路由管理距离。默认值为 200。取值范围是 1 到 255 的整数。

在 BGP 实例配置模式下使用该命令 no 的形式恢复默认 BGP 路由管理距离：

no distance

指定缺省度量

默认情况下，引入的 IGP 路由的度量保持不变，引入的直连路由的度量为 0。用户可以为引入路由指定缺省度量。指定引入路由的缺省度量，在 BGP 实例配置模式下，使用以下命令：

default-metric *value*

- *value* – 指定缺省度量值。范围是 1 到 4294967295。

在 BGP 实例配置模式下使用该命令 no 的形式恢复默认情况：

no default-metric

创建 BGP 对等体组

使用 BGP 对等体组，可以简化配置，也可以使信息更新更为有效。创建 BGP 对等体组，在 BGP 实例配置模式下，使用以下命令：

neighbor *peer-group-name* **peer-group**

- *peer-group-name* – 指定将要创建的对等体组的名称。

在 BGP 实例配置模式下使用该命令 no 的形式删除已创建的 BGP 对等体组：

no neighbor *peer-group-name* **peer-group**

添加 BGP 对等体到对等体组

添加 BGP 对等体到对等体组，在 BGP 实例配置模式下，使用以下命令：

neighbor *A.B.C.D* **peer-group** *peer-group-name*

- *A.B.C.D* – 指定将要添加的 BGP 对等体的 IP 地址。
- *peer-group-name* – 指定系统中已创建的对等体组的名称。

在 BGP 实例配置模式下使用该命令 no 的形式将 BGP 对等体从对等体组中删除：

no neighbor *A.B.C.D* **peer-group** *peer-group-name*

配置 BGP 对等体

用户需要为当前设备指定 BGP 对等体 (对等体组)，交换 BGP 路由信息。配置 BGP 对等体 (对等体组)，在 BGP 实例配置模式下，使用以下命令：

neighbor {*A.B.C.D* | *peer-group*} **remote-as** *number*

- *A.B.C.D* | *peer-group* – 指定对等体 IP 地址或者对等体组的名称。
- *number* – 指定所配置对等体或者对等体组所在的自治区域的编号。

在 BGP 实例配置模式下使用该命令 no 的形式取消 BGP 对等体或者对等体组的指定：

no neighbor {*A.B.C.D* | *peer-group*} **remote-as**

配置 BGP MD5 认证

为提高 BGP 的安全性，用户可以配置 BGP 对等体或者对等体组在建立 TCP 连接时进行 MD5 认证，认证通过后才可以建立 TCP 连接。配置 BGP MD5 认证，在 BGP 实例配置模式下，使用以下命令：

neighbor {*A.B.C.D* | *peer-group*} **password** *password*

- *A.B.C.D* | *peer-group* – 指定对等体 IP 地址或者对等体组的名称。
- **password** *password* – 指定 MD5 密码串，范围是 1 到 32 个字符。

在 BGP 实例配置模式下使用该命令 no 的形式取消 BGP MD5 认证的配置：

no neighbor {*A.B.C.D* | *peer-group*} **password**

注意：参与 MD5 认证的对等体或者对等体组的密码必须一样。

激活 BGP 连接

默认情况下，已配置的 BGP 对等体或者对等体组与当前设备的 BGP 连接是激活的。用户可以关闭连接也可以重新激活 BGP 连接。激活 BGP 连接，在 BGP 实例配置模式下，使用以下命令：

neighbor {*A.B.C.D* | *peer-group*} **activate**

- *A.B.C.D* | *peer-group* – 指定对等体 IP 地址或者对等体组的名称。

在 BGP 实例配置模式下使用该命令 no 的形式关闭指定对等体或者对等体组的 BGP 连接：

no neighbor {*A.B.C.D* | *peer-group*} **activate**

配置缺省信息发布

用户可以指定当前设备是否将默认路由发布到其它 BGP 对等体或者对等体组。默认情况下，不发送默认路由。

配置缺省信息发布到 BGP 对等体或者对等体组，在 BGP 实例配置模式下，使用以下命令：

default-information originate

如果路由表中没有默认路由，系统将不会发布默认路由。

在 BGP 实例配置模式下，使用该命令 no 的形式取消缺省信息发布：

no default-information originate

配置缺省信息发布到 BGP 对等体或者对等体组，在 BGP 实例配置模式下，使用以下命令：

neighbor {*A.B.C.D* | *peer-group*} **default-originate**

- *A.B.C.D* | *peer-group* – 指定对等体 IP 地址或者对等体组的名称。

如果路由表中没有默认路由，系统将会构造一条默认路由发布到 BGP 对等体或者对等体组。

在 BGP 实例配置模式下使用该命令 no 的形式取消缺省信息发布：

no neighbor {*A.B.C.D* | *peer-group*} **default-originate**

配置描述信息

为对等体或者对等体组配置描述信息，在 BGP 实例配置模式下，使用以下命令：

neighbor {*A.B.C.D* | *peer-group*} **description** *description*

- *A.B.C.D* | *peer-group* – 指定对等体 IP 地址或者对等体组的名称。
- *description* – 指定描述信息。范围是 1 到 80 个字符。

在 BGP 实例配置模式下使用该命令 no 的形式取消对等体或者对等体组的描述信息：

no neighbor {*A.B.C.D* | *peer-group*} **description**

配置 BGP 对等体定时器

默认情况下，在整个 BGP 系统中，BGP 对等体或对等体组之间的定时器按照 **timer** *keepalive holddown* 设置的值生效，用户可以为某个特定的 BGP 对等体或者对等体组指定不同的定时器数值，该数值优先级高于 **timer** *keepalive holddown* 设置的值。为 BGP 对等体或者对等体组指定定时器数值，在 BGP 实例配置模式下，使用以下命令：

neighbor {*A.B.C.D* | *peer-group*} **timers** *keepalive holddown*

- *A.B.C.D* | *peer-group* – 指定对等体 IP 地址或者对等体组的名称。
- *keepalive* – 指定发送保持激活信息的频率，单位为秒。默认是 60 秒。取值范围是 0 到 65535，且小于或者等于 HOLDDOWN/3 的值，如果大于 HOLDDOWN/3，实际生效的时间将为 HOLDDOWN/3。参数值为 0 表示不发送 KEEPALIVE 信息。
- *holddown* – 指定保持时间，单位为秒。默认是 180 秒。取值范围是 0 或者 3 到 65535。

参数值为 0 表示不检查保持时间。

在 BGP 实例配置模式下使用该命令 no 的形式取消对 BGP 对等体或对等体组定时器的指定：

no neighbor {*A.B.C.D* | *peer-group*} **timers**

配置下一跳为自身

配置该功能后，路由器将通告对等体或者对等体组 BGP 路由的下一跳为该路由器自身。配置下一跳路由为自身，在 BGP 实例配置模式下，使用以下命令：

neighbor {*A.B.C.D* | *peer-group*} **next-hop-self**

- *A.B.C.D* | *peer-group* - 指定对等体 IP 地址或者对等体组的名称。

在 BGP 实例配置模式下使用该命令 no 的形式取消下一跳为自身的指定：

no neighbor {*A.B.C.D* | *peer-group*} **next-hop-self**

配置 EBGP 多跳

对于运行在自治系统之间的 BGP（即 EBGP），如果 BGP 对等体或对等体组没有直接连接，用户需要配置 EBGP 多跳才能在设备之间创建邻居关系。配置 EBGP 多跳，在 BGP 实例配置模式下，使用以下命令：

neighbor {*A.B.C.D* | *peer-group*} **ebgp-multihop** [*ttl*]

- *A.B.C.D* | *peer-group* - 指定对等体 IP 地址或者对等体组的名称。
- *ttl* - 指定到对等体 IP 地址或者对等体组的最大下一跳数。取值范围是 1 到 255，默认值是 255。如果在达到最大下一跳数后仍无法找到指定的对等体或对等体组，系统会认为创建邻居关系失败。

在 BGP 实例配置模式下使用该命令 no 的形式取消 EBGP 多跳：**no neighbor** {*A.B.C.D* | *peer-group*} **ebgp-multihop**

关闭对等体或者对等体组

用户可以关闭指定的对等体或者对等体组。关闭对等体或者对等体组后，所有与被关闭对等体或者对等体组相关的会话都会被中断，所有相关的路由信息也会被删除。关闭对等体或者对等体组，在 BGP 实例配置模式下，使用以下命令：

neighbor {*A.B.C.D* | *peer-group*} **shutdown**

- *A.B.C.D* | *peer-group* – 指定对等体 IP 地址或者对等体组的名称。

在 BGP 实例配置模式下使用该命令 no 的形式开启对等体或者对等体组：

no neighbor {*A.B.C.D* | *peer-group*} **shutdown**

重置 BGP 连接

重置 BGP 连接，在执行模式下，使用以下命令：

clear ip bgp {***** | *A.B.C.D* | **external** | **peer-group** *peer-group-name* | *number*} [**vrouter** *vrouter-name*]

- ***** - 重置当前所有 BGP 会话连接。
- *A.B.C.D* – 重置指定对等体的 BGP 连接。
- **external** – 重置所有 EBGP 连接。
- **peer-group** *peer-group-name* – 重置指定 BGP 对等体组的连接。
- *number* – 重置指定自治系统中的 BGP 连接。
- **vrouter** *vrouter-name* – 指定需重置连接所在的 VRouter。

配置 AS 路径访问控制列表

AS 路径是路由在到达目的网络之前所经过的 AS 号码序列。在到达目的网络之前，BGP 路由每经过一个 AS，在出 AS 时就会将 AS 号码添加到 AS 路径中。

用户可以通过 AS 路径访问控制列表实现路由过滤。AS 路径访问控制列表主要由正则表达式和匹配成功后所执行操作（允许或拒绝）两部分组成。如果正则表达式匹配路由的 AS 路径，系统会继续执行指定的操作；如果匹配失败，系统会执行拒绝操作。系统最多允许配置 64 个 AS 路径访问控制列表，每个 AS 路径访问控制列表最多允许配置 8 条正则表达式。

配置 AS 路径访问控制列表，在全局配置模式下使用以下命令：

ip as-path access-list *access-list-number* {**deny** | **permit**} regular-expression

- *access-list-number* – 指定 AS 路径访问控制列表号。范围为 1 到 500。
- **deny** | **permit** – 指定对匹配的路由所执行的操作。**deny** 为拒绝，**permit** 为允许。
- regular-expression – 指定用于匹配 AS 路径的正则表达式。StoneOS 支持 PCRE（Perl Compatible Regular Expressions）正则表达式语法。

在全局配置模式下使用该命令 no 的形式删除 AS 路径访问控制列表：

no ip as-path access-list *access-list-number* [{**deny** | **permit**} regular-expression]

例如，配置序号为 1 的 AS 路径控制列表，拒绝经过 AS 31 的路由，但允许其他路由，请输入以下命令：

```
hostname(config)# ip as-path access-list 1 deny _31_
hostname(config)# ip as-path access-list 1 permit .*
hostname(config)#
```

配置团体属性列表

在 BGP 中，团体属性标识一组具有相同特征的路由信息，与其所在的 IP 子网和 AS 无关。除用户自定义的团体属性外，系统支持如下的公认团体属性：

- No-export：带有这一团体属性值的路由不能通告给 AS 之外的对等体。
- No-adverties：带有这一团体属性值的路由不能通告给任何 BGP 对等体。
- Local-as：带有这一团体属性值的路由可以通告给本地 AS 内的其他对等体，不能通告到本地 AS 以外的对等体。
- Internet：带有这一团体属性值的路由可以通告给任何 BGP 邻居。默认情况下所有路由都携带该属性。

团体属性列表主要由团体属性和匹配成功后所执行操作（允许或拒绝）两部分组成。如果引入路由的团体属性匹配指定的团体属性，系统会继续执行指定的操作；如果匹配失败，系统会执行拒绝操作。系统最多允许配置 128 个团体属性列表，每个团体属性列表最多允许配置一条 Permit 规则和一条 Deny 规则。

配置团体属性列表，在全局配置模式下使用以下命令：

ip community-list {**standard** *community-list-name* | *community-list-number*} {**deny** | **permit**} {[**internet**] [**local-as**] [**no-advertise**] [**no-export**] [*community-number*]}

- **standard** *community-list-name* – 指定团体属性列表名称。为 1 到 31 个字符的字符串。
- *community-list-number* – 指定团体属性列表号。范围为 1 到 99。
- **deny** | **permit** – 指定对匹配的路由所执行的操作。**deny** 为拒绝，**permit** 为允许。
- [**internet**] [**local-as**] [**no-advertise**] [**no-export**] [*community-number*] – 指定团体属性，可以同时指定多个团体属性，不同团体属性间用空格隔开。*community-number* 为 1 到 4294967295 之间的数字。

在全局配置模式下使用该命令 no 的形式删除团体属性列表：

no ip community-list {**standard** *community-list-name* | *community-list-number*}

引入路由

BGP 协议允许用户引入其它路由协议（OSPF、直连、静态和 RIP）的路由信息，并向外发布。同时，用户可以设置被引入路由的度量，还可以引用路由映射表对路由信息进行过滤，仅允许引入或拒绝引入特定的路由信息。配置引入路由，在 BGP 实例配置模式下使用以下命令：

redistribute {**ospf** | **connected** | **static** | **rip**} [**metric** *value*] [**route-map** *name*]

- **ospf** | **connected** | **static** | **rip** – 指定引入路由的类型，可以是 OSPF（**ospf**）、直连路由（**connected**）、静态路由（**static**）或者 RIP（**rip**）。
- **metric** *value* – 指定引入路由的度量。范围是 0 到 4294967295。如果不指定该数值，系统会使用 BGP 的缺省度量（通过 **default-metric** *value* 配置）。
- **route-map** *name* – 指定用于过滤引入路由信息的路由映射表。有关路由映射表的更多信息，请参考“配置路由映射表”。

用户可以配置多条该命令引入不同类型的路由。

使用 **no redistribute** {**ospf** | **connected** | **static** | **rip**}命令取消指定类型路由的引入。

配置路由映射表

默认情况下系统会引入所有的路由信息。用户可以引用路由映射表对引入的路由信息进行过滤。路由映射表主要由路由匹配规则和匹配成功后所执行操作（允许或拒绝）两部分组成。如果引入的路由信息命中了任何路由匹配规则，系统就会执行对应的操作，允许或拒绝引入这些路由信息。

注意：

- 如果用户设置的操作是允许，匹配成功后系统仅允许引入匹配的路由信息，拒绝引入所有未匹配的路由信息。
- 如果用户设置的操作是拒绝，匹配成功后系统会拒绝引入匹配的路由信息，但仍允许引入未匹配的路由信息。

用户可通过以下步骤配置路由映射表，实现对引入路由信息的过滤：

1.创建路由映射表并在表中创建路由匹配规则。不同的匹配规则通过序列号区分。序列号越小，

匹配优先级越高。默认情况下，引入的路由信息命中任何路由匹配规则，系统将不再继续匹配后续的规则；如果引入的路由信息没有命中任何匹配规则，系统将执行拒绝操作。

2.在路由匹配规则中配置匹配条件。匹配条件可以是引入路由的 AS 路径、团体属性、度量值、目的地址或下一跳地址。一条路由匹配规则中可以包含多个匹配条件，这些匹配条件之间是与(AND)关系，即引入的路由信息必须满足匹配规则中的所有匹配条件才会认定为命中了该条规则。

3.如有需要，可以设置系统在命中一条路由匹配规则后继续匹配其他规则。有关匹配多条路由匹配规则配置的更多信息，请参考“匹配多条路由匹配规则”。

4.如有需要，修改引入路由的部分属性后再对外发布。

创建路由映射表并在表中配置路由匹配规则，在全局配置模式下，使用以下命令：

route-map *name* {**deny** | **permit**} *sequence*

- **route-map** *name* – 指定路由映射表名称，并进入路由映射表配置模式。取值范围是 1 到 31 个字符。如果该名称已经存在，则直接进入路由映射表配置模式。
- **deny** | **permit** – 指定对匹配的路由信息所执行的操作。**deny** 为拒绝，**permit** 为允许。
- *sequence* – 指定该路由映射表下路由匹配规则的序列号。取值范围是 1 到 65535。

使用该命令 no 的形式删除路由映射表：

no route-map *name* [*sequence*]

- *sequence* – 仅删除路由映射表中指定的匹配规则。

配置路由匹配规则中的匹配条件，在路由映射表配置模式下，使用以下命令：

match {**as-path** *access-list-number* | **community** {*community-list-name* | *community-list-number*} [exact-match] | **metric** *metric-value* | **ip address** *access-list* | **ip next-hop** *access-list*}

- **as-path** *access-list-number* – 匹配路由的 AS 路径。*access-list-number* 为用户配置的 AS 路径访问控制列表号。如果路由的 AS 路径匹配该访问控制列表中允许的 AS 路径，则认为匹配成功。有关 AS 路径访问控制列表配置的更多信息，请参考“配置

AS 路径访问控制列表 "。

- **community** {*community-list-name* | *community-list-number*} [exact-match] – 匹配路由的团体属性。*community-list-name* 为团体属性列表名称；*community-list-number* 为团体属性列表号；exact-match 指定对团体属性进行精确匹配。有关团体属性列表列表配置的更多信息，请参考 "配置团体属性列表 "。
- **metric** *metric-value* – 匹配路由的度量值。取值范围是 0 到 4294967295。
- **ip address** *access-list* – 匹配路由的目的地址。*access-list* 为用户配置的路由访问控制列表。如果路由的目的地址属于该访问控制列表中允许的地址，则认为匹配成功。有关访问控制列表配置的更多信息，请参考 "配置路由访问控制列表 "。
- **ip next-hop** *access-list* – 匹配路由的下一跳地址。*access-list* 为用户配置的路由访问控制列表。如果路由的下一跳地址属于该访问控制列表中允许的地址，则认为匹配成功。有关访问控制列表配置的更多信息，请参考 "配置路由访问控制列表 "。

重复以上命令向路由匹配规则中添加多个不同类型的匹配条件。使用该命令 no 的形式删除匹配条件：

no match {**as-path** | **community** | **metric** | **ip address** | **ip next-hop**}

注意：如果用户仅创建了路由映射表但没有在映射表中配置任何路由匹配规则，系统默认会认为引入的路由信息匹配成功。

修改引入路由属性

对于满足匹配条件的引入路由，用户可以在修改路由的部分属性后再对外发布。修改引入路由的属性，在路由映射表配置模式下，使用以下命令：

set {**as-path prepend** *as-number* | **commu-list** {*community-list-name* | *community-list-number*} **delete** | **community** {[**internet**] [**local-AS**] [**no-advertise**] [**no-export**] [*community-list-number*]} [**additive**] | **ip next-hop** *ip-address* | **local-preference** *value* | **metric** *metric-value* | **origin** {**egp** | **igp** | **incomplete**}}

- **as-path prepend** *as-number* – 在引入路由的 AS 路径后添加新的 AS 路径。取值范围为 1 到 65535 之间的数字，多个数字之间用空格隔开。

- **commu-list** {*community-list-name* | *community-list-number*} **delete** – 指定团体属性列表名称（*community-list-name*）或者团体属性列表号（*community-list-number*），删除匹配的团体属性。
- **community** {[**internet**] [**local-AS**] [**no-advertise**] [**no-export**] [*community-list-number*]} [**additive**] – 修改引入路由的团体属性。**additive** 为在引入路由的团体属性中添加新的团体属性。
- **ip next-hop** *ip-address* – 修改引入路由的下一跳地址。
- **local-preference** *value* – 修改引入路由的本地优先属性。取值范围是 0 到 4294967295。
- **metric** *metric-value* – 修改引入路由的度量值。取值范围是 0 到 4294967295。
- **origin** {**igp** | **egp** | **incomplete**} – 修改引入路由的来源属性。**igp** 为路由起始于 AS 内部；**egp** 为路由通过 EGP 获得；**incomplete** 为路由通过其他方法获得。

使用该命令 no 的形式取消对路由属性的修改并还原到引入路由时的设置：

no set {**as-path prepend** | **commu-list** | **community** | **ip next-hop** | **local-preference** | **origin** | **metric** | **metric-type**}

配置基于 AS 路径访问控制列表的路由过滤

BGP 协议支持通过 AS 路径访问控制列表对对等体（对等体组）引入的路由或者向外发布的路由进行过滤。配置基于 AS 路径访问控制列表的路由过滤，在 BGP 实例配置模式下，使用以下命令：

neighbor {*A.B.C.D* | *peer-group*} **filter-list** *access-list-number* {**in** | **out**}

- *A.B.C.D* | *peer-group* – 指定 BGP 对等体的 IP 地址或者对等体组的名称。
- *access-list-number* – 指定 AS 路径访问控制列表号。有关 AS 路径访问控制列表的更多信息，请参考“配置 AS 路径访问控制列表 “。
- **in** | **out** – 指定对引入的路由（**in**）或者向外发布的路由（**out**）进行过滤。

使用该命令 no 的形式取消基于 AS 路径访问控制列表的路由过滤配置：

no neighbor {*A.B.C.D* | *peer-group*} **filter-list** {**in** |**out**}

配置向对等体或者对等体组发送团体属性

配置向对等体（对等体组）发送团体属性，在 BGP 实例配置模式下，使用以下命令：

neighbor {*A.B.C.D* | *peer-group*} **send-community** {**standard** | **extended** | **both**}

- *A.B.C.D* | *peer-group* – 指定 BGP 对等体的 IP 地址或者对等体组的名称。
- **standard** | **extended** | **both** – 指定发送团体属性的类别，可以是标准团体属性（**standard**），扩展团体属性（**extended**），或者标准团体属性和扩展团体属性（**both**）。

使用该命令 no 的形式取消发送团体属性配置：

no neighbor {*A.B.C.D* | *peer-group*} **send-community**

配置基于路由映射表的路由过滤

BGP 协议支持通过路由映射表对对等体（对等体组）引入的路由或者向外发布的路由进行过滤。

配置基于路由映射表的路由过滤，在 BGP 实例配置模式下，使用以下命令：

neighbor {*A.B.C.D* | *peer-group*} **route-map** {**in** |**out**}

- *A.B.C.D* | *peer-group* – 指定 BGP 对等体的 IP 地址或者对等体组的名称。
- **in** | **out** – 指定对引入的路由（**in**）或者向外发布的路由（**out**）进行过滤。

使用该命令 no 的形式取消基于路由映射表的路由过滤配置：

no neighbor {*A.B.C.D* | *peer-group*} **route-map** {**in** |**out**}

等价负载均衡

配置 BGP 负载均衡的最大路径数，在 BGP 实例配置模式下，使用以下命令：

maximum-paths {**ebgp** | **ibgp**} *maximum-number*

- *maximum-number* – 指定 EBGP/IBGP 最大 ECMP 路径数。配置路径数后，若存在多条等价路径，多条路径均会被加入到路由表中。这样即可使 BGP 在多条路径上实现负载均衡。取值范围是 1 到 8，默认值是 1。

在 BGP 实例配置模式下，使用该命令 no 的形式取消等价负载均衡：

no maximum-paths {**ebgp** | **ibgp**}

注意：配置该功能前，用户需先开启 ECMP 功能。如何开启 ECMP，请参阅 "等价多径路由 (ECMP)"。

查看 BGP 信息

显示 BGP 路由信息，在任何模式下使用以下命令：

show ip route bgp [**vrouter** *vrouter-name*]

- *vrouter-name* – 显示指定 VRouter 的 BGP 路由信息。

显示整个 BGP 路由表的路由信息，在任何模式下使用以下命令：

show ip bgp [*A.B.C.D* | *A.B.C.D/M*] [**vrouter** *vrouter-name*]

- *A.B.C.D* | *A.B.C.D/M* – 显示到指定网络的 BGP 路由信息。
- *vrouter-name* – 显示指定 VRouter 的 BGP 路由信息。

显示 BGP 数据库中存储的所有自治系统路径信息，在任何模式下使用以下命令：

show ip bgp paths [**vrouter** *vrouter-name*]

- *vrouter-name* – 显示指定的 VRouter 的自治系统路径信息。

显示所有 BGP 连接的状态参数，包括前缀、路径和属性信息等，在任何模式下使用以下命令：

show ip bgp summary [**vrouter** *vrouter-name*]

- *vrouter-name* – 显示指定 VRouter 的 BGP 连接状态参数。

显示 BGP 对等体状态，在任何模式下使用以下命令：

show ip bgp neighbor [*A.B.C.D*] [**vrouter** *vrouter-name*]

- *A.B.C.D* – 显示指定对等体的状态。
- *vrouter-name* – 显示指定 VRouter 的 BGP 对等体的状态。

显示 BGP 团体属性列表信息，在任何模式下使用以下命令：

show ip community [*community-list-name*]

- *community-list-name* –显示指定名称或者序号的团体属性列表信息。如不输入该参数，则显示所有团体属性列表信息。

show ip as-path-access-list [*access-list-number*]

- *access-list-number* –显示指定序号的 AS 路径访问控制列表信息。如不输入该参数，则显示所有 AS 路径访问控制列表信息。

等价多径路由（ECMP）

等价多径路由（ECMP）是对经过安全设备的数据流量在多条等价路径（同协议）上进行负载均衡转发的方法。

配置 ECMP 功能

默认情况下，系统的 ECMP 功能为开启状态，并允许最多 40 条等价路由条目进行负载均衡。在 VRouter 配置模式下，使用以下命令开启或关闭 ECMP 功能：

ecmp enable *ecmp-route-num*

- *ecmp-route-num* – 系统允许的最大 ECMP 路由条目数。取值范围为 1 到 1000。当取值为 1 时表示不使用 ECMP 功能。

配置 ECMP 选路方式

在全局配置模式下，使用以下命令配置 ECMP 选路方式：

ecmp-route-select {**by-5-tuple** | **by-src** | **by-src-and-dst**}

- **by-5-tuple** – 基于五元组（源 IP 地址、目的 IP 地址、源端口、目的端口和服务类型）进行选路。
- **by-src** – 基于源 IP 地址进行选路。
- **by-src-and-dst** - 基于源 IP 地址和目的 IP 地址进行选路。该方式为系统默认选路方式。

静态组播路由

组播是将数据从一个源点传送到多个目的节点的一种通信方式。发送数据的源点称为组播源，接收数据的多个节点构成组播组。组播源将数据发送至目的地址，其地址范围是 224.0.0.0 至 239.255.255.255 之间的 D 类地址，称为组播地址。

互联网内任意一台主机均可作为组播源，源点只发送一份数据至组播地址，组内的所有接收者均可接收到相同的数据。应用组播方式传递信息，能够有效的节约网络带宽；如果接入网络用户数量增加，不会增大发送数据主机的负担，降低了网络负荷。

用户可以通过手工配置组播路由规则来实现将数据从组播源传送给组播成员。组播路由规则需要定义以下信息：

- 组播源和组播地址：即组播源 IP 和目的 IP。
- 入接口和出接口：匹配对应组播源和组播地址的数据从组播路由规则中指定的入接口进，从指定的出接口出。

开启/关闭组播路由功能

默认情况下，组播路由功能为关闭状态。在 VRouter 配置模式下，使用以下命令开启或关闭组播路由功能：

- 开启组播路由：**ip multicast-routing**
- 关闭组播路由：**no ip multicast-routing**

配置静态组播路由

在 VRouter 配置模式下，使用以下命令创建静态组播路由：

ip mroute *A.B.C.D A.B.C.D* [**iif** *interface-name*] [**eif** *interface-name*]

- *A.B.C.D A.B.C.D* – 指定组播源和组播地址。第一个 *A.B.C.D* 为组播源 IP 地址；第二个 *A.B.C.D* 为组播地址，其地址范围是 224.0.0.0 至 239.255.255.255 之间。
- **iif** *interface-name* – 指定入接口名称。在此命令中，最多允许用户指定 2 个入接口名称。
- **eif** *interface-name* – 指定出接口名称。在此命令中，最多允许用户指定 4 个出接口名称。

在 VRouter 配置模式下，使用该命令的 no 形式删除静态组播路由：

no ip mroute *A.B.C.D A.B.C.D* [**iif** *interface-name*] [**eif** *interface-name*]

指定入接口/出接口

用户可以为已创建的静态组播路由条目配置入接口或出接口。系统允许为每条组播路由条目最多配置 2 个入接口，32 个出接口。入接口或出接口的配置需要在静态组播路由配置模式下进行。

进入静态组播路由配置模式，在 VRouter 配置模式下，使用以下命令：

ip mroute *A.B.C.D A.B.C.D*

- *A.B.C.D A.B.C.D* – 指定组播源和组播地址。第一个 *A.B.C.D* 为组播源 IP 地址；第二个 *A.B.C.D* 为组播地址。

为已创建的静态组播路由条目指定入接口或出接口名称，在静态组播路由配置模式下，使用以下命令：

- 指定入接口名称：**iif** *interface-name*
- 指定出接口名称：**eif** *interface-name*

多次执行以上命令配置多个入接口或出接口。

显示组播路由信息

用户可以在任何模式下，随时使用 show 命令查看组播路由信息。命令如下：

show ip mroute [*A.B.C.D A.B.C.D* | **static** | **summary**] [**vrouter** *vr-name*]

- **show ip mroute** – 显示全部组播路由信息。
- *A.B.C.D A.B.C.D* – 通过指定组播源地址和组播地址，显示其组播路由信息。第一个 *A.B.C.D* 为组播源地址，第二个 *A.B.C.D* 为组播地址。
- **static** – 显示静态组播路由信息。
- **summary** – 显示组播路由的摘要信息。
- **vrouter** *vr-name* – 显示指定 VRouter 下的组播路由信息。

显示组播 FIB 信息

用户可以在任何模式下，使用以下命令查看组播 FIB 信息：

show mfib [*A.B.C.D A.B.C.D* | **summary**] [**vrouter** *vr-name*]

- **show mfib** – 显示所有组播 FIB 信息。
- *A.B.C.D A.B.C.D* – 通过指定组播源地址和组播地址，显示其组播 FIB 信息。第一个 *A.B.C.D* 为组播源地址，第二个 *A.B.C.D* 为组播地址。
- **summary** – 显示组播 FIB 的摘要信息。
- **vrouter** *vr-name* – 显示指定 VRouter 下的组播 FIB 信息。

互联网组管理协议

互联网组管理协议 IGMP（Internet Group Message Protocol）是用于在主机和路由器之间建立并维护组播成员关系的协议。通过 IGMP 协议，主机向路由器报告组成员的加入和离开，路由器周期性地发送查询报文查看是否有组成员处于活动状态，如果未收到组播成员的报告报文，则认为该组播组中已无组成员。

当前版本的 StoneOS 支持 IGMPv1（由 RFC1112 定义）、IGMPv2（由 RFC2236 定义）和 IGMPv3（由 RFC3376 定义）。并且支持 IGMP Proxy（工作在应用层）和 IGMP Snooping（工作在链路层）两个功能。

IGMP Proxy

IGMP Proxy 靠代理拦截主机和路由器之间的 IGMP 报文来建立组播路由表项，进行组播数据的转发。IGMP Proxy 在安全设备的两个接口上分别实现不同的功能。上联到组播路由器的上行接口代理实现主机的功能，响应来自路由器的查询。当组播组新增一个成员或者最后一个成员退出时，安全设备通过上行接口主动发送成员报告报文或者离开报文。下联到用户主机的下行接口代理实现路由器的功能，进行组成员的登记、查询和删除工作。

配置 IGMP 代理，请按照以下步骤进行操作：

1. 启用组播路由功能。具体操作，请参阅“开启/关闭组播路由功能”。
2. 启用 IGMP 代理功能。
3. 配置上行接口为主机模式，代理主机功能。
4. 配置下行接口为路由器模式，代理 IGMP 路由器功能。
5. 配置策略规则。

启用 IGMP 代理

在 VRouter 配置模式下，使用以下命令启用或禁用 IGMP 代理功能：

- 启用 IGMP 代理：**ip igmp-proxy enable**
- 禁用 IGMP 代理：**no ip igmp-proxy enable**

在全局配置模式下，使用以下命令进入 VRouter 配置模式：

ip vrouter *vrouter-name*

- *vrouter-name* – 指定 VRouter 的名称。如果指定的名称已存在，则直接进入 VRouter 配置模式。

配置接口的 IGMP 代理模式

在接口配置模式下，用户可使用以下命令配置接口的 IGMP 代理模式，使它处于主机模式或路由器模式：

ip igmp-proxy {**router-mode** | **host-mode**} [*A.B.C.D*] [**v2**| **v3**]

- **router-mode** – 配置下行接口的 IGMP 代理模式为路由器模式。
- **host-mode** – 配置上行接口的 IGMP 代理模式为主机模式。

- [A.B.C.D] – 指定组播组地址。配置组播地址后，系统认为 IGMP 代理模式仅对此组播地址有效。
- **v2** – 指定接口发送的 IGMP 报文的协议版本为 IGMPv2。默认情况下，使用 IGMPv2 协议。
- **v3** – 指定接口发送的 IGMP 报文的协议版本为 IGMPv3。

在接口配置模式下，使用该命令 no 的形式取消指定接口的 IGMP 代理模式：

no ip igmp-proxy {**router-mode** | **host-mode**} [*A.B.C.D*]

查看 IGMP Proxy 信息

用户可以在任何模式下，随时使用 show 命令查看 IGMP Proxy 信息。命令如下：

show ip igmp-proxy [*A.B.C.D*] [**vrouter** *vrouter-name*]

- **show ip igmp-proxy** – 查看系统中全部 IGMP Proxy 信息。
- [*A.B.C.D*] – 查看指定的组播组地址的 IGMP Proxy 信息。
- [**vrouter** *vrouter-name*] – 查看指定的 VRouter 下的 IGMP Proxy 信息。

IGMP Snooping

IGMP Snooping 是通过监听主机和路由器之间的 IGMP 报文，在二层设备上建立针对某个组播地址的组播路由表项。开启 IGMP Snooping 功能后，安全设备根据组播路由表项转发组播数据，有效的减少了组播通信的开销。如果没有开启 IGMP Snooping 功能，安全设备只能广播组播数据。

配置 IGMP Snooping，请按照以下步骤进行操作：

1. 开启组播路由功能。具体操作，请参阅“开启/关闭组播路由功能”。
2. 开启 IGMP Snooping 功能。
3. 配置 IGMP Snooping。
4. 配置策略规则。

启用 IGMP Snooping

在 VSwitch 配置模式下，使用以下命令启用或禁用 IGMP Snooping 功能：

- 启用 IGMP Snooping 功能：**ip igmp-snooping enable**
- 禁用 IGMP Snooping 功能：**no ip igmp-snooping enable**

在全局配置模式下，使用以下命令创建或进入 VSwitch 配置模式：

vswitch vswitch*Number*

- *Number* – 指定 VSwitch 的数字标识。*Number* 的取值范围根据平台不同而不同。例如，命令 **vswitch vswitch2** 创建了名为 VSwitch2 的 VSwitch，同时也创建了 VSwitchif2 接口，并且进入 VSwitch2 的配置模式。如果指定的 VSwitch 名称已存在，则直接进入 VSwitch 配置模式。

配置 IGMP Snooping

在接口配置模式下，使用以下命令配置 IGMP Snooping 功能：

ip igmp-snooping {**router-mode** [*A.B.C.D*] | **host-mode** [*A.B.C.D*] | **disable** | **auto**}

- **router-mode** – 配置下行接口的 IGMP Snooping 模式为路由器模式。
- **host-mode** – 配置上行接口的 IGMP Snooping 模式为主机模式。
- [*A.B.C.D*] – 指定组播组地址。
- **disable** – 禁用接口的 IGMP Snooping 功能。
- **auto** – 指定该参数，系统通过 IGMP 报文自动确定接口的模式。

在接口配置模式下，使用该命令 no 的形式取消配置 IGMP Snooping 功能：

no ip igmp-snooping {**router-mode** *A.B.C.D* | **host-mode** *A.B.C.D*}

未知组播丢弃

默认情况下，未知组播丢弃功能为关闭状态。开启该功能后，安全设备将丢弃发往未知组播组的报文，从而节省带宽。在 VSwitch 配置模式下，使用以下命令开启未知组播丢弃功能：

unknown-multicast drop

在 VSwitch 配置模式下，使用该命令 no 的形式关闭未知组播丢弃功能：

no unknown-multicast drop

查看 IGMP Snooping 信息

用户可以在任何模式下，随时使用 show 命令查看 IGMP Snooping 信息。命令如下：

show ip igmp-snooping [*A.B.C.D*] [**vswitch** *name*]

- **show ip igmp-snooping** – 显示全部 IGMP Snooping 信息。
- [*A.B.C.D*] – 查看指定的组播组地址的 IGMP Snooping 信息。
- [**vswitch** *name*] – 查看指定的 VSwitch 下的 IGMP Snooping 信息。

BFD

BFD（Bidirectional Forwarding Detection，双向转发检测）是一套全网统一的检测机制，用于快速检测、监控网络中链路或者 IP 路由的转发连通状况，为了提升现有网络性能，协议邻居之间必须能快速检测到通信故障，从而更快的建立起备用通道恢复通信。

BFD 在两台路由器上建立会话，用来监测两台路由器间的双向转发路径，为上层协议服务，如路由协议。BFD 本身并没有发现机制，而是靠被服务的上层协议通知其该与谁建立会话，会话建立后如果在检测时间内没有收到对端的 BFD 报文则认为发生故障，通知被服务的上层协议，上层协议进行相应的处理。

当前版本的 StoneOS 支持 BFD 与静态路由、OSPF、BGP 路由协议联动。实现在运行静态路由、OSPF、BGP 路由协议的链路上进行转发连通状况检测。

BFD 工作模式

BFD 会话建立有两种模式：主动模式和被动模式。目前只支持主动模式，不支持被动模式。

- 主动模式：在建立会话前不管是否收到对端发来的 BFD 控制报文，都会主动发送 BFD 控制报文。
- 被动模式：在建立会话前不会主动发送 BFD 控制报文，直到收到对端发送来的控制报文。在会话初始化过程中，通信双方至少要有一个运行在主动模式才能成功建立起会话。

BFD 会话建立后有两种检测模式：异步模式和查询模式。通信双方要求运行在相同的模式。

- 异步模式：以异步模式运行的设备周期性地发送 BFD 控制报文，如果在检测时间内对端没有收到 BFD 控制报文，则认为会话 down。
- 查询模式：假定有一个独立的方法，确认自己和对端系统的连通性。这样，BFD 会话建立后，会停止周期发送 BFD 控制报文，除非需要显式地验证连接性。

BFD Echo 功能

BFD Echo 功能即 BFD 回声功能，本端设备周期性地发送 BFD Echo 报文，远端设备不对报文进行处理，只通过转发通道将报文返回到本端。通过 Echo 功能，可以更快的检测到故障。

Echo 功能可以和两种检测模式配合使用，如果在异步模式下启用 Echo 功能，可以减少控制报文的发送;如果在查询模式下启用 Echo 功能,在 BFD 会话建立后可以取消发送 BFD 控制报文。

注意：如果需要使用 Echo 功能，在本端设备开启 Echo 功能的基础上，对端设备必须能够对 Echo

报文进行转发，否则功能不生效。

配置 BFD 基本功能

BGP 基本功能的配置包括以下各项：

- 配置 BFD 检测模式
- 配置 BFD 会话参数
- 开启/关闭 Echo 功能
- 指定接收 Echo 报文时间间隔
- 配置 Echo 报文的源 IP 地址

配置 BFD 检测模式

BFD 会话建立后有两种检测模式：异步模式和查询模式。通信双方要求运行在相同的模式。默认情况下，BFD 会话的检测模式为异步模式。用户可以根据需要指定 BFD 会话检测模式为查询模式，在接口配置模式下，使用以下命令：

bfd demand enable

在接口配置模式下使用该命令 no 的形式恢复默认为异步模式：

no bfd demand enable

配置 BFD 会话参数

在 BFD 会话建立之后，用户可以根据需要修改发送或接收 BFD 会话报文的最小时间间隔以及检测时间倍数。配置 BFD 会话检测参数，在接口配置模式下，使用以下命令：

bfd min-tx *min-tx-value* **min-rx** *min-rx-value* **detect-multiplier** *value*

- *min-tx-value* – 指定发送 BFD 报文的最小时间间隔，单位是毫秒。默认值为 100，取值范围为 100 到 1000。
- *min-rx-value* – 指定接收 BFD 报文的最小时间间隔，单位是毫秒。默认值为 100，取值范围为 100 到 1000。
- *value*– 指定检测时间倍数，用来计算检测超时时间。

使用 no bfd min-tx min-rx detect-multiplier 恢复默认 BFD 会话参数。

注意：检测超时时间计算方法如下：

- 异步模式：超时时间= max(本端配置的 min-tx-value,对端配置的 min-rx-value)* 对端检测时间倍数。
- 查询模式下并开启 Echo 功能：超时时间= max(本端配置的 min-tx-value,对端配置的

接收 Echo 报文时间间隔)* 本端检测时间倍数。

- 异步模式下并开启 echo 功能：超时时间= max(本端配置的 min-tx-value,对端配置的接收 Echo 报文时间间隔)* 对端检测时间倍数

关于如何配置接收 Echo 报文时间间隔，请参阅“指定接收 Echo 报文时间间隔”。

开启/关闭 Echo 功能

默认情况下，Echo 功能是关闭的，启用此功能，在接口配置模式下，使用以下命令：

```
bfd echo enable
```

在接口配置模式下，用该命令 no 的形式关闭此功能：

```
no bfd echo enable
```

指定接收 Echo 报文时间间隔

指定接收 BFD Echo 报文时间间隔，在接口配置模式下，使用以下命令：

bfd min-echo-rx *value*

- *value* – 指定接收 BFD Echo 报文时间间隔，单位为毫秒。取值范围是 100 到 1000 毫秒。默认为 0，即表示不接收 BFD Echo 报文。

在接口配置模式下，使用 **no bfd min-echo-rx** 命令恢复默认值。

配置 Echo 报文的源 IP 地址

为了避免对端发送大量的 ICMP 重定向报文造成网络拥塞，用户需要配置 Echo 报文的源 IP 地址，在接口配置模式下，使用以下命令：

bfd echo-source-ip *echo-src-address*

- *echo-src-address* – 指定 BFD Echo 报文的源 IP 地址。

在接口配置模式下，使用 **no bfd echo-source-ip** 命令删除 Echo 报文的源 IP 地址。

注意：

- Echo 报文的源 IP 地址用户可以任意指定。建议用户配置 Echo 报文的源 IP 地址不属于该设备任何一个接口所在网段。
- 本端发送 Echo 报文的目的地址使用本端接口地址。

配置 BFD 与路由协议联动

BFD 与路由协议联动的配置包括以下各项：

- 配置 BFD 与 静态路由联动
- 配置 BFD 与 OSPF 联动
- 配置 BFD 与 BGP 联动

配置 BFD 与 静态路由联动

由于静态路由没有发现邻居机制，BFD 与静态路由联动，如果 BFD 会话检测到故障，则表明该静态路由下一跳不可达，即不会添加此路由到路由表中，从而实现快速路由选路。

配置 BFD 与静态路由联动，对指定的静态路由下一跳开启 BFD 检测功能，在 VRouter 配置模式下，使用以下命令：

ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} *interface-name A.B.C.D* **bfd**

- *A.B.C.D/M* | *A.B.C.D A.B.C.D* – 指定静态路由条目的网络地址。安全网关支持两种方式，A.B.C.D/M 或者 A.B.C.D A.B.C.D，例如 1.1.1.0/24 或者 1.1.1.0 255.255.255.0。
- *interface-name A.B.C.D*– 指定下一跳接口地址。
- **bfd** – 对指定下一跳开启 BFD 检测功能。

在 VRouter 配置模式下，使用以上命令 no 的形式取消 BFD 与指定静态路由联动：

no ip route {*A.B.C.D/M* | *A.B.C.D A.B.C.D*} *interface-name A.B.C.D* **bfd**

配置 BFD 与 OSPF 联动

通过 BFD 与 OSPF 联动，实现优于 OSPF 协议 Hello 检测机制的快速链路检测，从而提高 OSPF 协议的收敛性能。

配置 BFD 与 OSPF 联动，对指定的 OSPF 相关接口上开启 BFD 检测功能，在接口配置模式下，使用以下命令：

ip ospf bfd

在接口配置模式下，使用以上命令 no 的形式取消 BFD 与 OSPF 联动：

no ip ospf bfd

配置 BFD 与 BGP 联动

配置 BFD 与 BGP 联动，对指定的 BGP 邻居开启 BFD 检测功能，在 BGP 实例配置模式下，使用以下命令：

neighbor *A.B.C.D* **fall-over bfd**

- *A.B.C.D* – 指定 BGP 对等体的 IP 地址。

在 BGP 实例配置模式下，使用以上命令 no 的形式取消 BFD 与指定 BGP 邻居联动：

no neighbor *A.B.C.D* **fall-over bfd**

显示 BFD 会话信息

显示 BFD 会话信息，在任何模式下使用以下命令：

show bfd session [**neighbor** [*A.B.C.D* | **detail**]]

- A.B.C.D – 指定相邻路由器的 ID。
- **detail**– 显示所有路由器的 BFD 会话详细信息。

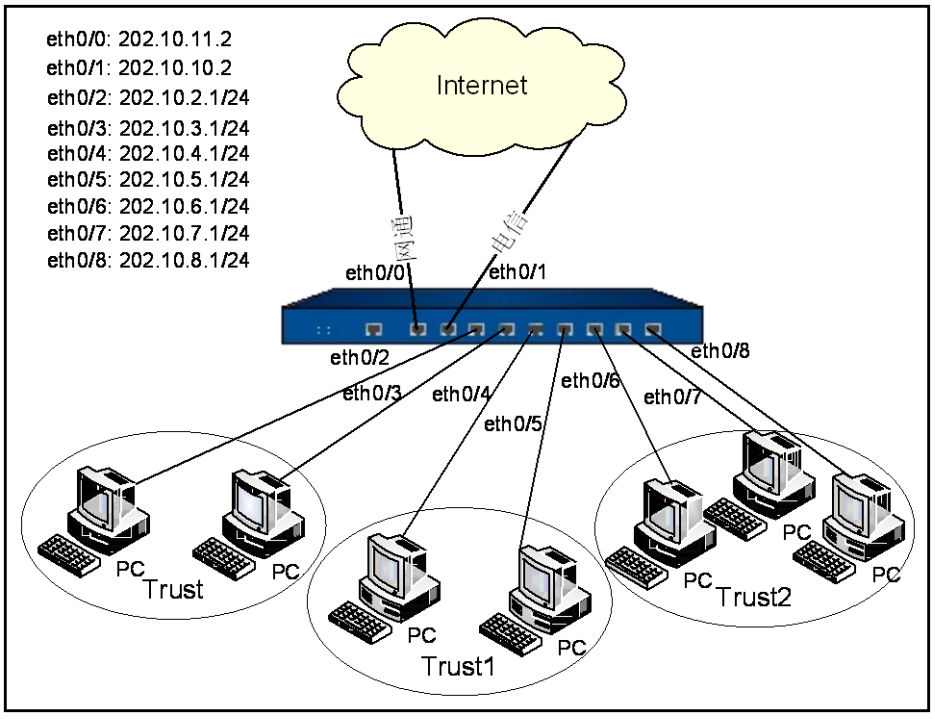
路由配置举例

本节介绍路由相关配置实例，包括开启/关闭静态路由查询功能配置举例、多 VR 配置举例、静态组播路由配置举例、IGMP Proxy 配置举例和链路负载均衡配置举例。

开启/关闭静态路由查询功能配置举例

设备的 ethernet0/0 和 ethernet0/1 两个接口分别连接网通和电信的两条线路，内网中 Trust 域和 Trust1 域的流量走网通线路，其它的流量走电信线路。组网图如下图所示：

图 2：开启/关闭静态路由查询功能配置组网图



如上图所示，接口 etherent0/0 和 ethernet0/1 属于 untrust 域，IP 地址分别是 202.10.11.2 和 202.10.10.2，接口 etherent0/2 和 ethernet0/3 属于 Ttrust 域，IP 地址分别是

202.10.2.1/24 和 202.10.3.1/24，接口 etherent0/4 和 ethernet0/5 属于 Ttrust1 域，IP 地址分别是 202.10.4.1/24 和 202.10.5.1/24，接口 etherent0/6、ethernet0/7 和 etherent0/8 属于 Ttrust2 域，IP 地址分别是 202.10.6.1/24、202.10.7.1/24 和 202.10.8.1/24。

配置步骤

以下配置步骤略去安全域以及接口配置，重点描述路由配置。路由配置：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 202.10.10.2（默认流量走电信）
hostname(config-vrouter)# ip route source 202.10.2.1/24 202.10.11.2（该网段流量走网通）
hostname(config-vrouter)# ip route source 202.10.3.1/24 202.10.11.2（该网段流量走网通）
hostname(config-vrouter)# ip route source 202.10.4.1/24 202.10.11.2（该网段流量走网通）
hostname(config-vrouter)# ip route source 202.10.5.1/24 202.10.11.2（该网段流量走网通）
```

根据以上源路由配置，Trust 和 Trust1 域的流量都走网通线路，而其它的流量走电信线路。如果由于某些原因，网通线路故障，Trust 和 Trust1 域的用户将无法上网，此时需要将以上的四条源路由删除，流量才会全部汇总到电信线路进行传输。如果相关的源路由很多，删除工作和线路故障排除后的路由添加工作的工作量将十分庞大，同时也容易出错。现在的解决方案是：线路故障时，关闭源路由的查询，Trust 和 Trust1 域的用户就都可以走默认路由通过电信线路上网。配置命令如下：

```
hostname(config)# route disable sbr
```

故障排除后，重新开启源路由的查询功能：

```
hostname(config)# route enable sbr
```

多 VR 配置举例

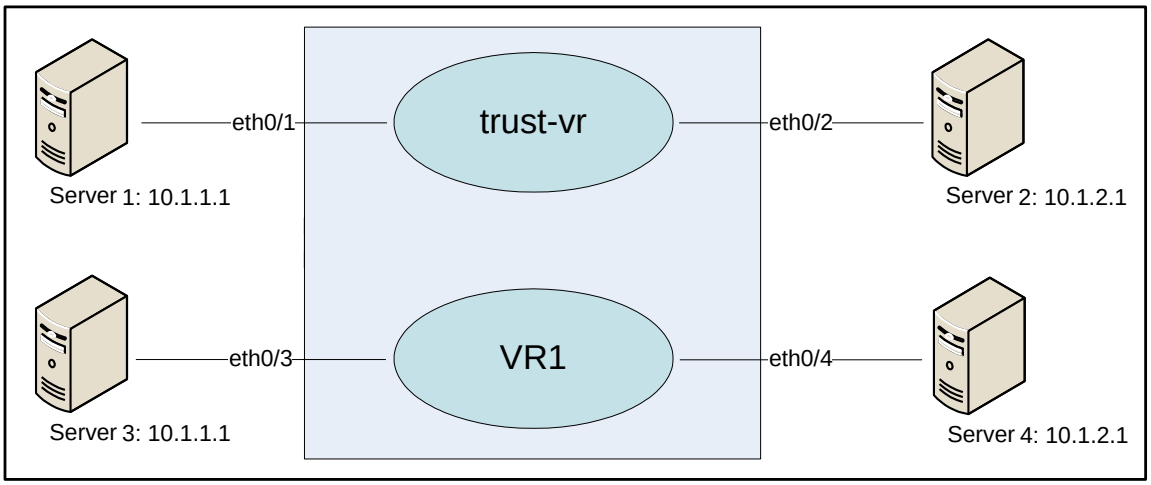
本节介绍几个多 VR 配置的具体实例，包括

- 多 VR 独立转发
- 跨 VR 转发

多 VR 独立转发

Trust-vr 和 VR1 两个 VR 中有重叠的 IP 地址段，但是要求两个 VR 的数据转发各自进行，互不影响。组网图如下图所示：

图 3：多 VR 独立转发组网图



系统有两个 VR，分别是 trust-vr 和 VR1。接口 ethernet0/1 属于 zone1，ethernet0/2 属于 zone2，zone1 和 zone2 均属于 trust-vr；接口 ethernet0/3 属于 zone3，ethernet0/4 属于 zone4，zone3 和 zone4 均属于 VR1。接口 ethernet0/1 和 ethernet0/3 的 IP 地址重叠，而 ethernet0/2 和 ethernet0/4 的 IP 地址也重叠。

配置步骤

第一步：开启 Hillstone 设备的多 VR 功能：

```
hostname# exec vrouter enable
Warning: please reboot the device to make the change validation!
hostname# reboot
System reboot, are you sure? y/[n]: y
```

第二步：重启设备后，创建 VR1：

```
hostname(config)# ip vrouter VR1
```

第三步：配置接口以及安全域（zone1 和 zone2 默认属于 trust-vr）：

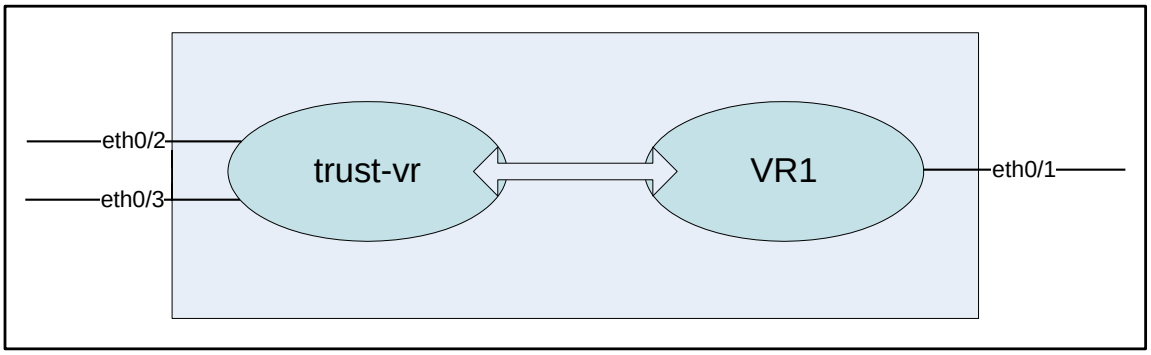
```
hostname(config)# zone zone1
hostname(config-zone-zone1)# exit
hostname(config)# zone zone2
hostname(config-zone-zone2)# exit
hostname(config)# zone zone3
hostname(config-zone-zone3)# vrouter VR1
hostname(config-zone-zone3)# exit
hostname(config)# zone zone4
```

```
hostname(config-zone-zone4)# vrouter VR1
hostname(config-zone-zone4)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone zone1
hostname(config-if-eth0/1)# ip address 10.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone zone2
hostname(config-if-eth0/2)# ip address 10.1.2.1/24
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone zone3
hostname(config-if-eth0/3)# ip address 10.1.1.1/24
hostname(config-if-eth0/3)# exit
hostname(config)# interface ethernet0/4
hostname(config-if-eth0/4)# zone zone3
hostname(config-if-eth0/4)# ip address 10.1.2.1/24
hostname(config-if-eth0/4)# exit
hostname(config)#
```

跨 VR 转发

系统有两个 VR，即 trust-vr 和 VR1。要求实现 trust-vr 通过 VR1 进行数据转发。组网图如下图所示：

图 4：跨 VR 转发组网图



系统有两个VR,分别是trust-vr和VR1。接口ethernet0/0属于zone1,zone1属于trust-vr;接口 ethernet0/2 和 ethernet0/3 属于 zone2，zone2 属于 trust-vr。通过配置，实现 trust-vr 通过 VR1 进行数据转发。

配置步骤

第一步：开启 Hillstone 设备的多 VR 功能：

```
hostname# exec vrouter enable
Warning: please reboot the device to make the change validation!
```

```
hostname# reboot
System reboot, are you sure? y/[n]: y
```

第二步：重启设备后，创建 VR1：

```
hostname(config)# ip vrouter VR1
```

第三步：配置接口以及安全域（和 zone2 默认属于 trust-vr）：

```
hostname(config)# zone zone1
hostname(config-zone-zone1)# vrouter VR1
hostname(config-zone-zone1)# exit
hostname(config)# zone zone2
hostname(config-zone-zone2)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone zone1
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone zone2
hostname(config-if-eth0/2)# ip address 10.1.1.1/24
hostname(config-if-eth0/2)# exit
hostname(config)# interface ethernet0/3
hostname(config-if-eth0/3)# zone zone2
hostname(config-if-eth0/3)# ip address 10.1.2.1/24
hostname(config-if-eth0/3)# exit
hostname(config)#
```

第四步：配置跨 VR 转发路由：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 0.0.0.0/0 vrouter VR1
hostname(config-vrouter)# exit
hostname(config)# ip vrouter VR1
hostname(config-vrouter)# ip route 10.1.1.0/24 vrouter trust-vr
hostname(config-vrouter)# ip route 10.1.2.0/24 vrouter trust-vr
hostname(config-vrouter)# exit
hostname(config)#
```

静态组播路由配置举例

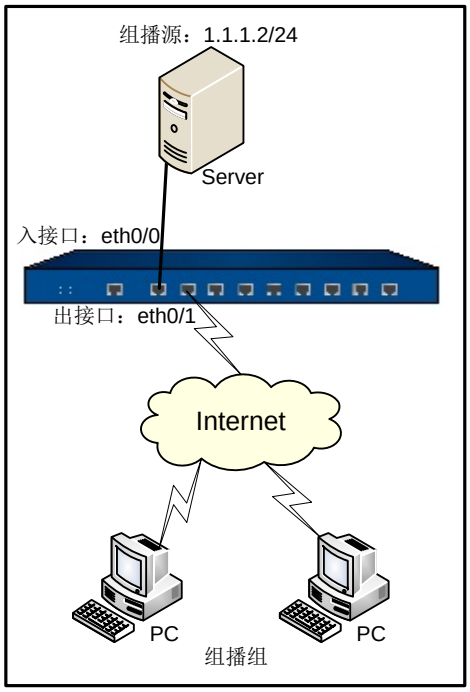
本节介绍一个静态组播路由的配置举例。

组网需求

组播源发送数据至组播组，组播地址为 224.91.91.2。接口 ethernet0/0 属于 trust 安全域，为组播数据入接口；接口 ethernet0/1 属于 untrust 安全域，为组播数据出接口。配置静态组播

路由使组播数据可以正常转发给属于组播组的客户端 PC。组网图如下图所示：

图 5：组播路由配置举例组网图



配置步骤

第一步：配置接口和安全域：

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone trust
hostname(config-if-eth0/0)# ip address 1.1.1.1/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 2.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

第二步：配置并开启静态组播功能：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# ip mroute 1.1.1.2 224.91.91.2 iif ethernet0/0 eif
ethernet0/1
hostname(config-vrouter)# exit
hostname(config)#
```

第三步：配置策略：

```
hostname(config)# address src
hostname(config-addr)# ip 1.1.1.2/32
hostname(config-addr)# exit
```

```
hostname(config)# address dst
hostname(config-addr)# ip 224.91.91.2/32
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone trust
hostname(config-policy-rule)# dst-zone untrust
hostname(config-policy-rule)# src-addr src
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

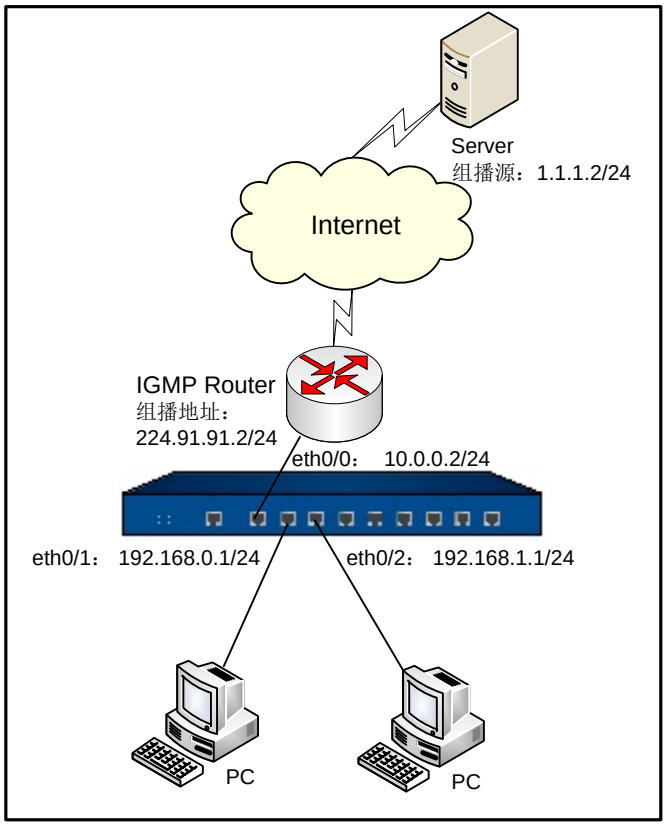
IGMP Proxy 配置举例

本节介绍一个 IGMP Proxy 的配置举例。

组网需求

组播源发送数据至组播组，组播地址为 224.91.91.2。ethernet0/0 为上行接口，ethernet0/1 和 ethernet0/2 为下行接口。配置 IGMP Proxy 使组播数据可以正常转发给属于组播组的客户端 PC。组网图如下图所示：

图 6：IGMP Proxy 配置举例组网图



配置步骤

第一步：配置接口和安全域：

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 10.0.0.2/24
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# ip address 192.168.0.1/24
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone trust
hostname(config-if-eth0/2)# ip address 192.168.1.1/24
hostname(config-if-eth0/2)# exit
hostname(config)#
```

第二步：开启组播路由功能：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# exit
hostname(config)#
```

第三步：开启并配置 IGMP Proxy 功能：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip igmp-proxy enable
hostname(config-vrouter)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# ip igmp-proxy host-mode
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# ip igmp-proxy router-mode
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip igmp-proxy router-mode
hostname(config-if-eth0/2)# exit
hostname(config)#
```

第四步：配置策略：

```
hostname(config)# address src
hostname(config-addr)# ip 1.1.1.2/32
hostname(config-addr)# exit
hostname(config)# address dst
hostname(config-addr)# ip 224.91.91.2/32
hostname(config-addr)# exit
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone untrust
hostname(config-policy-rule)# dst-zone trust
hostname(config-policy-rule)# src-addr src
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

IGMP Snooping 配置举例

本节介绍一个 IGMP Snooping 的配置举例。

组网需求

组播源发送数据至组播组，组播地址为 224.91.91.2。设备工作在透明模式，ethernet0/0 为上行接口，ethernet0/1 和 ethernet0/2 为下行接口。配置 IGMP Snooping 使组播数据可以正常转发给属于组播组的客户端 PC。

配置步骤

第一步：配置接口和安全域：

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone l2-untrust
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone l2-trust
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# zone l2-trust
hostname(config-if-eth0/2)# exit
hostname(config)# interface vswitchif1
        hostname(config-if-vsw1)# ip address 192.30.1.100 255.255.255.0
hostname(config-if-vsw1)# exit
        hostname(config)#
```

第二步：开启组播路由功能：

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip multicast-routing
hostname(config-vrouter)# exit
hostname(config)#
```

第三步：开启并配置 IGMP Snooping 功能：

```
hostname(config)# vswitch vswitch1
hostname(config-vswitch)# ip igmp-snooping enable
hostname(config-vswitch)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# ip igmp-snooping host-mode
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# ip igmp-snooping router-mode
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet0/2
hostname(config-if-eth0/2)# ip igmp-snooping router-mode
hostname(config-if-eth0/2)# exit
hostname(config)#
```

第四步：配置策略：

```
hostname(config)# address src
hostname(config-addr)# ip 1.1.1.2/32
hostname(config-addr)# exit
hostname(config)# address dst
hostname(config-addr)# ip 224.91.91.2/32
hostname(config-addr)# exit
hostname(config)# policy-global
```

```
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone l2-untrust
hostname(config-policy-rule)# dst-zone l2-trust
hostname(config-policy-rule)# src-addr src
hostname(config-policy-rule)# dst-addr dst
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

BFD 配置举例

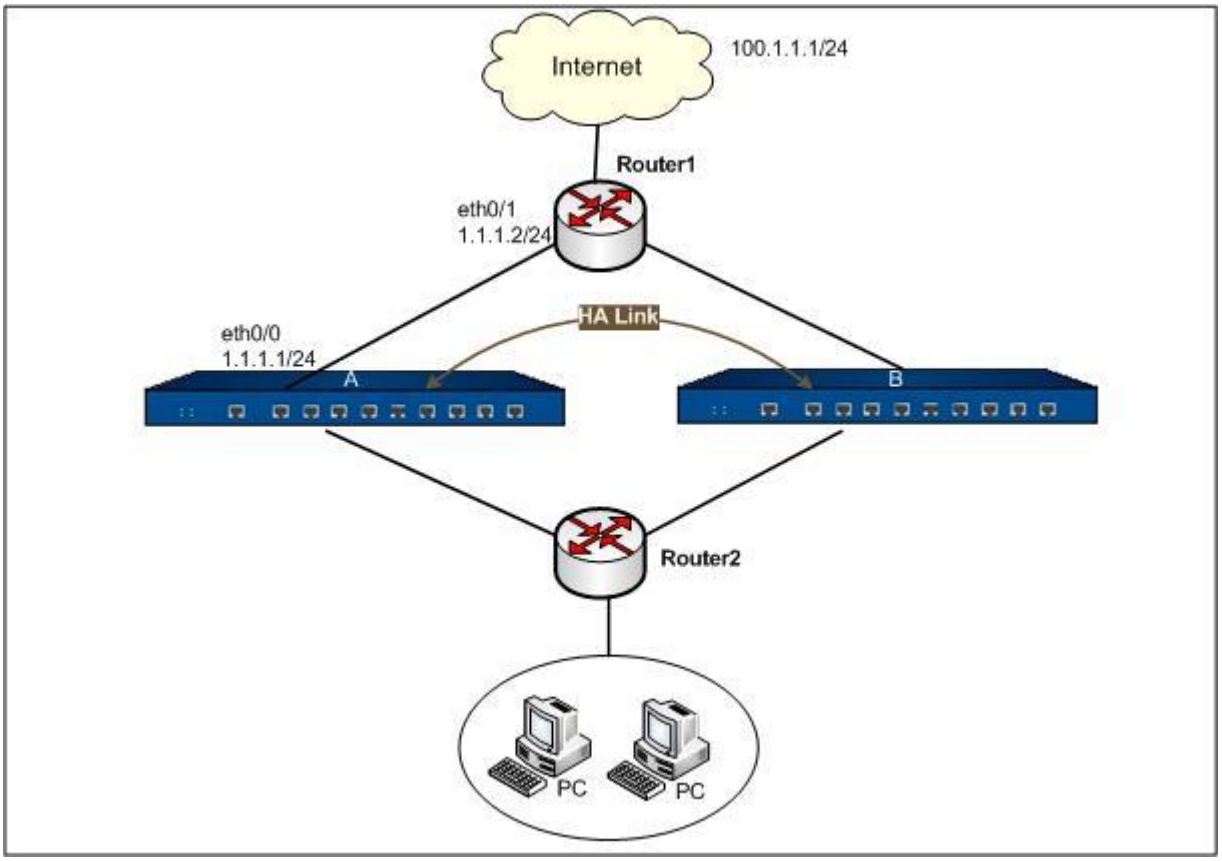
本节列举 3 个 BFD 的配置实例，分别是：

- BFD 与静态路由联动配置举例
- BFD 与 OSPF 联动配置举例
- BFD 与 BGP 联动配置举例

组网需求

两台安全网关和两台路由器组成一个冗余链路，路由器与安全网关之间采用 BFD 检测。Router1 可达网段为 100.1.1.1/24。以 Router1 与安全网关 A 之间的配置为例，介绍 BFD 与静态路由、OSPF、BGP 联动的配置。组网图如下图所示：

图 7：BFD 与静态路由联动组网图



配置步骤

BFD 与静态路由联动配置

第一步：配置安全网关 A 的接口。

安全网关 A

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

第二步：在安全网关 A 的接口上配置 BFD 会话参数。检测模式默认为异步模式。

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# bfd min-tx 100 min-rx 100 detect-multiplier
3
hostname(config-if-eth0/0)# exit
hostname(config)#
```

第三步：在安全网关 A 上配置 BFD 与静态路由 Router1 联动。

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# ip route 100.1.1.1/24 ethernet0/1 1.1.1.2 bfd
hostname(config-vrouter)# exit
```

```
hostname(config)#
```

第四步：配置 Router1 的接口以及 BFD 基本功能。接口地址 1.1.1.2/24。

BFD 与 OSPF 联动配置

第一步：配置安全网关 A 的接口。

```
安全网关 A
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

第二步：在安全网关 A 的接口上配置 BFD 会话参数。检测模式指定为查询模式并开启 Echo 功能，以及配置 BFD 与 OSPF 联动。

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# bfd demand enable
hostname(config-if-eth0/0)# bfd min-echo-rx 100
hostname(config-if-eth0/0)# bfd echo enable
hostname(config-if-eth0/0)# ip ospf bfd
hostname(config)#
```

第三步：在安全网关 A 上配置 OSPF 协议。

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router ospf
hostname(config-router)# route id  1.1.1.1
hostname(config-router)# network 1.1.1.1/24 area 0
hostname(config-router)# exit
hostname(config)#
```

第四步：配置 Router1 的接口、BFD 基本功能以及 OSPF 协议。接口地址 1.1.1.2/24，检测模式指定为查询模式并开启 Echo 功能，且需要能够对 Echo 报文进行转发。

BFD 与 BGP 联动配置

第一步：配置安全网关 A 的接口。

```
安全网关 A
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone untrust
hostname(config-if-eth0/1)# ip address 1.1.1.1/24
hostname(config-if-eth0/1)# exit
hostname(config)#
```

第二步：在安全网关 A 的接口上配置 BFD 会话参数。检测模式指定为查询模式并开启 Echo 功能。

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# bfd demand enable
hostname(config-if-eth0/0)# bfd min-echo-rx 100
```

```
hostname(config-if-eth0/0)# bfd echo enable
hostname(config-if-eth0/0)# exit
hostname(config)#
```

第三步：在安全网关 A 上配置 BGP 协议以及配置 BFD 与 BGP 联动。

```
hostname(config)# ip vrouter trust-vr
hostname(config-vrouter)# router bgp 100
hostname(config-router)# route id 1.1.1.1
hostname(config-router)# neighbor 1.1.1.2 fall-over bfd
hostname(config-router)# network 1.1.1.1/24
hostname(config-router)# exit
hostname(config)#
```

第四步：配置 Router1 的接口、BFD 基本功能以及 BGP 协议。接口地址 1.1.1.2/24，检测模式指定为查询模式并开启 Echo 功能，且需要能够对 Echo 报文进行转发。