Hillstone Networks Inc.

StoneOS CLI User Guide

High Availability

Version 5.5R6



Copyright 2018 Hillstone Networks Inc. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished under a license agreement or nondisclosure agreement. The software may be used or copied only in accordance with the terms of those agreements. No part of this publication may be reproduced, stored in a retrieval system, or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Hillstone Networks Inc.

Hillstone Networks Inc

Contact Information:

US Headquarters:

Hillstone Networks

292 Gibraltar Drive, Suite 105

Sunnyvale, CA 94089

Phone: 1-408-508-6750

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

About this Guide:

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

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

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

hs-doc@hillstonenet.com

TWNO: TW-CUG-UNI-HA-5.5R6-EN-V1.0-Y18M07

Table of Contents

Table of Contents *3*
About This Guide *1*
Content 1
CLI 1
WebUI 1
Command Line Interface 2
High Availablity (HA) *8*
Overview 8
Configuring HA 12
Twin-mode HA 26
Examples of Configuring HA 37

About This Guide

This document follows the conventions below:

Content

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

CLI

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

WebUI

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

Command Line Interface

Overview

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

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

CLI Modes and Prompts

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

Execution Mode

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

```
hostname#
```

Global Configuration Mode

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

```
hostname(config)#
```

Sub-module Configuration Mode

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

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

Switching between CLI Modes

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

Table 1: CLI Mode Switching Commands

Mode	Command

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

CLI Error Message

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

Table 2: Error Messages and Description

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

Command Input

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

Command Short Form

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

Listing Available Commands

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

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

Completing Partial Commands

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

Using CLI

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

Previous Commands

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

Shortcut Keys

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

Table 3: Shortcut Key List

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

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

Filtering Output of Show Commands

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

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

CLI output filter syntax is shown as follows:

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

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

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

Table 4: Regular Expression and Meaning

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

CLI Page Display

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

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

Specifying Screen Size

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

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

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

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

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

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

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

Specifying Connection Timeout

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

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

`console timeout` *`timeout-value`*

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

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

ssh timeout *timeout-value*

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

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

telnet timeout *timeout-value*

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

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

Redirecting the Output of Show Commands

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

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

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

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

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

Diagnostic Commands

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

High Availablity (HA)

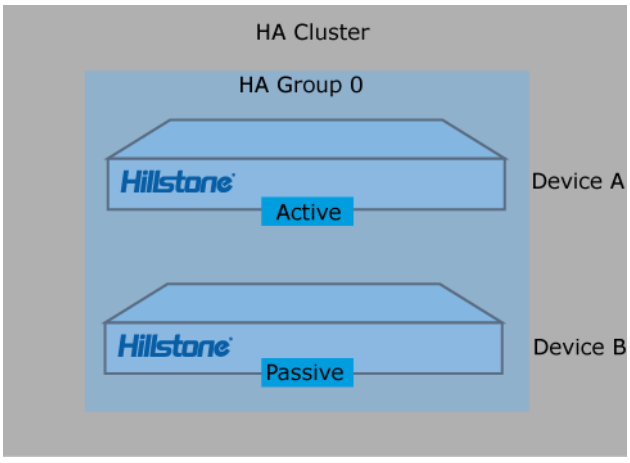
Overview

HA (High Availability) provides a failover solution for malfunction of the communication line or devices in order to ensure smooth communication and effectively improve the network reliability. To implement the HA function, you need to group two Hillstone devices as an HA cluster, using the identical hardware platform, firmware version, and licenses. When one device is unavailable or cannot handle the request from the client properly, the request will be promptly directed to the other device that works normally, thus ensuring uninterrupted network communication and greatly improving the reliability of communications.

Hillstone devices support three HA modes: Active-Passive (A/P), Active-Active (A/A), and Peer mode.

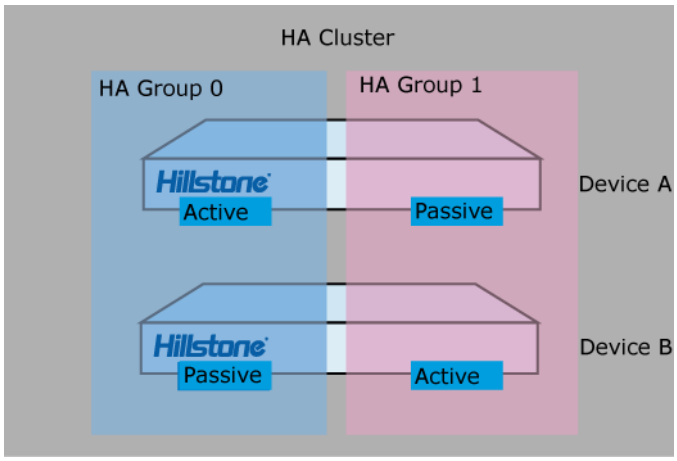
- Active-Passive (A/P) mode: In the HA cluster, configure two devices to form an HA group, with one device acting as a master device and the other acting as its backup device. The master device is active, forwarding packets, and meanwhile synchronizes all of its network and configuration information and current session information to the backup device. When the master device fails, the backup device will be promoted to master and take over its work to forward packets. This A/P mode is redundant, and features a simple network structure for you to maintain and manage. The relationship between the devices in A/P mode is shown below:

  Figure 1: Relationship between the Devices in A/P Mode



- Active-Active (A/A) mode: When the security device is in NAT mode, routing mode or a combination of both, you can configure both the Hillstone devices in the HA cluster as active, so that they can perform their own tasks simultaneously, and monitor the operation status of each other. When one device fails, the other will take over the work of the failure device and also run its own tasks simultaneously to ensure uninterrupted work. This mode is known as the Active-Active mode. The A/A mode ensures high-performance and is able to provide load-balancing function. The relationship between the devices in A/A mode is shown below:

Figure 2: Relationship between the Devices in A/A Mode



As shown above, Device A acts as the master device of HA Group 0 and backup device of HA Group 1; HA Device B acts as the master device of HA Group 1 and backup device of HA Group 0. The master device of HA Group 0 is known as Admin Master, and the master device of HA Group 1 is known as Master.

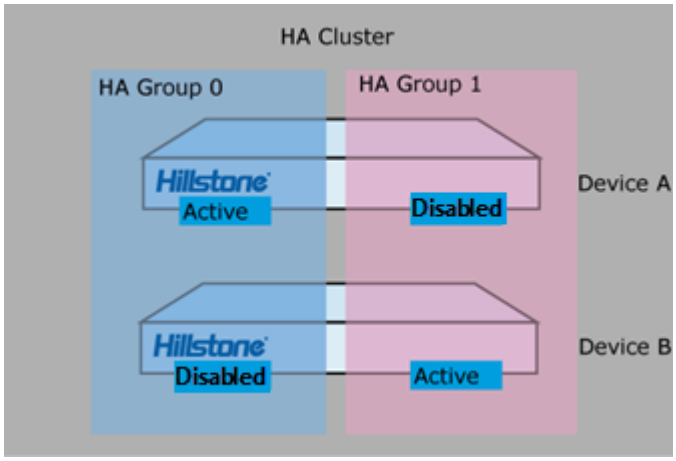
When configuring the HA Active-Active mode, you're recommended to take the following steps to avoid configuration synchronization failure between the master and backup device:

- Configure parameters in the Admin Master;
- First enable HA on Admin Master, and then enable HA on Master;

Note: If possible, configure the devices that are enabled with HA when the operation status of HA is stable, in order to avoid configuration synchronization failure or slow execution of the configuration commands.

- Peer mode: the Peer mode is a special HA Active-Active mode. In the Peer mode, two devices are both active, perform their own tasks simultaneously, and monitor the operation status of each other. When one device fails, the other will take over the work of the failure device and also run its own tasks simultaneously. In the Peer mode, only the device at the active status can send/receive packets. The device at the disabled status can make two devices have the same configuration information but its interfaces do not send/receive any packets. The Peer mode is more flexible and is suitable for the deployment in the asymmetric routing environment. The relationship between the devices in the Peer mode is shown in the figure below:

Figure 3:: **Relationship between the Devices in A/A Mode**



HA Cluster

For the external network devices, an HA cluster is a single device which handles network traffic and provides security services. The HA cluster is identified by its cluster ID. After specifying an HA cluster ID for the device, the device will be in the HA state to implement HA function.

HA Group

System will select the master and backup device of the same HA group ID in an HA cluster according to the HCMP protocol and the HA configuration. The master device is in active state and processes network traffic. When the master device fails, the backup device will take over its work.

When assigning a cluster ID to the device, the HA group with ID 0 will be automatically created. In Active-Passive (A/P) mode, the device only has HA group 0. In Active-Active (A/A) mode, the latest Hillstone version supports two HA groups, i.e., Group 0 and Group 1.

HA Node

To distinguish the HA device in an HA group, you can use the value of HA Node to mark the devices. StoneOS support the values of 0 and 1.

In the HA Peer mode, the system can decide which device is the master according to the HA Node value. In the HA group 0, the device whose HA Node value is 0 will be active and the device whose HA Node value is 1 is at the disabled status. In the HA group 1, the device whose HA Node value is 0 is at the disabled status and the device whose HA Node value is 0 is active.

HA Group Interface and Virtual MAC

In the HA environment, each HA group has an interface to forward traffic, which is known as Virtual Forward Interface. The master device of each HA group manages a virtual MAC (VMAC) address which corresponds to its interface and the traffic is forwarded on the interface. Different HA groups in an HA cluster cannot forward data

among each other. VMAC address is defined by HA base MAC, HA cluster ID, HA group ID and the physical interface index.

HA Selection

In an HA cluster, if the group ID of the HA devices is the same, the one with higher priority will be selected as the master device.

HA Synchronization

To ensure the backup device can take over the work of the master device when it fails, the master device will synchronize its information with the backup device. There are 3 types of information that can be synchronized: configuration information, files and RDO (Runtime Dynamic Object). The specific content of RDO includes:

- Session information (The following types of session information will not be synchronized: the session to the device itself, tunnel session, deny session, ICMP session, and the tentative session)
- IPsec VPN information
- SCVPN information
- DNS cache mappings
- ARP table
- PKI information
- DHCP information
- MAC table
- WebAuth information

StoneOS supports two methods to synchronize: real-time synchronization and batch synchronization. When the master device has just been selected successfully, the batch synchronization will be used to synchronize all information of the master device to the backup device. When the configurations change, the real-time synchronization will be used to synchronize the changed information to the backup device. Except for the HA related configurations and local configurations (for example, the host name), all the other configurations will be synchronized.

Notes:

- If you configure Local property for an interface , the system will not synchronize this configuration with the backup device. For this reason, it is recommended not to configure the Local property for the business interface.
- For some models (SG-6000-X6150, SG-6000-X6180, and SG-6000-X7180),in the Active-Passive (A/P) mode , the backup device dose not support hot plugging of IOM module, otherwise it will affect the synchronization configuration information.

Configuring HA

To configure the HA function, take the following steps:

1. Configure an HA group, including specifying the device priority (for selection) and HA packets-related parameters.
2. Configure an HA virtual forward interface.
3. Configure HA link interface which is used for the device synchronization and HA packets transmission.
4. Configure an HA cluster. Specify the ID of HA cluster and enable the HA function.

WebUI: Select **System** > **HA** from the menu bar. In the HA dialog, configure the options.

Configuring an HA Group

The HA group need to be configured in the HA group configuration mode. To enter the HA group configuration mode, in the global configuration mode, use the following command:

ha group *group-id*

- *group-id* - Specifies the HA group ID. The value range is 0 to 1.

After executing the command, the system will enter the HA group configuration mode. To delete the specified HA group, in the global configuration mode, use the following command:

no ha group *group-id*

In the HA group configuration mode, you can perform the following configurations:

- Specifying the priority
- Specifying the Hello interval
- Specifying the Hello threshold
- Configuring the preempt mode
- Specifying the gratuitous ARP packet number
- Specifying the description
- Specifying the track object

Specifying the Priority

The priority specified by the command is for used for HA selection. The device with higher priority (the smaller number) will be selected as the master device. To specify the priority, in the HA group configuration mode, use the following command:

priority *number*

- *number* - Specifies the priority. The value range is the 1 to 254. The default value is 100.

To restore to the default priority, in the HA group configuration mode, use the following command:

no priority

Note: When the priorities are identical, the device with smaller value in the 10th to 14th bit of the device S/N will be priorized.

Specifying the Hello Interval

Hello interval refers to the interval for the HA device to send heartbeats (Hello packets) to other devices in the HA group. The Hello interval in the same HA group must be identical. To specify the Hello interval, in the HA group configuration mode, use the following command:

hello interval *time-interval*

- *time-interval* - Specifies the interval for sending heartbeats. The value range is 50 to 10000 milliseconds. The default value is 1000.

To restore to the default Hello interval, in the HA group configuration mode, use the following command:

no hello interval

Specifying the Hello Threshold

If the device does not receive the specified number of Hello packets from the other device, it will judge that the other device's heartbeat fails. To specify the Hello threshold, in the HA group configuration mode, use the following command:

hello threshold *value*

- *value* - Specifies the Hello threshold value. The value range is 3 to 255. The default value is 3.

To restore to the default Hello threshold, in the HA group configuration mode, use the following command:

no hello threshold

Specifying the Hello Transport Protocol

This feature is only supported for CloudEdge. By default, the transport protocol of Hello packets is VRRP.But in a virtualized environment, the virtual core switch restricts both the transmission rate and the packet size of VRRP packets, affecting the synchronization function between the HA master and the backup device. You can change the transport protocol of Hello with UDP protocol to prevent the restriction, in the HA group configuration mode, use the following command:

ha transmit udp

To restore to the default protocol VRRP, in the HA group configuration mode, use the following command:

no ha transmit udp

Notes:

- When device is added to HA cluster and HA function take effective, you can not change the Hello transport protocol.If you want to change it, execute the command no ha cluster firstly.
- The master device and the backup device shoud be configured with the same Hello transport protocol.

Configuring the Preempt Mode

When the preempt mode is enabled, once the backup device find its own priority is higher than the master device, it will upgrade itself to the master device and the original master device will become the backup device. When the preempt mode is disabled, even if the device's priority is higher than the master device, it will not take over the master device unless the master device fails. When configuring the preempt mode, you can also set the delay time to make the backup device take over the master device after the specified delay time. To configure the preempt mode, in the HA group configuration mode, use the following command:

preempt [*delay-time*]

- *delay-time* - Specifies the delay time. The value range is 1 to 600 seconds. The default value is 30.

To cancel the preempt mode, in the HA group configuration mode, use the following command:

no preempt

Specifying the Gratuitous ARP Packet Number

When the backup device is selected as the master device, it will send an ARP request packet to the network to inform the relevant network devices to update its ARP table. This command is used to specify the number of ARP packets the upgraded master device will send. The maximum number of gratuitous ARP packages sent by new master device is determined by the number of sending gratuitous ARP packets specified by this command. The system will send five gratuitous ARP packets immediately after device switching, and sending one ARP packets per second until the number of gratuitous ARP packets reaches the number specified by this command. To specify the gratuitous ARP packet number, in the HA group configuration mode, use the following command:

arp *number*

- *number* - Specify the gratuitous ARP packet number. The value range is 10 to 180. The default value is 15.

To restore to the default gratuitous ARP packet number, in the HA group configuration mode, use the following command:

no arp

Sending Gratuitous ARP Packets

When the backup device is promoted to the master device, since the new master device only sent rather limited ARP packets to the network, some servers in the network may be unable to receive any ARP packets and therefore unable to update the ARP table. As a result, these servers may be unable to provide normal service within a short period. To solve the problem, the system supports sending gratuitous ARP packets manually via a specified interface. To send gratuitous ARP packets via the specified interface, in the execution mode, use the following command:

send gratuitous-arp interface *interface-name* [**count** *num* | **interval** *num*]

- **interface** *interface-name* - Specifies the interface on which gratuitous ARP packets are sent. This interface can be a physical interface, VSwitch interface, aggregate interface or redundant interface with an IP address configured.
- **count** *num* - Specifies the count for sending ARP packets. The value range is 0 to 60. The default value is 5. Value 0 indicates sending the packets consistently. You can stop sending by pressing Ctrl+C.
- **interval** *num* - Specifies the interval for sending ARP packets. The value range is 1 to 60 seconds. The default value is 1.

Specifying the Description

To specify description information, in the HA group configuration mode, use the following command:

description *string*

- *string* - Specifies the description information.

To cancel the description information, in the HA group configuration mode, use the following command:

no description

Specifying the Track Object

The track object is used to monitor the working status of the device. When the device cannot work normally, the system will take the corresponding action. To specify the track object, in the HA configuration mode, use the following command:

monitor track *track-object-name*

- *track-object-name* - Specifies the name of the track object configured in the system.

To cancel the track object, in the HA configuration mode, use the following command:

no monitor track

Tip: It is recommended that the track object in the HA group shoud be configured with the Local property. For more information about how to configure the track object, see "Configuring a Track Object" of "System Management"

Configuring an HA group interface

To configure the interface for HA Group 0, in the global configuration mode, use the following command:

interface {**ethernet***m/n* | **redundant***number* | **aggregate***number* | **tunnel***number* | **loopback***number* | **bgroup***number* | **ethernet***m/n.tag* | **redundant***number.tag* | **aggregate***number.tag*}

Tip: For more information about how to create and configure an interface, see "Interface" of "Firwall".

To configure the interface for HA Group 1, in the global configuration mode, use the following command:

interface {**ethernet***x/y*:*z* | **redundant***x*:*z* | **aggregate***x*:*z* | **tunnel***x*:*z* | **loopback***x*:*z* | **ethernet***x/y.u*:*z* | **redundant***x.y*:*z* | **aggregate***x.y*:*z*}

- **ethernet***x/y*:*z*: Specifies ethernetx/y as the interface for Group z and uses this interface for data forwarding.
- **redundant***x*:*z*: Specifies redundantx as the interface for Group z and uses this interface for data forwarding.
- **aggregate***x*:*z*: Specifies aggregatex as the interface for Group z and uses this interface for data forwarding.
- **tunnel***x*:*z*: Specifies tunnelx as the interface for Group z and uses this interface for data forwarding.
- **loopback***x*:*z*: Specifies loopbackx as the interface for Group z and uses this interface for data forwarding.
- **ethernet***x/y.u*:*z*: Specifies ethernetx/y.u as the interface for Group z and uses this interface for data forwarding.
- **redundant***x.y*:*z*: Specifies redundantx.y as the interface for Group z and uses this interface for data forwarding.
- **aggregate***x.y*:*z*: Specifies aggregatex.y as the interface for Group z and uses this interface for data forwarding.

To cancel the specified interface, in the global configuration mode, use the following command:

no interface {**ethernet***x/y:z* | **redundant***x:z* | **aggregate***x:z* | **tunnel***x:z* | **loopback***x:z* | **ethernet***x/y.u:z* | **redundant***x.y:z* | **aggregate***x.y:z*}

Note: In the current version, you can only specify the value of z as 1.

Configuring the Next-hop IP Address of the Interface

In the HA Peer mode network environment, to avoid the situation that fails to find the routes when synchronizing data with the peer device, you can configure the next-hop IP address of the interface, which ensures the successful creation of the sessions. To specify the next-hop IP address of the interface, use the following command in the interface configuration mode:

direct-send default-nexthop *A.B.C.D* [**local**]

- *A.B.C.D* – Specifies the next-hop IP address of the interface.
- **local** – If you enter this parameter, the system will not synchronize this configuration with the backup device. Without entering this parameter, this configuration will not be synchronized with the backup device.

In the interface configuration mode, use the following command to cannel the above configurations:

no direct-send default-nexthop [*A.B.C.D*] [**local**]

Configuring SNAT Port Distribution

HA supports the SNAT port distribution function. The function is that when you configure the same SNAT address pools for two HA devices, the system will averagely distribute the SNAT port resources according to the values of HA Node. If you disable this function, the SNAT address pool configured for each HA device must differ and each device will occupy the entire port resources. The SNAT port distribution function can only take effect I the HA Peer mode.

To enable the SNAT port distribution function, use the following command in the global configuration mode:

split-port-pool by ha-node

In the global configuration mode, use the following command to disable this function:

no split-port-pool by ha-node

Configuring an HA Link

The synchronization between the master and backup device and the Hello packets are transmitted over the HA link. There are two types of HA links, control Link and data

Link. The control link is used to synchronize all data between two devices and the data link is used to synchronize the data packet information such as session information. According to your requirements, you can choose whether to configure the data link. If you configure the data ink, the Hello packets will be transmitted over the data link and the information of data synchronization and others will be transmitted over the control link. Without the data link configured, all synchronization information will be transmitted over the control link.

You need to specify the HA link interface first, and then specify the IP address of the interface.

Specifying an HA Link Interface

You can specify up to two HA control link interfaces. The later configured HA link interface serves as the backup interface for the first configured one. When the first interface disconnects, the later configured interface will take over the task of transmitting HA packets. To specify an HA control link interface, in the global configuration mode, use the following command:

ha link interface *interface-name*

- *interface-name* – Specifies the name of the interface.

To specify an HA data link interface, in the global configuration mode, use the following command:

ha link data interface *interface-name*

- *interface-name* – Specifies the name of the interface.
- **data** – Specify the type of the HA link as the data link. After specifying this data link, the session information will be synchronized over this data link. You can configure the physical interface or aggregate interface as the interface of the data link and you can specify at most 1 HA data link interface.

To delete the specified HA link interface, in the global configuration mode, use the following command:

no ha link interface *interface-name*

no ha link data interface *interface-name*

Specifying the IP Address of HA link Interface

After specifying the HA link interface, to configure the IP address of the HA link interface, in the global configuration mode, use the following command:

ha link ip *ip-address netmask*

- *ip-address netmask* - Specifies the IP addresses and the netmask of the HA link interface.

To cancel the specified IP address, in the global configuration mode, use the following command:

no ha link ip *ip-address netmask*

Specifying the MAC Address of HA Link Interface on ClouldEdge

The MAC address of HA link interface refers to the source MAC address for the HA device to send heartbeats (Hello packets) to other devices in HA group. By default, system uses the default MAC address to send Hello packets. Users can specify the MAC address of control link interface or customize a MAC address as the MAC address of HA link interface. To specify the MAC address of HA link interface, in the global configuration mode, use the following command:

ha link mac { 1st-interface-mac | *mac-address*}

- **1st-interface-mac** – Specifies the MAC address of control link interface as the MAC address of HA link interface. When there is more than one configured control link interfaces, system will use the MAC address of the first control link interface as the MAC address of HA link interface.
- *mac-address* - Specifies a customized MAC address as the MAC address of HA link interface.

In the global configuration mode, use the following command to restore the default MAC address of HA link interface.

no ha link mac

Enable the Real MAC Address of Interface On CloudEdge

This function is only supports for the interface of CloudEdge, except HA link interface and the interface configured with the Local property. By default, the interface forwards traffic with the virtual MAC address provided by system. After configuring the function, each interface will use its real MAC address for conmunication. To enable the real MAC address of interface, in the global configuration mode, use the following command:

no ha virtual-mac enable

To restore to the default virtual MAC address, in the global configuration mode, use the following command:

ha virtual-mac enable

Notes: When device is added to HA cluster and HA function take effective, you can not change the MAC address of interface.If you want to change it, execute the command **no ha cluster** firstly.

Configuring Route Filters Based on the Route Access-list

OSFP uses the route access-list to filter the introduced route. To configure the route filter function based on the route access-list, use the following command in the OSPF routing configuration mode:

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

- *access-list-name* – Specifies name of the route access-list. For more information about route access-list, see **Configuring a Route Access-list**.
- **in** – Use **in** to filter the introduced routes.
- *interface-name* – Specifies name of the interface. After specifying this interface, the system will filter the OSPF route from the specified interface. If the interface name is not specified, the system will filter all OSPF routes.

Use the following command to cancel the above configurations:

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

Configuring an HA Cluster

After configuring the HA group, HA group interface and HA link interface, you need to add the device to the HA cluster to make the HA function take effective. If there are more than one pair of HA devices in the network, you need to configure different HA cluster IDs, otherwise the MAC addresses may conflict. To configure an HA cluster, in the global configuration mode, use the following command:

ha cluster *cluster-id* [[peer-mode node *ID* [symmetric-routing]]| node *ID*]

- *cluster-id* - Specifies the HA cluster ID. The value varies depending on the HA virtual MAC prefix.
- peer-mode node *ID* – Configures the HA Peer mode and specifies the role of this device in the HA cluster. The range is 0 to 1. By default, the group 0 in the device whose HA Node ID is 0 will be active and the group 0 in the device whose HA Node ID is will be in the disabled status.
- symmetric-routing – If you enter this parameter, the device will work in the symmetrical routing environment.
- node *ID* – Specifies the HA Node value for the device. The values for two devices must be different. The range is 0 to 1. If you do not specify this value, the devices will obtain the Node ID value by automatic negotiation.

To disable the specified HA cluster, in the global configuration mode, use the following command:

no ha cluster

Configuring HA VMAC Prefix

If more than 8 HA clusters in a network segment need to be configured, you can configure the prefix of the HA virtual base MAC address, i.e., the HA virtual MAC prefix, in order to avoid the HA virtual MAC address duplication. When the length of prefix is set to 7 hexadecimal, you can deploy up to 128 HA clusters on the same network segment. When the length of prefix is set to 8 or by default, you can deploy up to 8 HA clusters on the same network segment. After the configuration is complete, the system will prompt the HA virtual MAC range to be generated and the

configuration will take effect after reboot. To configure the HA virtual MAC prefix, in the global configuration mode, use the following command:

ha virtual-mac-prefix *prefix-addr*

- *prefix-addr* - Specifies the prefix of the HA base MAC in hexadecimal format. Its length can only be configured as seven or eight. By default, the HA virtual MAC prefix is 0x001C54FF. It should be noted that 0x00000000, 0x0000000, 0xFFFFFFFF, 0xFFFFFFF or multicast addresses (i.e., the second hexadecimal number is odd) are invalid.

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

no ha virtual-mac-prefix

Note: With the HA function enabled, if you want to modify the HA virtual MAC prefix, you may need to disable the HA function first.

Viewing HA VMAC Prefix

To view the current HA virtual MAC prefix and the maximum number of HA clusters that can be configured, use the following command in any mode:

show ha cluster

Configuring a Management IP

To manage the HA backup device, you need to configure a management IP for the backup device. To configure a management IP address, in the interface configuration mode, use the following command:

manage ip *ip-address*

- *ip-address* - Specifies the management IP address.

Manually Synchronizing HA Information

In some exceptional circumstances, the master and backup configurations may not be synchronized. In such a case you need to manually synchronize the configuration information of the master and backup device. To determine if you need to manually synchronize the HA information, take the following steps:

1. View the relevant configuration information of both master and backup device by using the command **show**.
2. According to the displayed configuration information, determine whether you need to manually synchronize the HA information:
   - If the configuration information is consistent, then you don't need to synchronize manually;

- If the configuration information is inconsistent, you need to run the corresponding commands to manually synchronize the configuration (for more information about the relevant commands, see table below).

Notes:

- You do not need to manually synchronize the inconsistent local configuration information, such as the interface timeout information.
- For dynamic information, such as session information, you do not need to synchronize the information manually unless the dynamic information is not synchronized properly.

Table 5: **Manual Synchronization Commands**

HA synchronization information	Show command	Manual synchronization command
Configuration information	**show configuration**	**exec ha sync configuration**
File information	**show file**	**exec ha sync file** *file-name*
ARP table	**show arp**	**exec ha sync rdo arp**
DNS configuration information	**show ip hosts**	**exec ha sync rdo dns**
DNS rewrite rule information	**show dns-rewrite-rule**	**exec ha sync rdo dns-rewrite**
DHCP configuration information	**show dhcp**	**exec ha sync rdo dhcp**
MAC address table	**show mac**	**exec ha sync rdo mac**
PKI configuration information	**show pki key**	**exec ha sync rdo pki**
	show pki trust-domain	
Session information	**show session**	**exec ha sync rdo session**
IPsecIPSec VPN information	**show ipsec sa**	**exec ha sync rdo vpn**
	show isakmp sa	
SCVPN information	**show scvpn client test**	**exec ha sync rdo scvpn**
	show scvpn host-check-profile	
	show scvpn pool	
	show scvpn user-host-binding	
	show scvpn session	
	show auth-user scvpn	
L2TP information	**show l2tp tunnel**	**exec ha sync rdo l2tp**
	show l2tp pool	
	show l2tp client {**tunnel-name** *name* [**user** *user-name*]| **tunnel-id** *ID*}	
	show auth-user l2tp [**interface** *interface-name*	**vrouter**	

	vrouter-name} | **slot** *slot-no*]	
WebAuth information	**show auth-user webauth**	**exec ha sync rdo webauth**
NTP information	**show ntp**	**exec ha sync rdo ntp**
SCVPN information	**show scvpn**	**exec ha sync rdo scvpn**
Route information	**show ip route**	**exec ha sync rdo route**
IGMP information	**show ha sync statistic igmp**	**exec ha sync rdo igmp**
	show ha sync state igmp	

Manually Switching Main and Backup Device Status of HA

To switch main and backup device status of HA manually, in any mode, use the following command:

```
exec ha master switch-over
```

Note:

- This command is only supported on the main device of HA.
- As the switching operation executes, this device is executing batch synchronization or some Hillstone devices (SG - 6000 - X6150, SG - 6000 - X6180, SG - 6000 - X7180) are executing batch synchronization of SCM, which will result in failed switching of HA main and backup device status.

Backing up Statistical Data

In HA cluster, when one device fails, the other will take over the work of the failed device and also run its original work simultaneously to ensure uninterrupted work. In order to keep statistical data(such as monitor and log data) consistent after device switching, you can configure statistical data backup. After this feature is enabled, the system will send statistical data to both devices in the HA state, so that all data and configurations of two devices can be backed up. Due to the large amount of data to back up, we recommend that you configure Ten-GigabitEthernet interface (interface expansion module which owns Ten-GigabitEthernet interface is needed) or aggregate interface as ha link interface, otherwise it may cause inconsistent data. By default, this feature is disabled.

To back up statistical data to the other HA member, in the global configuration mode, use the following command:

```
ha analysis-data multicast
```

In the global configuration mode, use the following command to disable backup:

```
no ha analysis-data multicast
```

Note: Currently, you can only back up statistical data via CLI, not WebUI.

Viewing the Backup Status of Statistical Data

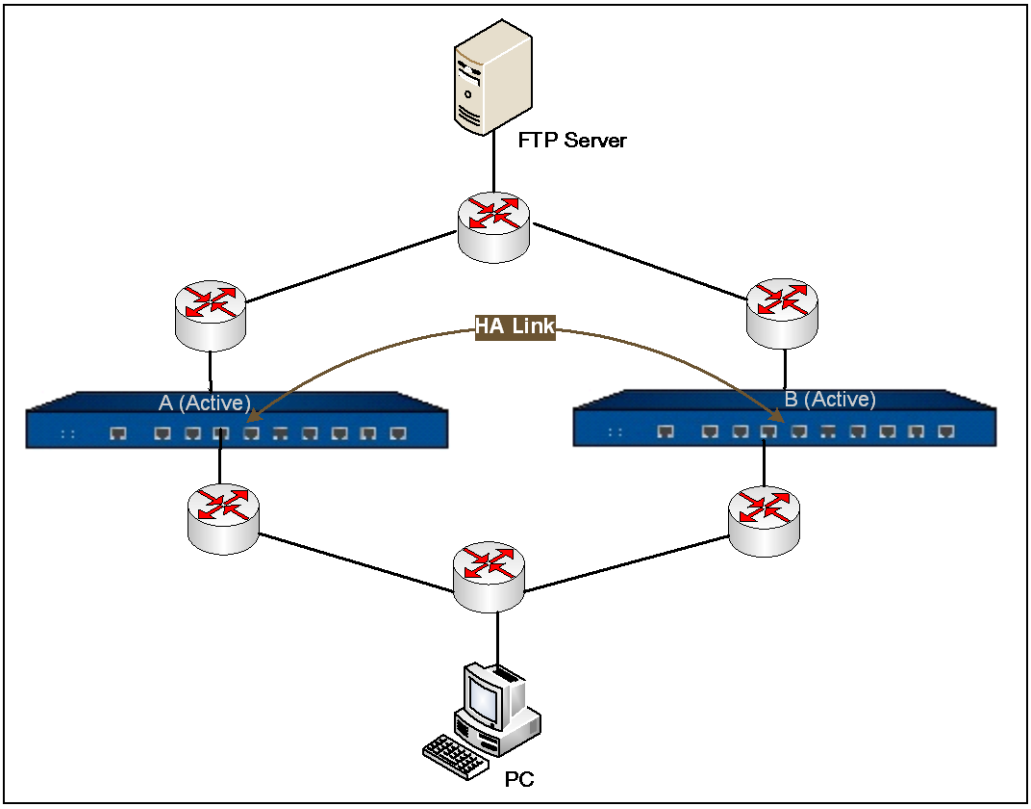
You can view the backup status of statistical data as needed, including whether statistical data backup is enabled or not, device online status, device priority, etc. To view the backup status of statistical data, in any mode, use the following command:

```
show ha apm state
```

Configuring HA Traffic

For the HA devices that are deployed in asymmetric routing environment (i.e., inbound and outbound traffic may take different routes), you can enable HA traffic to assure the inbound and outbound packets of a session are processed on the same device, thus avoiding session failure. Figure below illustrates a typical HA traffic application topology.

Figure 4: Typical HA Traffic Application Topology



As shown in the figure above, the left route is from PC to the FTP server by the way of Device A. the righ route is the same start and ending by the way of Device B. the metric value of these two routes are different from each other, making the network an asymmetric route,In addition, the FTP requests from PC are sent to the FTP server via Device A. In order to assure the response packets from the FTP server are returned to PC via Device A, you need to enable HA traffic on both Device A and Device B.

To enable HA traffic, use the following two steps:

1. Configure the two HA device to HA Peer mode;

2. Enable HA traffic.

Enabling HA Traffic

HA traffic is disabled by default. To enable or disable the function, in the global configuration mode, use the following commands:

- To enable: **ha traffic enable**
- To disable: **no ha traffic enable**

Note: After enabling the HA traffic function, the traffic between devices increase. Hillstone recommends you first configure the interface of the data link.

Configuring HA Traffic Delay

When processing outbound packets, the device with HA traffic enabled will synchronize packet-related information with the pairing device. If the peer device responses (i.e., inbound packet) before the synchronization is completed, the sessions will not be matched and the response to the request packet will be dropped. To solve this problem, in the transparent mode, you can configure HA traffic delay. The device will wait for the specified delay time so that the synchronization will be completed, and then process inbound packets.

To configure HA traffic delay, in the global configuration mode, use the following commands:

ha traffic delay *num*

- *num* - Specifies the delay time. The value range is 1 to 50 ms. The default value is 3.

To cancel the above configurations, use the following command in the global configuration mode:

no ha traffic delay

Configuring First Packet Forwarding

In the routing mode, you can configure the first packet forwarding function to ensure that when processing outbound packets, the device will synchronize packet-related information with the pairing device. To configure the first packet forwarding function, use the following command in the global configuration mode:

ha traffic first-packet [**max-size** *num*]

- **max-size** *num* – Specifies the size of the first packet. The unit is byte. The value is 64 to 1024. Without configuring this parameter, the default value is 124.

To cancel the above configurations, use the following command in the global configuration mode:

no ha traffic first-packet

Enabling/Disabling Automatic HA Session Synchronization

By default the system will synchronize sessions between HA devices automatically. Session synchronization will generate some traffic, and will possibly impact device performance when the device is overloaded. You can enable or disable automatic HA session synchronization according to the device workload to assure stability.

To enable or disable automatic HA session synchronization, in the global configuration mode, use the following command:

- Enable: **ha sync rdo session**
- Disable: **no ha sync rdo session**

Viewing HA Configuration

To view the HA configuration information, use the following commands:

- Show the HA cluster configuration information: **show ha cluster**
- Show the HA group configuration information: **show ha group** {**config** | *group-id*}
- Show the HA link status: **show ha link status**
- Show the HA synchronization state: **show ha sync state** {**pki** | **dns** | **dhcp** | **vpn** | **ntp** | **config** | **flow** | **scvpn** | **l2tp** | **route| igmp** }
- Show the HA traffic status: **show ha traffic**
- Show the HA synchronization statistics: **show ha sync statistic** {**pki** | **dns** | **dhcp** | **vpn** | **ntp** | **config** | **scvpn** | **route| igmp** }
- Show the HA protocol statistics: **show ha protocol statiscitc**
- Show the synchronized or unsynchronized HA session information: **show session** {**sync** | **unsync**}
- Show the HA statistics: **show ha flow [**[**slot** *slot-number*]| [**cpu** *cpu-number*]**] statistics**

Twin-mode HA

Twin-mode HA Introduction

Currently , data centers providing important data information and office services in many industries. In order to improve the reliability, companies generally build two or more data centers, and the extended mode of L2 (DCI: Data Center Interconnection) is used for inter-connections between two data centers. Two data centers running independently, providing business services and mutual backup, constitute a redundant data center.

The Hillstone devices are deployed in the data center under the routing mode, used to check traffic and isolated by policy across different regions. Because of the DCI, the asymmetric L3 traffic that across the data center and different regions may occurs (i.e., inbound and outbound traffic may take different routes), the policy isolation will not take effect. To resolve this problem, system provides the Twin-mode HA function. This function will optimizes the traffic forwarding, ensuring the business continuity and efficiency of redundant data centers.

Notes:

- This function only supports some devices (X series and E series).
- Currently, this function only support Active-Active (A/A) mode.
- This version does not support IPv6 function.
- You must enable HA function before enable the Twin-mode HA function, and the devices must in Active-Passive (A/P) mode.
- In twin-mode A/P mode or twin-mode A/A mode, you must configure the same HA cluster ID for the data center.

Currently, The system supports functions for Twin-mode HA listed in Table below. For more details and configuration, see relevant section.

Table 6: **Supported functions for Twin-mode HA**

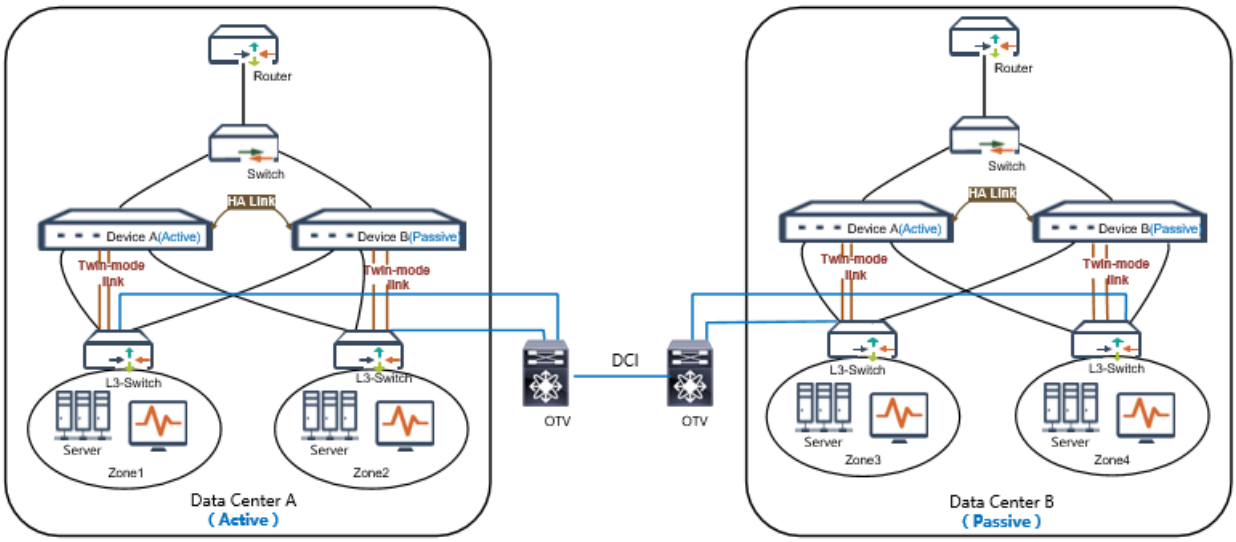
Function		
Application Layer Gateway (ALG)	Interface	High Availablity (HA)
Application Layer Identification and Control	System Management	Virtual System (VSYS)
Network Address Translation (NAT)	Report	Firewall
Attack Defense	Monitor	SNMP
Routing	Log	

Typical Twin-mode HA Deployment Scenarios

There are three kinds of typical L2TP twin-mode deployment scenarios:

- Active-Passive（A/P）deployment scenarios

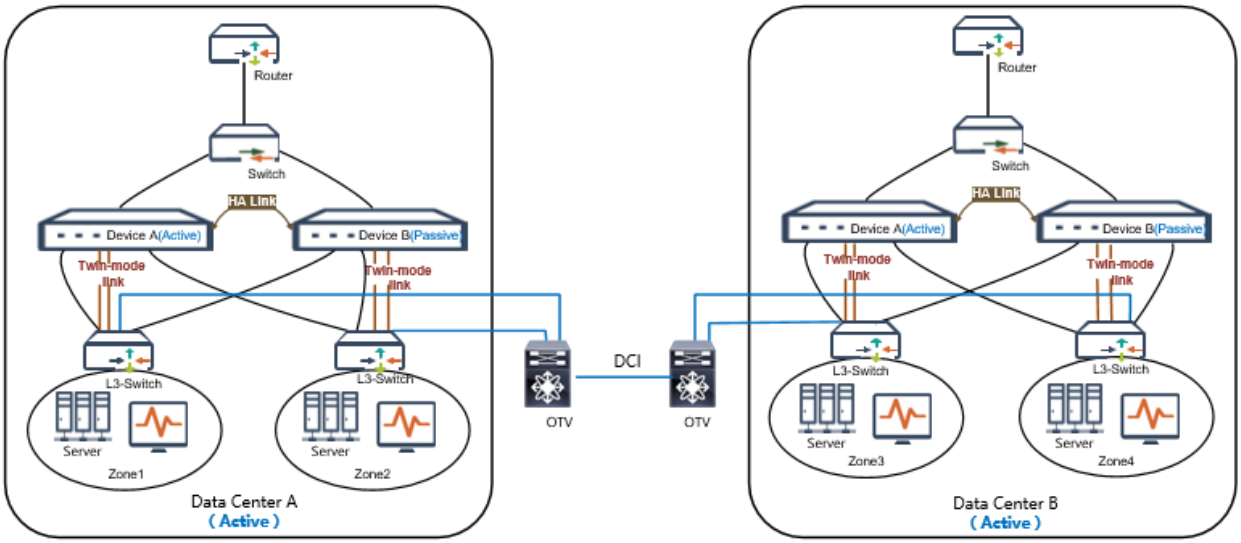
Figure 5: Twin-mode HA A/P mode deployment scenarios



As shown in the figure above, configure two data center to form an HA group, with one data center acting as a master device and the other acting as its backup device. When the master data center fails, the backup data center will be promoted to master and take over its work to forward packets. The Hillstone devices are deployed on each data center (you can use 3 straight series deployment or deploy the device in the gateway location), and make up the HA A/P mode.

- Active-Active（A/A）deployment scenarios

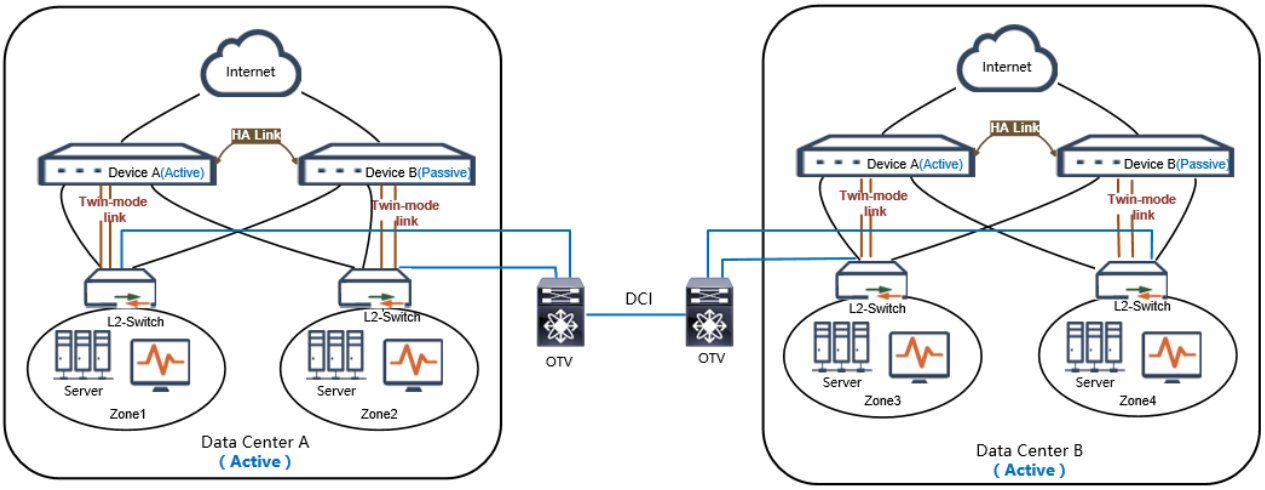
Figure 6 Twin-mode HA A/A mode deployment scenarios



As shown in the figure above, the two data centers perform their own tasks simultaneously, and monitor the operation status of each other. When one data center fails, the other will take over the work of the failure device and also run its own tasks simultaneously to ensure uninterrupted work. The Hillstone devices are deployed on each data center and make up the HA A/P mode. Through Twin-mode HA function, the problem of asymmetric L3 traffic that across the data center and different regions is solved.

- Gateway deployment scenarios: This deployment scenarios is a special Active-Active（A/A）deployment scenarios.

Figure 7 Gateway deployment scenarios



As shown in the figure above, the Hillstone devices are deployed in the data center as a gateway and make up the HA A/P mode. The two data centers consist of twin-mode A/A mode, and backup each other. Since the extended device of L2 filters the same IP address and MAC address of the data center gateway, this problem is solved by deploying the gateway mode and configuring the twin-mode HA gateway function.

Twin-mode HA Synchronization

To ensure the backup device can take over the work of the master data center when it fails, the master data center will synchronize its information with the backup data center. In different deployment modes, the system supports different synchronous mode and synchronous information types.

In twin-mode HA A/P mode, the types of information that can be synchronized includes:

- Configuration information
- Session information
- ARP tabel
- Pinhole
- Track information
- Route information
- NTP information
- Signature file

In twin-mode HA A/A mode, the system supports two synchronous mode: Part synchronization and No synchronization. About configuration steps, refer to Specifying the deployment mode and synchronization mode for Twin-mode HA.
The types of information that can be synchronized includes:

- Configuration information (Policy/Service Book/Address Book/IPS/AV/URL/Schedule)
- Session information
- Pinhole
- Signature file

Configuring Twin-mode HA

The Twin-mode HA need to be configured in the Twin-mode configuration mode. To enter the Twin-mode configuration mode, in the global configuration mode, use the following command:

twin-mode

After executing the command, the system will enter the Twin-mode configuration mode.

In the Twin-mode configuration mode, you can perform the following configurations:

- Specifying the deployment mode and synchronization mode for Twin-mode HA
- Specifying the Node
- Specifying the Priority
- Configuring the Preempt Mode
- Specifying the Hello Interval
- Specifying the Hello Threshold
- Configuring Twin-mode HA Link
- Enabling/Disabling Twin-mode HA

Note:

- Before configuring the twin-modefunction, you should install the Twin-mode License first.
-

Specifying the deployment mode and synchronization mode for Twin-mode HA

Currently, supports two deployment modes for Twin-mode HA: A/A mode and A/P mode. The system supports two synchronization mode: Part synchronization and No synchronization. In the Twin-mode configuration mode, use the following command:

mode {active-active [no-sync | part-sync] | active-passive }

- **active-active [no-sync | part-sync]** – Specifies the deployment mode is A/A mode.
- **no-sync** – Specifies the synchronization mode is no synchronization.

- **part-sync** – Specifies the synchronization mode is part synchronization mode. About specific synchronization information content, refer to Twin-mode HA Synchronization
- **active-passive** –Specifies the deployment mode is A/P mode.

To cancel the specified deployment mode, in the Twin-mode configuration mode, use the following command:

no mode

Specifying the Node

To distinguish the data center, you can use the value of Node to mark the data center. To specify the Node, in the global configuration mode, use the following command:

node node-*ID*

- node-*ID* – Specifies the Node. The range is 0 to 1.

To cancel the specified Node, in the Twin-mode configuration mode, use the following command:

no node

Notes:

- You must specify the different Node for each data center.
- User needs to restart the device to make it take effect after modifying the Node.

Specifying the Priority

The priority specified by the command is for used for HA selection. The device with higher priority (the smaller number) will be selected as the master device of data center. To specify the priority, in the Twin-mode configuration mode, use the following command:

priority *number*

- *number* - Specifies the priority. The value range is the 1 to 254. The default value is 100.

To restore to the default priority, in the Twin-mode configuration mode, use the following command:

no priority

Note: When the priorities are identical, the device with Node 0 will be priorized.

Configuring the Preempt Mode

When the preempt mode is enabled, once the backup device find its own priority is higher than the master device, it will upgrade itself to the master device and the original master device will become the backup device. When the preempt mode is disabled, even if the device's priority is higher than the master device, it will not take over the master device unless the master device fails. When configuring the preempt mode, you can also set the delay time to make the backup device take over the master device after the specified delay time. To configure the preempt mode, in the Twin-mode configuration mode, use the following command:

preempt [*delay-time*]

- *delay-time* - Specifies the delay time. The value range is 1 to 600 seconds. The default value is 3.

To cancel the preempt mode, in the Twin-mode configuration mode, use the following command:

no preempt

Specifying the Hello Interval

Hello interval refers to the interval for the HA device to send heartbeats (Hello packets) to other devices in the HA group. The Hello interval in the same HA group must be identical. To specify the Hello interval, in the Twin-mode configuration mode, use the following command:

hello interval *time-interval*

- *time-interval* - Specifies the interval for sending heartbeats. The value range is 1 to 100 seconds. The default value is 1s.

To restore to the default Hello interval, in the Twin-mode configuration mode, use the following command:

no hello interval

Specifying the Hello Threshold

If the device does not receive the specified number of Hello packets from the other device, it will judge that the other device’s heartbeat fails. To specify the Hello threshold, in the Twin-mode configuration mode, use the following command:

hello threshold *value*

- *value* - Specifies the Hello threshold value. The value range is 5 to 255. The default value is 10.

To restore to the default Hello threshold, in the Twin-mode configuration mode, use the following command:

no hello threshold

Configuring Twin-mode HA Link

There are two types of Twin-mode HA links, control Link and data Link. Currently, system only support to specify the physical interfaces and aggregation interfaces as a Twin-mode HA link interface.

You need to specify the Twin-mode HA link interface first, and then specify the IP address and peer IP address of the interface.

Specifying a Twin-mode HA Link Interface

To specify a Twin-mode HA link interface, in the Twin-mode configuration mode, use the following command:

link { **control** | **data** } **interface** *interface-name*

- **control** | **data** – Specifies the Twin-mode HA link type.
- *interface-name* – Specifies the name of the interface.

To delete the specified Twin-mode HA link interface, in the Twin-mode configuration mode, use the following command:

no link { **control** | **data** } **interface** *interface-name*

Notes:

- Data link interface does not allow specifying on the X series device panel interface ethernet0/0- ethernet0/3.
- Control Link and Data Link can specify up to two interfaces.
- When asymmetric data traffic is larger, it is recommended that users use two data links or using a aggregate interface to ensure sufficient bandwidth for transmitting data traffic.

Specifying the IP Address of Twin-mode HA link Interface

After specifying the Twin-mode HA link interface, to configure the IP address of the Twin-mode HA link interface, in the Twin-mode configuration mode, use the following command:

link ip *ip-address netmask*

- *ip-address netmask* - Specifies the IP addresses and the netmask of the Twin-mode HA link interface.

To cancel the specified IP address, in the Twin-mode configuration mode, use the following command:

no link ip *ip-address netmask*

Specifying the Peer IP Address

To configure the peer IP address, in the Twin-mode configuration mode, use the following command:

link peer-ip *ip-address*

- *ip-address* - Specifies the peer IP addresses.

To cancel the specified peer IP address, in the Twin-mode configuration mode, use the following command:

no link peer-ip

Enabling/Disabling Twin-mode HA

By default the Twin-mode HA function is disabled. To enable or disable Twin-mode HA, in the Twin-mode configuration mode, use the following command:

- Enable: **enable**
- Disable: **no enable**

Specifying the Forwarding Mode of Asymmetric Traffic

For the asymmetric traffic, Twin-mode HA provides two forwarding mode: tunnel mode and layer 2 tunnel mode.

- Tunnel Mode: The encapsulated package will be sent to the peer data center through Data Link, after the traffic was de-encapsulated , the peer data center will transfer it. By default, the forwarding mode is tunnel mode.
- Layer 2 Tunnel Mode: The MAC address of the packet is modified as the virtual MAC (VMAC) address which corresponds to its interface of peer data center, the traffic is forwarded through layer 2 tunnel. With this mode, the user needs to enable the layer 2 tunnel forwarding mode at all business interfaces of the device.

To enable the layer 2 tunnel forwarding mode, in the interface configuration mode, , use the following command:

twin-mode-l2-tunnel-enable

To restore to the default forwarding mode, in the interface configuration mode, use the following command:

no twin-mode-l2-tunnel-enable

Note: The forwarding mode must be specified. The two modes cannot be mixed, otherwise the function is not effective.

Configuring Twin-mode HA Gateway

In the gateway deployment scenarios, because the extended device of L2 filters the same IP address and MAC address of the data center gateway, the asymmetric traffic blocked. In order to avoid this problem, you needs to enable the twin-mode gateway function, and configure gateway interface IP address for sending the ARP request message, the system will take this IP address as the source of IP, Twin-mode virtual MAC (VMAC) as the source MAC address to send the ARP request message, and

forward the data traffic with Twin-mode virtual MAC (VMAC) address as the source address, so as to solve the problem of asymmetric traffic.

To enable the twin-mode gateway function and configure gateway interface IP address for sending the ARP request message, in the interface configuration mode, use the following command:

twin-mode-gateway sender-ip *ip-address*

- *ip-address* – Specifies the gateway interface IP address for sending the ARP request message. This IP address must be in the same network segment as the IP address of the gateway interface.

To disable this function and delete the specified IP address, in the interface configuration mode, use the following command:

no twin-mode-gateway sender-ip *ip-address*

Note: The gateway interface IP for sending ARP request messages of both data centers must be different.

Configuring the Switching Mode of Twin-mode HA Session State

In the twin-mode HA A/A mode, system supports two switching modes of twin-mode HA session state, including unidirectional switching and bidirectional switching.

- Unidirectional switching: When a link of access extranet server fails in the data center, the system will quickly switch the inactive twin-mode HA session state to the active state, and ensure that the traffic will not be interrupted.
- Bidirectional switching: When you need to modify the traffic forwarding path of data center, you can use this switching mode, the system will quickly switch the inactive twin-mode HA session state to the active state, so as to optimize the traffic paths.

To configure the switching mode of twin-mode HA session state, in the Flow configuration mode, use the following command:

twin-mode-sess-owner-change {**follow-init-direction**|**follow-two-direction**}

- **follow-init-direction** – Unidirectional switching, when the traffic hits the upstream traffic of the inactive session, the system will switch the session state.
- **follow-two-direction** – Bidirectional switching, when the traffic hits both the upstream and downstream traffic of the inactive session, the system will switch the session state.

To disable this function, in the Flow configuration mode, use the following command **no twin-mode-sess-owner-change**.

Note: To enter the flow configuration mode, in the global configuration mode, use the command **flow**.

Manually Synchronizing Twin-mode HA Configuration Information

In some exceptional circumstances, the master and backup configurations of data center may not be synchronized. In such a case you need to manually synchronize the twin-mode HA configuration information of the master and backup data center. To determine if you need to manually synchronize the twin-mode HA information, take the following steps:

1. View the relevant configuration information of both master and backup datacenter by using the command **show twin-mode configuration difference** on the master device.
2. According to the displayed configuration information, determine whether you need to manually synchronize the twin-mode HA information:
   - If the configuration information is consistent, then you don't need to synchronize manually;
   - If the configuration information is inconsistent, you need to run the command **exec twin-mode sync configuration** to manually synchronize the configuration.

Note: The command **exec twin-mode sync configuration** can only be executed on the master HA device of the master data center.

Viewing/Clearing the Transfer Packet Count of Twin-mode HA

To view the transfer packet count of Twin-mode HA, in any mode, use the following command:

show twin-mode-counter

To clear the transfer packet count of Twin-mode HA, in any mode, use the following command:

clear twin-mode-counter

Viewing Twin-mode HA Configuration

To view the Twin-mode HA configuration information, use the following commands:

- Show the Twin-mode HA configuration information: **show twin-mode configuration**
- Show the Twin-mode HA link information: **show twin-mode link**

- Show the Twin-mode HA peer status: **`show twin-mode peer`**
- Show the Twin-mode HA status: **`show twin-mode status`**

Examples of Configuring HA

This section describes three HA configuration examples:

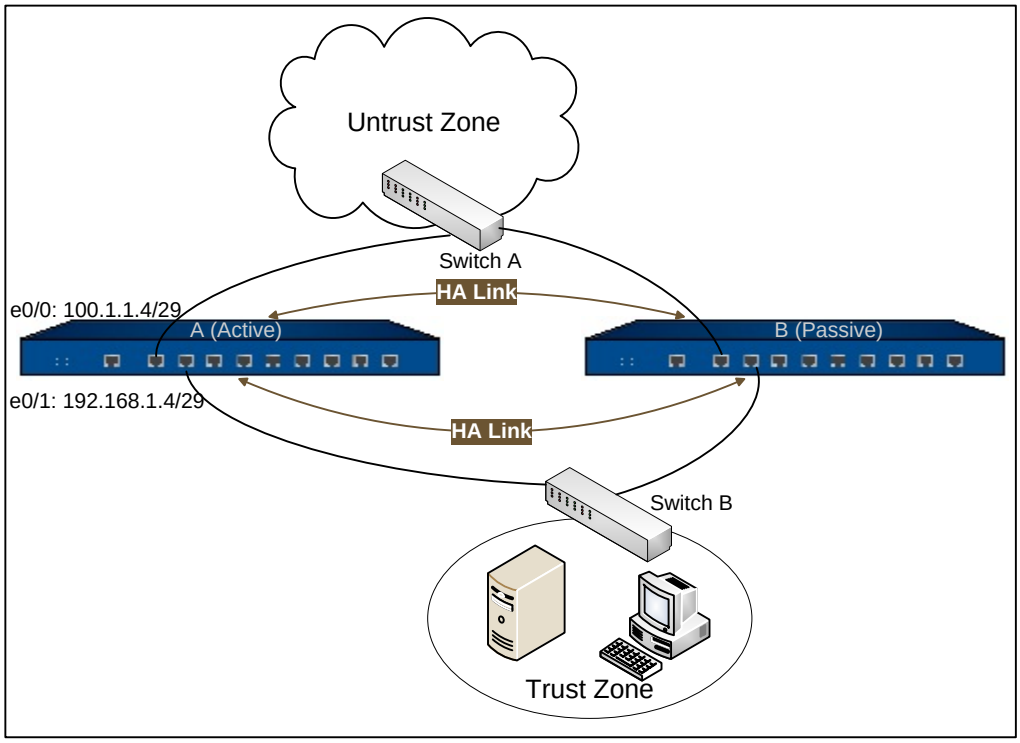
- Example 1: configuration example of HA in A/P mode
- Example 2: configuration example of HA in A/A mode
- Example 3: configuration example of HA Peer mode and HA traffic
- Example 4: configuration example of specific scenarios of HA A/A mode

Example 1: Example of HA in A/P Mode

Requirement

To goal is use two Hillstone devices, which are of the same hardware platform, firmware version, and license, to a form an HA cluster in Active-Passive mode. In addition, the two devices are using the same interface to connect to the network. The network topology is shown below:

Figure 8: HA A/P Network Topology



Configuration Steps

Step 1: Configure the interfaces and policy rules on Device A:

Device A

```
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone untrust
hostname(config-if-eth0/0)# ip address 100.1.1.4/29
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 192.168.1.4/29
hostname(config-if-eth0/1)# 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 any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 2: Configure a track object which is used for tracking the status of interface of the master device, and if the interface ethernet0/0 fails, the device will implement failover:

```
hostname(config)# track trackobj1
hostname(config-trackip)# interface ethernet0/0 weight 255
hostname(config-trackip)# exit
hostname(config)#
```

Step 3: Configure an HA group:

Device A

```
hostname(config)# ha group 0
hostname(config-ha-group)# priority 50
hostname(config-ha-group)# monitor track trackobj1
hostname(config-ha-group)# exit
hostname(config)#
```

Device B

```
hostname(config)# ha group 0
hostname(config-ha-group)# priority 100
hostname(config-ha-group)# exit
hostname(config)#
```

Step 4: Configure HA link interfaces and enable the HA function:

Device A

```
hostname(config)# ha link interface ethernet0/2
```

```
hostname(config)# ha link interface ethernet0/3
hostname(config)# ha link ip 1.1.1.1/24
hostname(config)#
```

Device B

```
hostname(config)# ha link interface ethernet0/2
hostname(config)# ha link interface ethernet0/3
hostname(config)# ha link ip 1.1.1.2/24
hostname(config)#
```

Step 5: Configure an HA cluster to enable HA:

Device A

```
hostname(config)# ha cluster 1
```

Device B

```
hostname(config)# ha cluster 1
```

Step 6: Configure the management IPs of the master device and backup device after synchronization:

Device A

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# manage ip 192.168.1.253
```

Device B

```
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone trust
hostname(config-if-eth0/1)# manage ip 192.168.1.254
```

Step 7: Configure a track object on Device B, and if the interface ethernet0/0 on Device B fails, the device will implement failover:

Device B

```
hostname(config)# ha group 0
hostname(config-ha-group)# monitor track trackobj1
hostname(config-ha-group)# exit
hostname(config)#
```

After the above configuration, the system will select Device A as the master device for forwarding traffic. Device B acts as the backup device. Device A will synchronize its configuration information and status to Device B. When Device A fails and cannot forward traffic, or the ethernet0/0 of Device A is disconnected, Device B will switch to the master device without interrupting user's communication, and continue to forward the traffic.

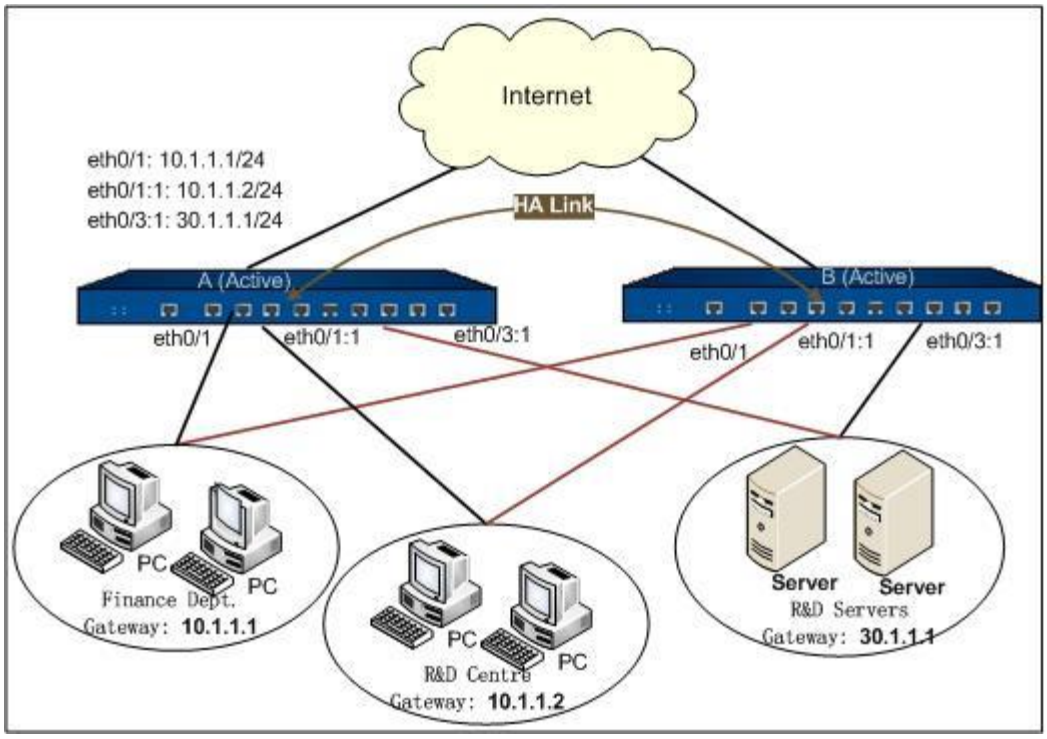
Example 2: Example of HA in A/A Mode

Requirement

This section describes a typical redundant HA Active-Active mode configuration example. Before configuring, make sure the two Hillstone devices constructing the HA structure are using the same hardware platform, firmware version, and license, been installed with anti-virus licenses, and the two devices are using the same interface to connect to the network.

After completing the configuration, both of the two devices enable the HA function. Device A is selected as the master device of HA group0, and synchronizes information to Device B. And Device B will preempt to be the master device of HA group1. Under normal conditions, Device A and Device B operate independently, Device A forwarding the traffic of Finance Department and R&D Center, Device B forwarding the traffic of R&D servers. If one of the two devices fails, the other can take over its work and go on forwarding traffic without interruption. For example, if Device B fails, Device A will forward the traffic of Finance Department, R&D Center and R&D servers. The network topology is shown below:

Figure 9:HA A/A Network Topology



Configuration Steps

Step 1: Configure HA groups:

Device A:

```
hostname(config)# ha group 0
hostname(config-ha-group)# priority 10
hostname(config-ha-group)# arp 15
```

```
hostname(config-ha-group)# preempt 3
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# priority 200
hostname(config-ha-group)# preempt 3
hostname(config-ha-group)# exit
```

Device B:

```
hostname(config)# ha group 0
hostname(config-ha-group)# priority 200
hostname(config-ha-group)# arp 15
hostname(config-ha-group)# preempt 3
hostname(config-ha-group)# arp 15
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# priority 20
hostname(config-ha-group)# arp 15
hostname(config-ha-group)# preempt 3
hostname(config-ha-group)# exit
```

Step 2: Configure the interfaces and zone on Device A:

Device A

```
hostname(config)# zone caiwu
hostname(config-zone-caiwu)# exit
hostname(config)# zone yanfa
hostname(config-zone-yanfa)# exit
hostname(config)# zone internet
hostname(config-zone-intern~)# exit
hostname(config)# zone server
hostname(config-zone-server)# exit
hostname(config)# interface ethernet0/0
hostname(config-if-eth0/0)# zone internet
hostname(config-if-eth0/0)# ip address 192.168.1.1 255.255.255.0
hostname(config-if-eth0/0)# exit
hostname(config)# interface ethernet0/1
hostname(config-if-eth0/1)# zone caiwu
hostname(config-if-eth0/1)# ip address 10.1.1.1 255.255.255.0
hostname(config-if-eth0/1)# exit
hostname(config)# interface ethernet 0/0:1
hostname(config-if-eth0/0:1)# zone internet
hostname(config-if-eth0/0:1)# ip address 192.168.1.2 255.255.255.0
hostname(config-if-eth0/0:1)# exit
hostname(config)# interface ethernet 0/1:1
hostname(config-if-eth0/1:1)# zone yanfa
hostname(config-if-eth0/1:1)# ip address 10.1.1.2 255.255.255.0
hostname(config-if-eth0/1:1)# exit
hostname(config)# interface ethernet 0/3:1
```

```
hostname(config-if-eth0/3:1)# zone server
hostname(config-if-eth0/3:1)# ip address 30.1.1.1 255.255.255.0
hostname(config-if-eth0/3:1)# exit

hostname(config)#
```

Step 3: Configure track objects which are used for tracking the status of interfaces of device A and device B. If the interfaces fail, the device will implement failover:

Device A

```
hostname(config)# track group0
hostname(config-trackip)# interface ethernet0/0
hostname(config-trackip)# exit
hostname(config)# track group1
hostname(config-trackip)# interface ethernet0/1:1
hostname(config-trackip)# interface ethernet0/3:1
hostname(config-trackip)# exithostname(config)# ha group 0
hostname(config-ha-group)# monitor track group0
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# monitor track group1
hostname(config-ha-group)# exit
```

Device B

```
hostname(config)# track group0
hostname(config-trackip)# interface ethernet0/0
hostname(config-trackip)# exit
hostname(config)# track group1
hostname(config-trackip)# interface ethernet0/1:1
hostname(config-trackip)# interface ethernet0/3:1
hostname(config-trackip)# exit
hostname(config)# ha group 0
hostname(config-ha-group)# monitor track group0
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# monitor track group1
hostname(config-ha-group)# exit
```

Step 4: Configure interfaces of HA links:

Device A

```
hostname(config)# ha link interface ethernet0/4

hostname(config)# ha link ip 100.0.0.1 255.255.255.0
```

Device B

```
hostname(config)# ha link interface ethernet0/4

hostname(config)# ha link ip 100.0.0.100 255.255.255.0
```

Step 5: Configure SNAT on Device A:

Device A

```
hostname(config)# address caiwu
```

```
hostname(config-addr)# ip 10.1.1.1/24
hostname(config-addr)# exit
hostname(config)# address yanfa
hostname(config-addr)# ip 10.1.1.2/24
hostname(config-addr)# exit
hostname(config)# nat
hostname(config-nat)# snatrule id 1 from caiwu to any eif ethernet0/0
trans-to eif-ip mode dynamicport
rule ID=1
hostname(config-nat)#  snatrule  id  2  from  yanfa  to  any  eif
ethernet0/0:1 trans-to eif-ip mode dynamicport group 1
rule ID=2 mode dynamicport group 1
hostname(config-nat)# exit

hostname(config)#
```

Step 7: Configure policy rules on Device A:

Device A

```
hostname(config)# policy-global
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone caiwu
hostname(config-policy-rule)# dst-zone internet
hostname(config-policy-rule)# src-addr caiwu
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone yanfa
hostname(config-policy-rule)# dst-zone internet
hostname(config-policy-rule)# src-addr yanfa
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
hostname(config-policy-rule)# src-zone yanfa
hostname(config-policy-rule)# dst-zone server
hostname(config-policy-rule)# src-addr yanfa
hostname(config-policy-rule)# dst-addr server
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
```

Step 8: Configure an HA cluster to enable HA:

Device A

```
hostname(config)# ha cluster 1
```

Device B

```
hostname(config)# ha cluster 1
```

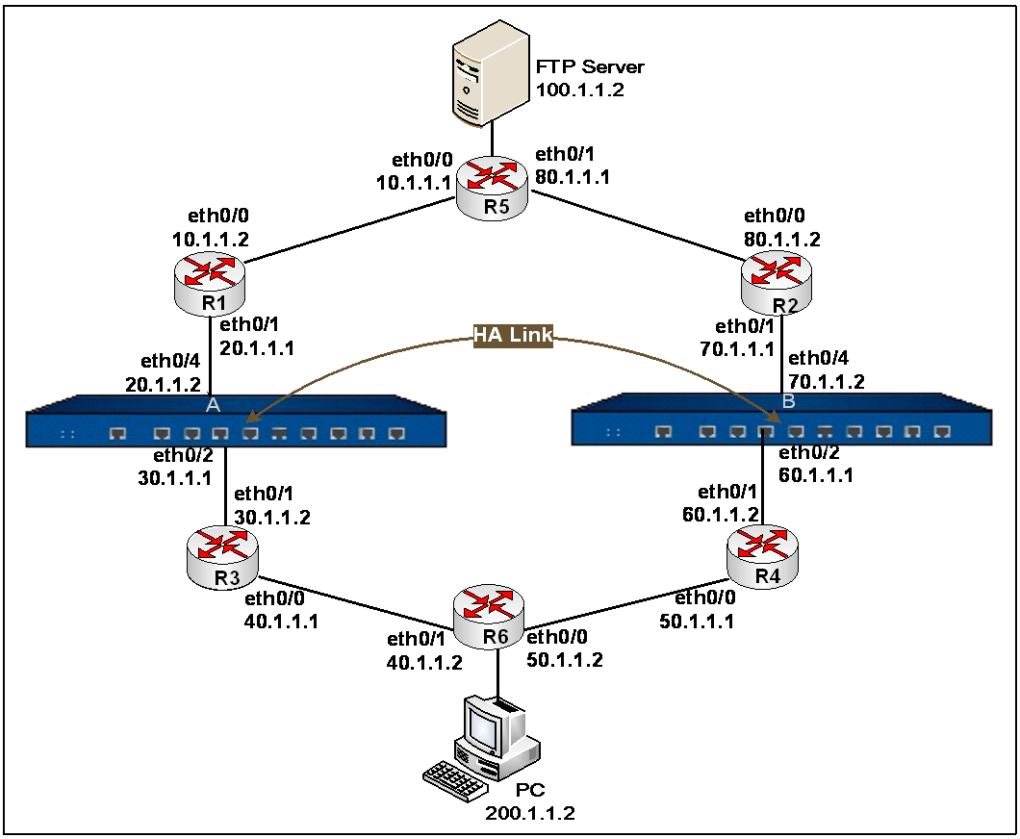
Example 3: Example of HA Peer Mode and HA Traffic

Requirement

This section describes how to configure HA Peer mode and HA traffic in asymmetrical routing environment. Before configuring, make sure the two Hillstone devices that will adopt HA Peer mode are using the same hardware platform, firmware version, license, and the interfaces that are connected to the network belong to the same security zone.

After completing the configuration, both of the two devices enable HA traffic. When PC requests any virus file in zip format from the FTP server, this function can assure the inbound and outbound packets will be processed on Device A, and related logs will also be generated on Device A. The network topology is shown below:

Figure 10: HA Traffic Network Topology



Configuration Steps

The following steps omit the configuration of interfaces and zones, and only focus on the configuration of HA Peer mode and HA traffic.

Step 1: Configure HA Peer mode and HA link interfaces:

Device A

```
hostname(config)# ha link interface eth0/1
hostname(config)# ha link ip 1.1.1.1/24
hostname(config)# ha link data interface eth0/3
hostname(config)# ha cluster 1 peer-mode node 0
hostname(config)# ha mode non-group
hostname(config)# exit
```

Device B

```
hostname(config)# ha link interface eth0/1
hostname(config)# ha link ip 1.1.1.2/24
hostname(config)# ha link data interface eth0/3
hostname(config)# ha cluster 1 peer-mode node 0
hostname(config)# ha mode non-group
hostname(config)# exit
```

Step 2: Enable HA traffic:

Device A

```
hostname(M0D1) (config)# ha traffic enable
hostname(M0D1) (config)# exit
```

Device B

```
hostname(config)(M0D1) # ha traffic enable
hostname(config)(M0D1) # exit
```

Step 3: Configure the asymmetric routing environment. Assume that all routers use the OSPF protocols and you have set the default metric and cost.

Device A

```
hostname(M0D1) (config) # ip vrouter trust-vr
hostname(M0D1) (config-vrouter)# router ospf
hostname(M0D1) (config-router) # router-id 1.1.1.1 local
hostname(M0D1) (config-router) # network 20.1.1.1/24 area 0
hostname(M0D1) (config-router) # network 30.1.1.1/24 area 0
hostname(M0D1) (config-router)# network 60.1.1.1/24 area 0
hostname(M0D1) (config-router)# network 70.1.1.1/24 area 0
hostname(M0D1) (config-router)# end
hostname(M0D1)# config
hostname(M0D1) (config)# interface eth0/2
hostname(M0D1) (config-if-eth0/2)# zone trust
hostname(M0D1) (config-if-eth0/2)# ip address 30.1.1.1/24
hostname(M0D1) (config-if-eth0/2)# exit
hostname(M0D1) (config)# interface eth0/2:1
hostname(M0D1) (config-if-eth0/2:1)# zone trust
hostname(M0D1) (config-if-eth0/2:1)# ip address 60.1.1.1/24
hostname(M0D1) (config-if-eth0/2:1)# exit
hostname(M0D1) (config)# interface eth0/4
hostname(M0D1) (config-if-eth0/4)# zone trust
hostname(M0D1) (config-if-eth0/4)# ip address 20.1.1.2/24
```

```
hostname(M0D1) (config-if-eth0/4)# exit
hostname(M0D1) (config)# interface eth0/4:1
hostname(M0D1) (config-if-eth0/4:1)# zone trust
hostname(M0D1) (config-if-eth0/4:1)# ip address 70.1.1.2/24
hostname(M0D1) (config-if-eth0/4:1)# exit
hostname(M0D1) (config-if-eth0/4:1)# end
```

Device B

```
hostname(D0M1) (config)# ip vrouter trust-vr
hostname(D0M1) (config-vrouter)# router ospf
hostname(D0M1) (config-router)# router-id 1.1.1.2 local
```

Step 4: Configure a track object to monitor the status of ethernet0/1 on R3. If the interface fails, all the sessions will be switched to Device B:

Device A

```
hostname(M0D1) (config)# track track1
hostname(M0D1) (config-trackip)# ip 30.1.1.2 interface eth0/2
hostname(M0D1) (config-trackip)# exit
hostname(M0D1) (config)# ha group 0
hostname(M0D1) (config-ha-non-group)# monitor track track1
hostname(M0D1) (config-ha-non-group)# exit
```

Step 5: Configure an AV profile on Device A and bind to the security zone:

Device A

```
hostname(M0D1) (config)# av-profile av
hostname(M0D1) (config-av-prifile)# profile-type ftp action log-only
hostname(M0D1) (config-av-prifile)# file-type zip
hostname(M0D1) (config-av-prifile)# exit
hostname(M0D1) (config)# zone untrust
hostname(M0D1) (config-zone-untrust)# av enable av
hostname(M0D1) (config-zone-untrust)# exit
```

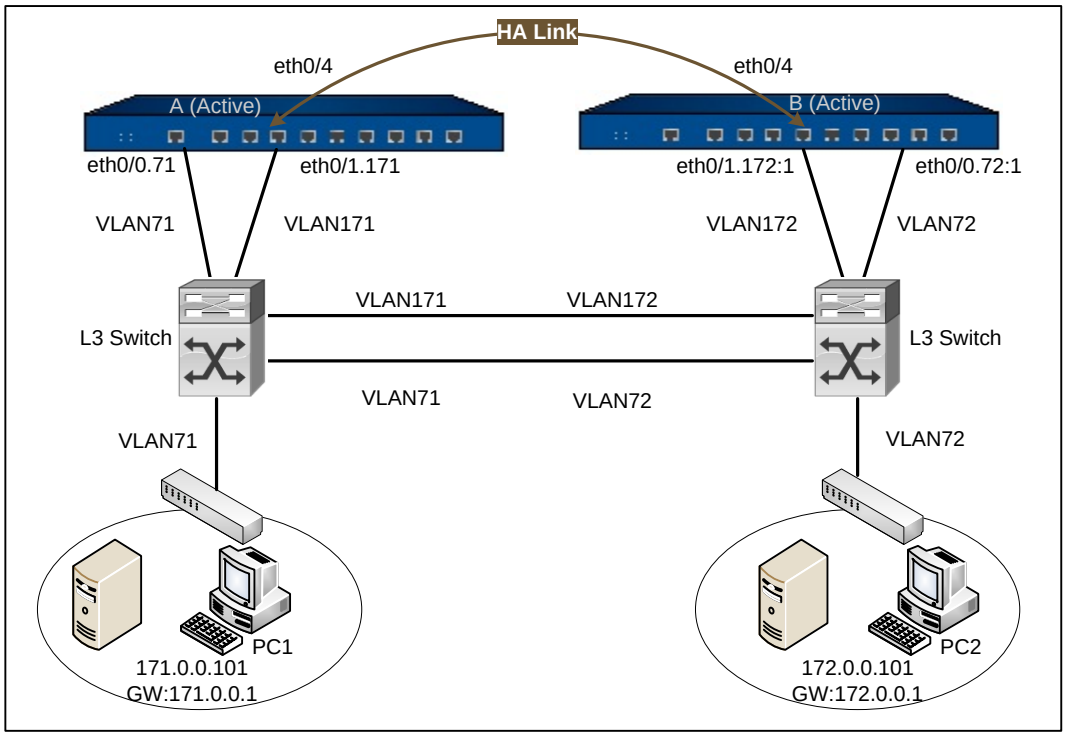
Example 4: Example of Configuring Specific Scenarios of HA A/A Mode

Requirement

PC1 and PC2 individually belong to different VLANs, and by configuring VRRP and STP, they accomplish the redundant backup.

PC1 and PC2 individually belong to different VLANs; the redundancy is implemented via VRRP and STP in L3 switches. Two Hillstone devices are accessed in bypass mode. The goal is to implement HA A/A redundancy and access control between VLANs. The network topology is shown as below:

Figure 11: HA A/A Network Topology



Configure as follows:

- Configure the two devices to HA A/A mode;
- Configure Virtual Wire to allow traffic between VLANs;
- Configure policy rules to implement access control between VLANs.

Configuration Steps

Step 1: Configure a track object to monitor the interface status of Device A and Device B. If the interface fails, all the sessions will be switched to Device B:

Device A

```
hostname(config)# track group0
hostname(config-trackip)# interface ethernet0/0.71
hostname(config-trackip)# interface ethernet0/1.171
hostname(config-trackip)# exit
hostname(config)# track group1
hostname(config-trackip)# interface ethernet0/0.72:1
hostname(config-trackip)# interface ethernet0/1.172:1
hostname(config-trackip)# exit
hostname(config)#
```

Step 2: Configure an HA group:

Device A

```
hostname(config)# ha group 0
hostname(config-ha-group)# priority 50
hostname(config-ha-group)# preempt 1
```

```
hostname(config-ha-group)# monitor track group0
hostname(config-ha-group)# exithostname(config)# ha group 1
hostname(config-ha-group)# priority 150
hostname(config-ha-group)# preempt 1
hostname(config-ha-group)# exit
hostname(config)#
```

Device B

```
hostname(config)# ha group 0
hostname(config-ha-group)# priority 150
hostname(config-ha-group)# preempt 1
hostname(config-ha-group)# exit
hostname(config)# ha group 1
hostname(config-ha-group)# priority 50
hostname(config-ha-group)# preempt 1
hostname(config-ha-group)# monitor track group0
hostname(config-ha-group)# exit
hostname(config)#
```

Step 3: Configure HA link interfaces:

Device A

```
hostname(config)# ha link interface ethernet0/4
hostname(config)# ha link ip 77.77.77.1 255.255.255.0
```

Device B

```
hostname(config)# ha link interface ethernet0/4
hostname(config)# ha link ip 77.77.77.2 255.255.255.0
```

Step 4: Configure interfaces and zones of Device A:

Device A

```
hostname(config)# zone l2-trust-1 l2
hostname(config-zone-l2-tru~)# exit
hostname(config)# zone l2-trust-2 l2
hostname(config-zone-l2-tru~)# exit
hostname(config)# zone l2-untrust-1 l2
hostname(config-zone-l2-unt~)# exit
hostname(config)# zone l2-untrust-2 l2
hostname(config-zone-l2-unt~)# exit
hostname(config)# interface ethernet0/0.71
hostname(config-if-eth0/0.71)# zone l2-trust-1
hostname(config-if-eth0/.71)# exit
hostname(config)# interface ethernet0/0.72:1
hostname(config-if-eth0/0.72:1)# zone l2-trust-2
hostname(config-if-eth0/0.72:1)# exit
hostname(config)# interface ethernet0/1.171
hostname(config-if-eth0/1.171)# zone l2-untrust-1
hostname(config-if-eth0/1.171)# exit
hostname(config)# interface ethernet0/1.172:1
hostname(config-if-eth0/1.172:1)# zone l2-untrust-2
hostname(config-if-eth0/1.172:1)# exit
hostname(config)#
```

Step 5: Configure Virtual Wire on Device A:

Device A

```
hostname(config)# vswitch vswitch1
hostname(config-vswitch)# ha-gratuious-mac-enable
hostname(config-vswitch)# virtual-wire set ethernet0/0.71
ethernet0/1.171
hostname(config-vswitch)# virtual-wire set ethernet0/0.72:1
ethernet0/1.172:1
hostname(config-vswitch)# virtual-wire enable unstrict
hostname(config-vswitch)# exit
hostname(config)#
```

Step 6: Configure policy rules on Device A:

Device A

```
hostname(config)# policy-global
hostname(config-policy)# rule
Rule id 1 is created
hostname(config-policy-rule)# src-zone l2-trust-1
hostname(config-policy-rule)# dst-zone l2-untrust-1
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
Rule id 2 is created
hostname(config-policy-rule)# src-zone l2-untrust-1
hostname(config-policy-rule)# dst-zone l2-trust-1
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
Rule id 3 is created
hostname(config-policy-rule)# src-zone l2-trust-2
hostname(config-policy-rule)# dst-zone l2-untrust-2
hostname(config-policy-rule)# src-addr any
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# rule
Rule id 4 is created
hostname(config-policy-rule)# src-zone l2-untrust-2
hostname(config-policy-rule)# dst-zone l2-trust-2
hostname(config-policy-rule)# src-addr any
```

```
hostname(config-policy-rule)# dst-addr any
hostname(config-policy-rule)# service any
hostname(config-policy-rule)# action permit
hostname(config-policy-rule)# exit
hostname(config-policy)# exit
hostname(config)#
```

Step 7: Configure the HA cluster and enable the HA function:

Device A

```
hostname(config)# ha cluster 1
```

Device B

```
hostname(config)# ha cluster 1
```