Hillstone Networks

Hillstone Networks Application Delivery Controller WebUI Guide

Version 2.10

Hillstone Networks

This document is forbidden to use in commercial.

Contact Information:

US Headquarters:

Hillstone Networks

5201 Great America Pkwy, #420

Santa Clara, CA 95054

Phone: 1-800-889-9860

About this Guide:

This guide gives comprehensive configuration instructions of Hillstone NetworksApplication Delivery Controller(ADC) .

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

To provide feedback on the documentation, please write to us at: TechDocs@hillstonenet.com

Hillstone Networks

TWNO: TW-WUG-ADC-2.10-EN-V1.0-11/4/2021

Table of Contents

Welcome

Thanks for choosing Hillstone products!

This part introduces how to get user guides of Hillstone products.

OS Operation Guides:

- Hillstone ADC WebUI User Guide (Download PDF)
- Hillstone vADC Deployment Guide (Download PDF)
- Hillstone ADC SNMP MIB Reference Guide (Download PDF)

Hardware Installation Guides:

- Hillstone ADC Hardware Reference Guide (Download PDF)

Other Support Links:

- Webiste: www.hillstonenet.com
- Download Documentations: https://docs.hillstonenet.com
- Technical Support: 1-800-889-9860

Chapter 1 Deploying Your Device

This chapter introduces how an ADC device works and its most commonly used scenarios. Understanding the system structure, basic elements and flow chart will help you in better organizing your network and making the most of the ADC device. Click here for ADC introduction and how the ADC works.

An ADC has more than one deployment scenario. Each scenario applies to one environment requirement. The usual deployment modes are:

- "One-Arm Mode" on Page 2

  One-arm mode applies when the IT administrator does not wish to change his/her existing network settings. In one-arm mode, the ADC device is added to the existing network environment in a bypass manner, and it only provides load balance features.

- "Transparent Mode" on Page 6

  Transparent mode also applies when the IT administrator does not wish to change his/her existing network settings. In transparent mode, the ADC device is invisible to the network. Because no IP address configuration is needed, the device only provides load balance features.

- "Serial Routing Mode" on Page 11

  In serial routing mode, the ADC device is usually deployed between a server and a gateway that are on different network segments. This mode can maximize the effects of load balance.

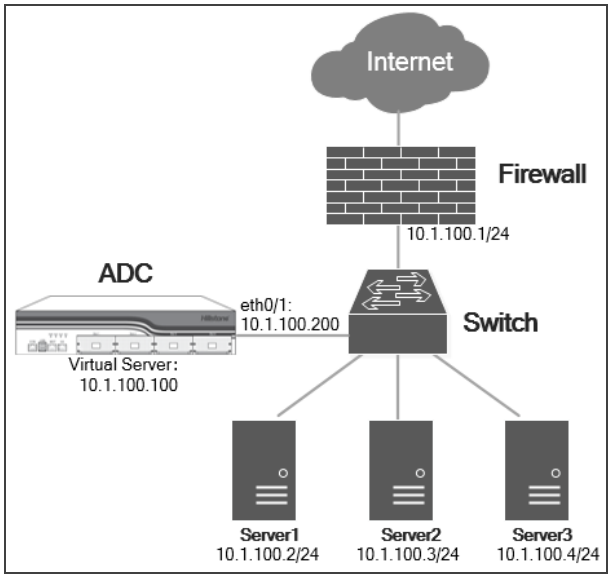
- "DSR Mode" on Page 16

  DSR mode is often used in network scenarios that require low latency, such as voice and video applications. Nevertheless, this mode is only supported on Layer 4, but not on Layer 7.

One-Arm Mode

One-arm mode is often used when the IT administrator wants to deploy the ADC device in a bypass manner to the existing network environment without affecting the entire network's performance. When the server load balance is implemented in the one-arm mode, the real IP of the client is invisible to the server side.

In one-arm mode, the device is usually directly connected to the internal network switch. The example which is based on the below topology shows you how to connect and configure a new device in transparent mode.



To deploy the device in one-arm mode, take the following steps:

Step 1: Configuring an interface

1. Log in the device via WebUI.
2. Select **Network** > **Interface**.
3. Double click **ethernet0/1**.

   In the Ethernet Interface dialog box, enter values.

Option	Value
Binding Zone	Layer 3 Zone
Zone	trust
Type	Static IP
IP Address	10.1.100.200
Netmask	255.255.255.0
Reverse Route	Close

4. Click **OK**.

Step 2: Configuring a route

1. Select **Network** > **Routing** > **Destination Route**.

2. Click **New**, and create a route entry in the pop-up **Destination Route Configuration** dialog box.

   In the Destination Route Configuration dialog box, enter values.

Option	Value
Destination	0.0.0.0
Netmask	0.0.0.0 (means all subnets)
Gateway	10.1.100.1

3. Click **OK**.

Step 3: Configuring a real server

1. Select **Load Balance** > **Server Load Balance** > **Real Server**.

2. Click **New**.

   In the Real Server Configuration dialog box, enter values.

Option	Value
Name	server2
IP Address	10.1.100.2
Port	80
Max Connections	10000 (means that the maximum number of concurrent connections allowed for the real server is 10000. The value of 0 indicates no limitation.)
Recovery Time	20 (means that the recovery period of the real server is 20s. That is to say, after the health check is configured, the amount of time that the real server takes to change from down to up. Within the recovery period, the real server will not receive client requests. After the recovery period ends, the real server will enter the warmup period.)
Warmup Time	300 (means that the warmup period of the real server is 300s. Within the warmup period, the real server will respond to part of client requests. After the warmup period ends, the real server will respond to all the client

Option	Value
	requests until the maximum number of connections is reached. You can set the warmup period according to the performance of the server.)

3. Repeat step 2 to create "server3", configure its **IP Address** as "10.1.100.3", and keep other parameters consistent with those of the server2.
4. Repeat step 2 to create "server4", configure its **IP Address** as "10.1.100.4", and keep other parameters consistent with those of the server2.

Step 4: Binding real servers to a server pool

1. Select **Load Balance** > **Server Load Balance** > **Server Pool**.
2. Click **New**, and select **TCP** from the drop-down list.

   In the TCP Server Pool Configuration dialog box, enter values.

Option	Value
Name	pool_tcp
Member	Select **server2**, **server3** and **server4** from the left pane, and click → to add them to the server pool.
Health Check	tcp-def (means that the status of the TCP connection between the device and a real server will be checked.)
Balance Method	Round Robin (means that client requests will be distributed to each real server in turn.)
Persistence Method	Source IP (means that client requests from the same source IP address, including all subsequent connection requests, will be sent to the same real server.)
Timeout	3000 (means that if the timeout value is exceeded, the device will clear the session information of the client.)

3. Click **Save**.

Step 5: Binding the server pool to a virtual server

1. Select **Load Balance** > **Server Load Balance** > **Virtual Server**.

2. Click **New**, and select **TCP** from the drop-down list.

   In the TCP Virtual Server Configuration dialog box, enter values.

Option	Value
Name	vs_tcp
IP: Port	Select **IP Address**, and type "10.1.100.100" into the text box; select **Port**, and type "8888" into the text box, and then click **Add**.
Server Pool	Select **pool_tcp** from the drop-down list.

3. Click **Save**.

Step 6: Configuring SNAT

1. Select **Network** > **NAT** > **SNAT**.

2. Click **New**, and create an SNAT entry in the pop-up **SNAT Configuration** dialog box.

   In the SNAT Configuration dialog box, enter values.

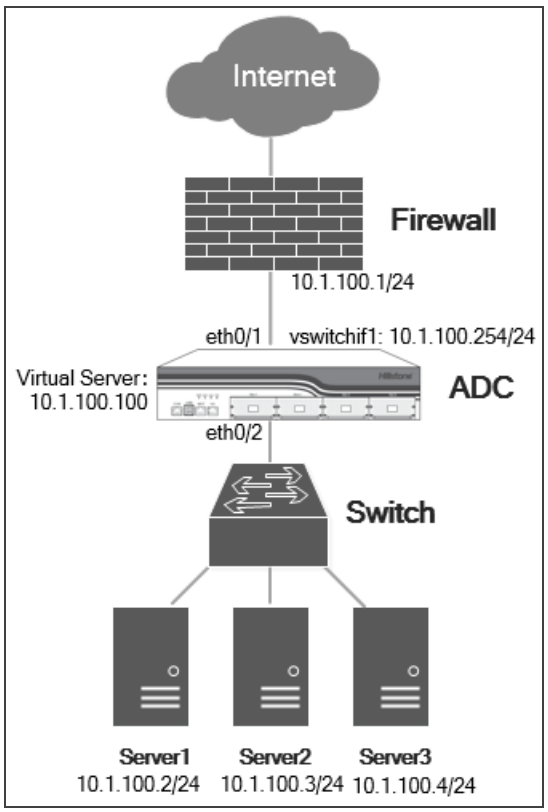
Option	Value
Source Address	Address Entry, Any
Destination Address	Address Entry, Any
Ingress Traffic	All Traffic
Egress	Egress Interface, etherent0/1
Translated	Egress IF IP

3. Click **OK**.

Transparent Mode

Transparent mode is also known as bridge mode or transparent bridging mode. It is used when the IT administrator does not wish to change the existing network layout, which has already been set up with routers and switches. The deployment is simple and easy to use, and is applicable to most network environments.

In transparent mode, the device usually replaces the internal network switch, or is deployed between the gateway and the internal network switch. The example which is based on the below topology shows you how to connect and configure a new device in transparent mode.



To deploy the device in transparent mode, take the following steps:

Step 1: Configuring interfaces and zones

1. Log in the device via WebUI.
2. Select **Network** > **Interface**.
3. Double click **ethernet0/1**, and the Ethernet Interface dialog box will appear.
4. Select **Layer 2 Zone** as the binding zone, select **l2-untrust** from the **Zone** drop-down list, and click **OK**.
5. Repeat steps 3 through 4 to bind the interfaces "ethernet0/2", "ethernet0/3" and "ethernet0/4" to the Layer 2 zone "l2-trust".
6. Select **Network** > **Zone**.

7. Double click **l2-trust**.

   In the Zone Configuration dialog box, enter values.

Option	Value
Zone	l2-trust
VSwitch	vswitch1
Binding Interface	Select **ethernet0/2**, **ethernet0/3** and **ethernet0/4** from the drop-down list.

8. Click **OK**.

9. Repeat steps 6 through 8 to bind the zone "l2-untrust" to the virtual switch "vswitch1".

Step 2: Configuring a VSwitch interface

1. Select **Network** > **Interface**.

2. Double click **vswitchif1**.

   In the VSwitch Interface dialog box, enter values.

Option	Value
Binding Zone	Layer 3 Zone
Zone	trust
Type	Static IP
IP Address	10.1.100.254
Netmask	255.255.255.0
Reverse Route	Close

3. Click **OK**.

Step 3: Configuring a route

1. Select **Network** > **Routing** > **Destination Route**.

2. Click **New**, and create a route entry in the pop-up **Destination Route Configuration** dialog box.

   In the Destination Route Configuration dialog box, enter values.

Option	Value
Destination	0.0.0.0
Netmask	0.0.0.0 (means all subnets)
Gateway	10.1.100.1

3. Click **OK**.

Step 4: Configuring a real server

1. Select **Load Balance** > **Server Load Balance** > **Real Server**.
2. Click **New**.

   In the Real Server Configuration dialog box, enter values.

Option	Value
Name	server2
IP Address	10.1.100.2
Port	80
Max Connections	10000 (means that the maximum number of concurrent connections allowed for the real server is 10000. The value of 0 indicates no limitation.)
Recovery Time	20 (means that the recovery period of the real server is 20s. That is to say, after the health check is configured, the amount of time that the real server takes to change from down to up. Within the recovery period, the real server will not receive client requests. After the recovery period ends, the real server will enter the warmup period.)
Warmup Time	300 (means that the warmup period of the real server is 300s. Within the warmup period, the real server will respond to part of client requests. After the warmup period ends, the real server will respond to all the client requests until the maximum number of connections is reached. You can set the warmup period according to the performance of the server.)

3. Repeat step 2 to create "server3", configure its **IP Address** as "10.1.100.3", and keep other parameters consistent with those of the server2.

4. Repeat step 2 to create "server4", configure its **IP Address** as "10.1.100.4", and keep other parameters consistent with those of the server2.

Step 5: Binding real servers to a server pool

1. Select **Load Balance** > **Server Load Balance** > **Server Pool**.
2. Click **New**, and select **TCP** from the drop-down list.

   In the TCP Server Pool Configuration dialog box, enter values.

Option	Value
Name	pool_tcp
Member	Select **server2**, **server3** and **server4** from the left pane, and click → to add them to the server pool.
Health Check	tcp-def (means that the status of the TCP connection between the device and a real server will be checked.)
Balance Method	Round Robin (means that client requests will be distributed to each real server in turn.)
Persistence Metho	Source IP (means that client requests from the same source IP address, including all subsequent connection requests, will be sent to the same real server.)
Timeout	3000 (means that if the timeout value is exceeded, the device will clear the session information of the client.)

3. Click **Save**.

Step 6: Binding the server pool to a virtual server

1. Select **Load Balance** > **Server Load Balance** > **Virtual Server**.
2. Click **New**, and select **TCP** from the drop-down list.

   In the TCP Virtual Server Configuration dialog box, enter values.

Option	Value
Name	vs_tcp
IP: Port	Select **IP Address**, and type "10.1.100.100" into the text box; select **Port**, and type "8888" into the text box, and then click **Add**.
Server Pool	Select **pool_tcp** from the drop-down list.

3. Click **Save**.

Step 7: Configuring SNAT

1. Select **Network** > **NAT** > **SNAT**.

2. Click **New**, and create an SNAT entry in the pop-up **SNAT Configuration** dialog box.

   In the SNAT Configuration dialog box, enter values.

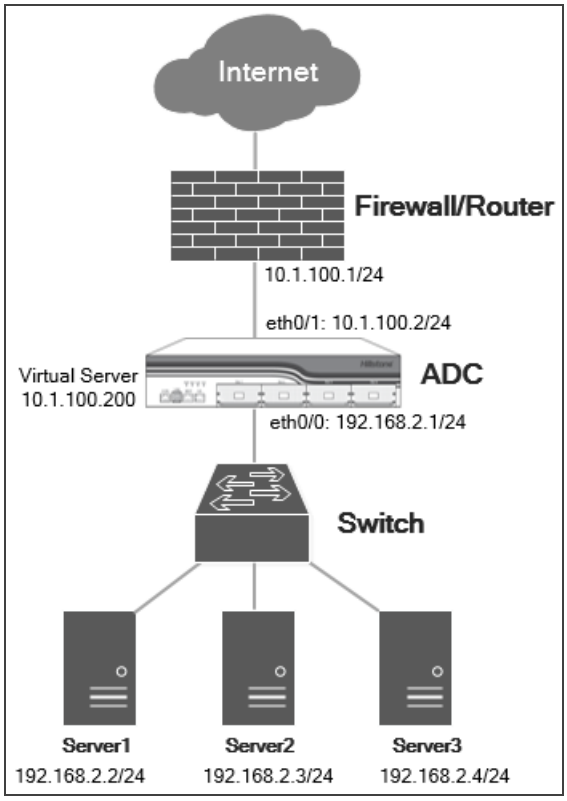
Option	Value
Source Address	Address Entry, Any
Destination Address	Address Entry, Any
Ingress Traffic	All Traffic
Egress	Egress Interface, vswitchif1
Translated	Egress IF IP

3. Click **OK**.

Serial Routing Mode

Serial routing mode is characterized by deploying the ADC device between a server and a gateway, which can maximize the effects of load balance. The two sides of the ADC device (i.e., the server and the gateway) are on different network segments, so that the server can be isolated and the server security can be ensured.

According to the following topology, the IT administrator configures the device through the management port MGT0, and uses cables to connect the interface eth0/1 to the router and the interface eth0/0 to the switch. Meanwhile, the original intranet deployment will remain unchanged.



To deploy the device in serial routing mode, take the following steps:

Step 1: Configuring interfaces and zones

1. Log in the device via WebUI.
2. Select **Network** > **Interface**.
3. Double click **ethernet0/1**.

   In the Ethernet Interface dialog box, enter values.

Option	Value
Binding Zone	Layer 3 Zone
Zone	trust
Type	Static IP
IP Address	10.1.100.2
Netmask	255.255.255.0

4. Click **OK**.
5. Repeat step 3 to configure the interface "ethernet 0/0".

   In the Ethernet Interface dialog box, enter values.

Option	Value
Binding Zone	Layer 3 Zone
Zone	trust
Type	Static IP
IP Address	192.168.2.1
Netmask	255.255.255.0

6. Click **OK**.

Step 2: Configuring a route

1. Select **Network** > **Routing** > **Destination Route**.
2. Click **New**, and create a route entry in the pop-up **Destination Route Configuration** dialog box.

   In the Destination Route Configuration dialog box, enter values.

Option	Value
Destination	0.0.0.0
Netmask	0.0.0.0 (means all subnets)
Gateway	10.1.100.1

3. Click **OK**.

Step 3: Configuring a real server

1. Select **Load Balance** > **Server Load Balance** > **Real Server**.
2. Click **New**.

   In the Real Server Configuration dialog box, enter values.

Option	Value
Name	server2
IP Address	192.168.2.2
Port	80
Max Connections	10000 (means that the maximum number of concurrent connections allowed for the real server is 10000. The value of 0 indicates no limitation.)
Recovery Time	20 (means that the recovery period of the real server is 20s. That is to say, after the health check is configured, the amount of time that the real server takes to change from down to up. Within the recovery period, the real server will not receive client requests. After the recovery period ends, the real server will enter the warmup period.)
Warmup Time	300 (means that the warmup period of the real server is 300s. Within the warmup period, the real server will respond to part of client requests. After the warmup period ends, the real server will respond to all the client requests until the maximum number of connections is reached. You can set the warmup period according to the performance of the server.)

3. Repeat step 2 to create "server3", configure its **IP Address** as "192.168.2.3", and keep other parameters consistent with those of the server2.
4. Repeat step 2 to create "server4", configure its **IP Address** as "192.168.2.4", and keep other parameters consistent with those of the server2.

Step 4: Binding real servers to a server pool

1. Select **Load Balance** > **Server Load Balance** > **Server Pool**.
2. Click **New**, and select **TCP** from the drop-down list.

   In the TCP Server Pool Configuration dialog box, enter values.

Option	Value
Name	pool_tcp
Member	Select **server2**, **server3** and **server4** from the left pane, and click → to add

Option	Value
	them to the server pool.
Health Check	tcp-def (means that the status of the TCP connection between the device and a real server will be checked.)
Balance Method	Round Robin (means that client requests will be distributed to each real server in turn.)
Persistence Method	Source IP (means that client requests from the same source IP address, including all subsequent connection requests, will be sent to the same real server.)
Timeout	3000 (means that if the timeout value is exceeded, the device will clear the session information of the client.)

3. Click **Save**.

Step 5: Binding the server pool to a virtual server

1. Select **Load Balance** > **Server Load Balance** > **Virtual Server**.
2. Click **New**, and select **TCP** from the drop-down list.

   In the TCP Virtual Server Configuration dialog box, enter values.

Option	Value
Name	vs_tcp
IP: Port	Select **IP Address**, and type "10.1.100.200" into the text box; select **Port**, and type "8888" into the text box, and then click **Add**.
Server Pool	Select **pool_tcp** from the drop-down list.

3. Click **Save**.

Step 6: Configuring SNAT

1. Select **Network** > **NAT** > **SNAT**.
2. Click **New**, and create an SNAT entry in the pop-up **SNAT Configuration** dialog box.

In the SNAT Configuration dialog box, enter values.

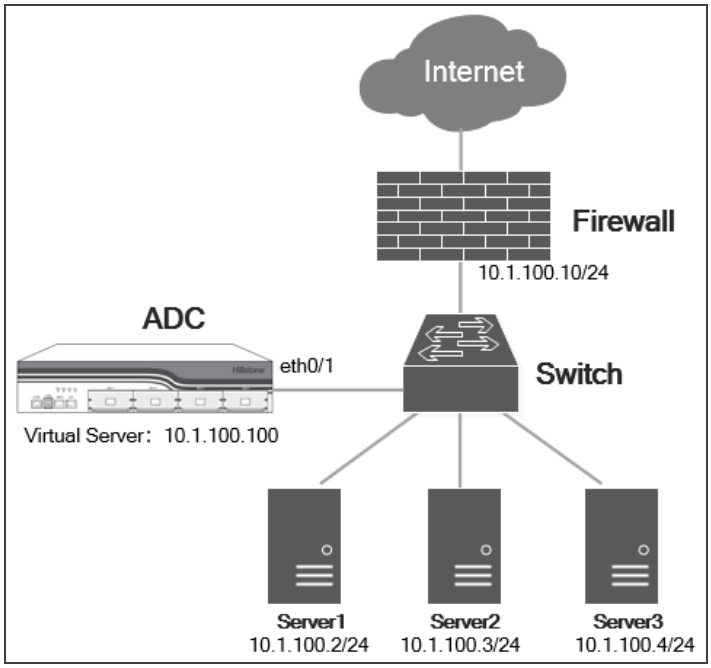
Option	Value
Source Address	Address Entry, Any
Destination Address	Address Entry, Any
Ingress Traffic	All Traffic
Egress	Egress Interface, etherent0/0
Translated	Egress IF IP

3. Click **OK**.

DSR Mode

Direct Server Return (DSR) mode is also called the triangle mode, which is characterized by that a server responds directly to a client. In DSR mode, a request sent by a client to a server will be processed by the ADC device first, and then forwarded to the server. However, a response returned by the server will be sent directly to the client instead of passing through the device. Such asymmetric deployment mode can avoid performance bottlenecks caused by load balancers, and reduce network latency. It is often used in network scenarios that require low latency, such as voice and video applications. Nevertheless, this mode is only supported on Layer 4, but not on Layer 7.

In DSR mode, the device is usually directly connected to the internal network switch. The example which is based on the below topology shows you how to connect and configure a new device in transparent mode. **Note**: Loopback interface should be configured for server 1/server 2/server 3, and its address is 10.1.100.100.



To deploy the device in DSR mode, take the following steps:

Step 1: Configuring interfaces and zones

1. Log in the device via WebUI.
2. Select **Network** > **Interface**.
3. Double click **ethernet0/1**.

   In the Ethernet Interface dialog box, enter values.

Option	Value
Binding Zone	Layer 3 Zone
Zone	trust
Type	Static IP
IP Address	10.1.100.200
Netmask	255.255.255.0

4. Click **OK**.

Step 2: Configuring a route

1. Select **Network** > **Routing** > **Destination Route**.

2. Click **New**, and create a route entry in the pop-up **Destination Route Configuration** dialog box.

   In the Destination Route Configuration dialog box, enter values.

Option	Value
Destination	0.0.0.0
Netmask	0.0.0.0 (means all subnets)
Gateway	10.1.100.1

3. Click **OK**.

Step 3: Configuring a real server

1. Select **Load Balance** > **Server Load Balance** > **Real Server**.

2. Click **New**.

   In the Real Server Configuration dialog box, enter values.

Option	Value
Name	server2
IP Address	10.1.100.2
Port	80
Max Connections	10000 (means that the maximum number of concurrent connections allowed for the real server is 10000. The value of 0 indicates no limitation.)
Recovery Time	20 (means that the recovery period of the real server is 20s. That is to say, after the health check is configured, the amount of time that the real server takes to change from down to up. Within the recovery period, the real server will not receive client requests. After the recovery period ends, the real server will enter the warmup period.)
Warmup Time	300 (means that the warmup period of the real server is 300s. Within the warmup period, the real server will respond to part of client requests. After the warmup period ends, the real server will respond to all the client

Option	Value
	requests until the maximum number of connections is reached. You can set the warmup period according to the performance of the server.

3. Repeat step 2 to create "server3", configure its **IP Address** as "10.1.100.3", and keep other parameters consistent with those of the server2.
4. Repeat step 2 to create "server4", configure its **IP Address** as "10.1.100.4", and keep other parameters consistent with those of the server2.

Step 4: Binding real servers to a server pool

1. Select **Load Balance** > **Server Load Balance** > **Server Pool**.
2. Click **New**, and select **TCP** from the drop-down list.

   In the TCP Server Pool Configuration dialog box, enter values.

Option	Value
Name	pool_tcp
Member	Select **server2**, **server3** and **server4** from the left pane, and click → to add them to the server pool.
Health Check	tcp-def (means that the status of the TCP connection between the device and a real server will be checked.)
Balance Method	Round Robin (means that client requests will be distributed to each real server in turn.)
Persistence Method	Source IP (means that client requests from the same source IP address, including all subsequent connection requests, will be sent to the same real server.)
Timeout	3000 (means that if the timeout value is exceeded, the device will clear the session information of the client.)

3. Click **Save**.

Step 5: Binding the server pool to a virtual server

1. Select **Load Balance** > **Server Load Balance** > **Virtual Server**.

2. Click **New**, and select **TCP** from the drop-down list.

   In the TCP Virtual Server Configuration dialog box, enter values.

Option	Value
Name	vs_tcp
IP: Port	Select **IP Address**, and type "10.1.100.100" into the text box; select **Port**, and type "8888" into the text box, and then click **Add**.
Server Pool	Select **pool_tcp** from the drop-down list.
DSR	Select the **Enable** check box to enable the DSR mode. In the DSR mode, a request sent by a client to a real server will be processed by the device first, and then forwarded to the real server. However, a response returned by the real server will be sent directly to the client instead of passing through the device.

3. Click **Save**.

Chapter 2 Dashboard

Customize

You can customize the dashboard display function or modify the function area location as needed.

- To customize the dashboard display function, take the following steps:

  1. Click **Customize** at the top-right corner.
  2. Select the functions you want to display in the dashboard from the expanded list.

- To modify the function area location, take the following steps:

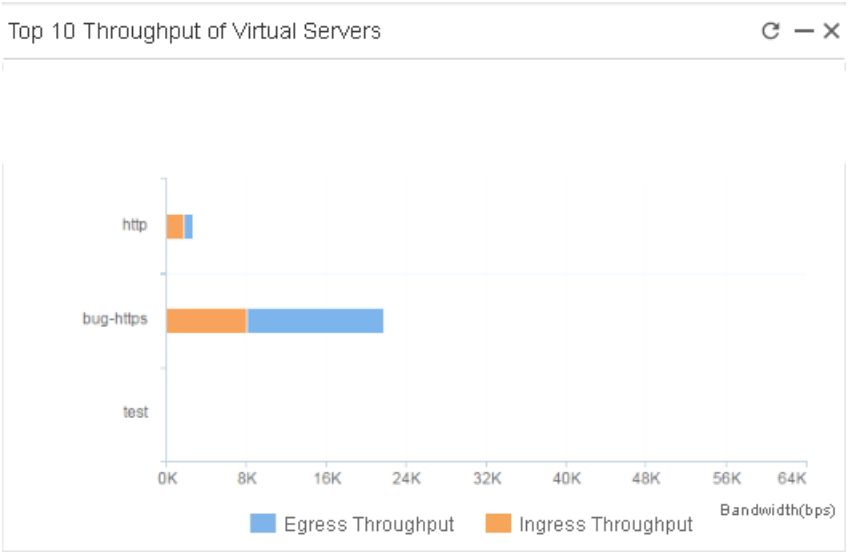
  1. Hover your mouse over the title part in the ribbon.
  2. When  appears, press and hold the mouse, and move the function area to the location you desire.

- To set the refresh interval of the page, take the following steps:

  1. Click the drop-down list behind Refresh Interval at the top-right corner.
  2. Select a specific time interval, or select **Manual**.

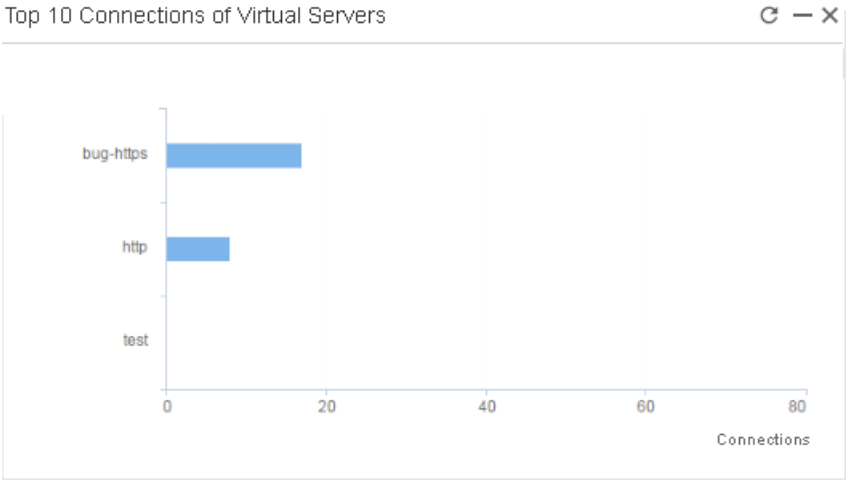
Top 10 Throughput of Virtual Servers

This widget displays the top 10 throughput of virtual servers as a bar chart. Hover your mouse over a bar to view the virtual server name and values of the egress and ingress throughput.



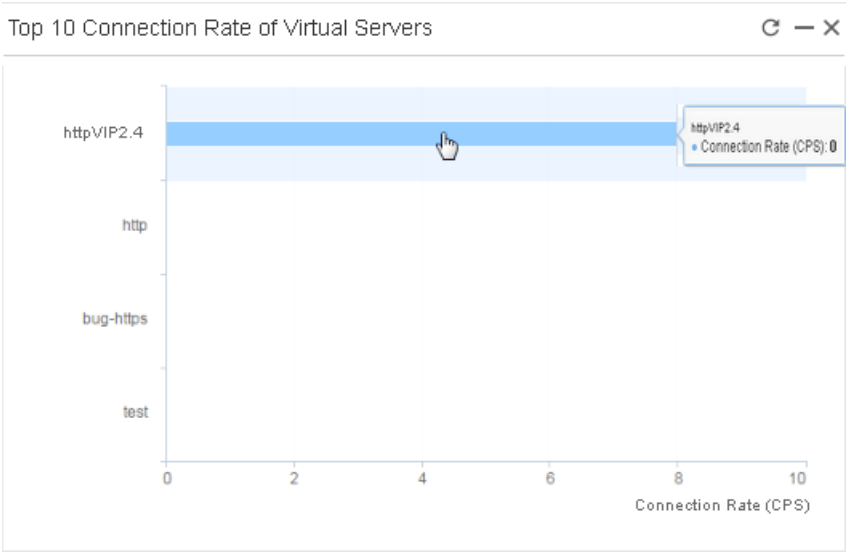
Top 10 Connections of Virtual Servers

This widget displays the top 10 current connections of virtual servers as a bar chart. Hover your mouse over a bar to view the virtual sever name and the number of current connections.



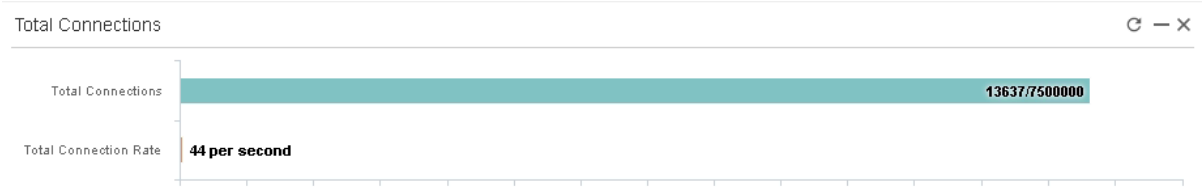
Top 10 Connection Rate of Virtual Servers

This widget displays the top 10 rate of new connections of virtual servers as a bar chart. Hover your mouse over a bar to view the virtual server name and the value of the rate of new connections.



Total Connections

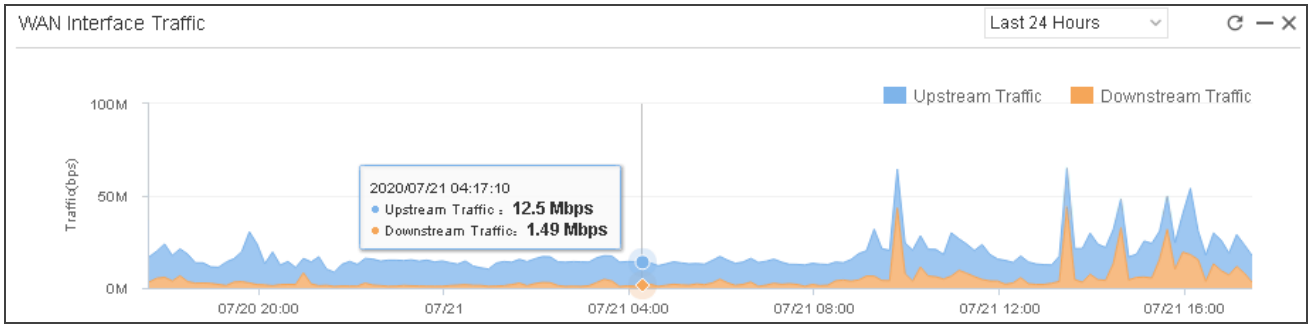
This widget displays the number of current connections/total connections of the device, and the current rate of new connections.



WAN Interface

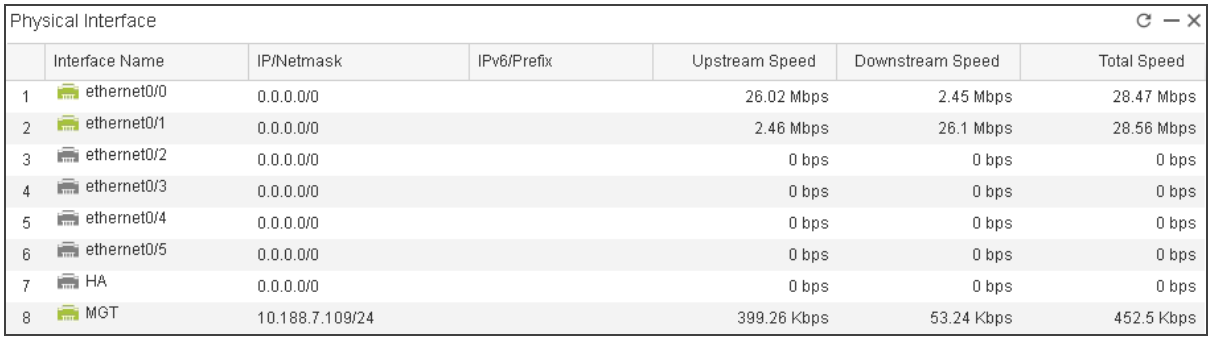
This widget displays the traffic statistics on all WAN-enabled interfaces of the device within the specified period.

Hover your mouse over the graph to view the upstream and downstream traffic of WAN interfaces at a specific time point.



Physical Interface

This widget displays the statistical information of all physical interfaces of the device, including the interface name, primary IP/netmask, upstream speed, downstream speed, and total speed.



	Interface Name	IP/Netmask	IPv6/Prefix	Upstream Speed	Downstream Speed	Total Speed
1	ethernet0/0	0.0.0.0/0		26.02 Mbps	2.45 Mbps	28.47 Mbps
2	ethernet0/1	0.0.0.0/0		2.46 Mbps	26.1 Mbps	28.56 Mbps
3	ethernet0/2	0.0.0.0/0		0 bps	0 bps	0 bps
4	ethernet0/3	0.0.0.0/0		0 bps	0 bps	0 bps
5	ethernet0/4	0.0.0.0/0		0 bps	0 bps	0 bps
6	ethernet0/5	0.0.0.0/0		0 bps	0 bps	0 bps
7	HA	0.0.0.0/0		0 bps	0 bps	0 bps
8	MGT	10.188.7.109/24		399.26 Kbps	53.24 Kbps	452.5 Kbps

System Information

System information includes:

- Serial Number: The serial number of the device.
- Hostname: The host name of the device.
- Platform: The platform type of the device.
- System Time: The system date and time of the device.
- System Uptime: The system uptime of the device.
- Firmware: The current firmware version of the device.
- Boot File: The boot file name and the last update time.

Chapter 3 Server Load Balance

As the application traffic increases, a single server may be unable to handle multiple simultaneous access requests due to the insufficient performance, so that multiple servers are needed to provide services. Server Load Balance (SLB) function is designed to distribute client requests to different servers according to specified load balance algorithms to achieve fast response.

The ADC device can map the addresses of multiple real servers to a single virtual server address (Virtual IP). When the user's access requests reach the ADC device, the virtual server will forward the requests to the real servers according to the configured SLB rule or load balance algorithm. At the same time, the device will monitor the status of real servers. If any abnormality is found in a real server, it will forward the requests to other real servers that work normally.

Currently, the ADC device supports Layer 4 and Layer 7 load balance. Taking the Layer 7 load balance as an example, the processing flow is as follows:

1. First, the client initiates a request. Then, after reaching the ADC device, the request will be matched to a virtual server according to the device configuration.
2. The virtual server will perform matching according to the SLB rules, wherein content rewrite rules, Layer 4 content switching rules and Layer 7 content switching rules will be matched sequentially.
3. If a content rewrite rule is matched, the device will rewrite the message according to the rule configuration, and then continue to match the request with Layer 4 content switching rules. If no content rewrite rule is matched, the device will directly match the request with Layer 4 content switching rules without rewriting the message.
   Note: If the content rewrite is configured with a redirection rewrite rule, the virtual server will not match the request with Layer 4 content switching rules, but will directly return a response to the client.
4. If a Layer 4 content switching rule is matched, the request will be distributed to a real server according to the rule configuration, or to a real server according to the server pool configuration. If no Layer 4 content switching rule is matched, the device will continue to match the request with Layer 7 content switching rules.
5. If a Layer 7 content switching rule is matched, the request will be distributed to a real server according to the rule configuration, or to a real server according to the server pool configuration.
6. If no SLB rules are matched, a real server will be selected according to the session persistence table of the default server pool or a load balance algorithm, and then the request will be distributed to the real server.
7. The virtual server will return the response of the real server to the client.

Note:

After a client request enters the server pool, it will be matched with an entry in the session persistence table first. If an entry is matched, the device will directly allocate a real server. Otherwise, a real server will be selected according to the load balance algorithm configured in the server pool.

SLB Concepts

Basic concepts related to the SLB function include:

- Real Server: A dedicated physical server which is deployed in the user's network environment and responsible for processing client requests.
- Server Pool: A group of real servers provide same services.
- Virtual Server: The starting point of the SLB process. Traffic of different services will match different virtual servers. According to the configuration, the virtual server will distribute client requests to corresponding servers, and then return server responses to clients.
- "Load Balance Algorithm" on Page 26: The algorithm is responsible for distributing requests across a server pool. The virtual server will distribute client requests according to different load balance algorithms.
- SLB Rule: It includes Layer 4 content switching rules, content rewrite rules and Layer 7 content switching rules. The virtual server distributes client requests according to SLB rules.
- Health Check: System performs health checks on the status of real servers. If a server works abnormally, it will be excluded from the server resources that can be allocated to ensure that client requests are distributed to working servers.
- **Session Persistence**: To maintain the continuity and consistency of a session, requests from the same client will be distributed to the same server instead of multiple servers.

Load Balance Algorithm

System supports multiple load balance algorithms, including:

Algorithm	Description
Round Robin	Client requests will be distributed to each real server in a queue in turn.

Weighted Round Robin	According to their performance, real servers will be given different weights. The device will distribute client requests in proportion to weights of real servers. The real server with higher weight will receive a higher proportion of requests.
IP Hash	First, the source address of a client will be hashed. Then, the client will be allocated to a real server according to the hash value. If the server list remains unchanged, clients on the same IP address will be allocated to the same real server every time.
Weighted IP Hash	Based on the IP Hash algorithm, the device will distribute client requests in proportion to weights of real servers. The real server with higher weight will receive a higher proportion of requests.
IP-Port Hash	First, the IP address and port number of the client will be hashed. Then, the client will be allocated to a real server according to the hash value.
Weighted IP-Port Hash	Based on the IP-Port Hash algorithm, the device will distribute client requests in proportion to weights of real servers. The real server with higher weight will receive a higher proportion of requests.
Consistent IP Hash	First, the source address of a client will be hashed. Then, the client will be allocated to a real server according to the hash value. If a real server fails to function due to a fault or other reasons, the requests originally sent to the failed real server will be redistributed to other available real servers; and the requests (from the same source IP or the same client) originally sent to the real servers without failure will not be redistributed.
Least Connection	The device will record the number of connections on each real server or port. After a new connection is generated, the device will distribute it to the real server with the fewest active connections.
Weighted Least Connection	Based on the least connection algorithm, each real server will be given a weight according to its performance. The weight indicates the performance of each real server. After a new connection is generated, the latest request will be distributed to the real server with the smallest ratio of the number of active connections to the weight (Calculation method: divide the current number of connections by the weight).
Fastest Response	The device will record the number of connections on each real server or port. After a new connection is generated, the device will distribute it to the real server with the fastest response time.
Priority	Requests will be distributed to a real server with the highest priority. The smaller the priority value is, the higher the priority of the real server will be. If there are multiple real

	servers with the same highest priority, resources will be allocated by round robin among these real servers.
Dynamic Ratio	According to the different processing capabilities of real servers, the device calculates different dynamic weights. The device will distribute client requests in proportion to dynamic weights of real servers. The real server with higher dynamic weight will receive a higher proportion of requests. If the dynamic weight is 0, the real server will not be distributed with requests. In general, the dynamic weight value is calculated by the SNMP health check; in other cases, the value of 1 means that the real server can provide services, while 0 means it is unavailable.
Least Bandwidth	The device will record the sum of upstream and downstream bandwidth on each real server or port. When a new connection is requested, the device will distribute it to the real server with the least sum.
Weighted Least Bandwidth	Based on the least bandwidth algorithm, each real server will be given a weight according to its performance. The weight indicates the performance of each real server. When a new connection is requested, the latest request will be distributed to the real server with the smallest ratio of the sum to the weight (Calculation method: dividing the sum by the weight).

Virtual Server

The device can map the addresses of multiple real servers to a single virtual server address. When client requests reach the AX device, the device will forward the requests to corresponding real servers according to the configuration of the virtual server.

You can configure an IPv4 or IPv6 address for the virtual server. To configure a virtual server with an IPv6 address, you need to configure the address of the corresponding interface as the IPv6 first. To enable the IPv6 on an interface, select **Network** > **Interface**. When editing an interface, click the **IPv6 Configuration** tab, and select the **Enable** check box.

For HTTP and HTTPS/HTTP-Proxy virtual servers, external link rewrite is supported. If a client is upgraded to IPv6, and a response returned from a real server contains an external link (IPv4), system will rewrite the response body containing the external link (IPv4), and return it to the client. In this situation, the device will still act as a proxy for accessing the external link, and return the response to the client, eliminating the problem that external links (IPv4) cannot be accessed by the client upgraded to IPv6.

Configuring a Virtual Server

You can configure different protocols on different virtual servers. Currently, system supports the following protocols: HTTP, HTTPS, TCP, UDP, Any, Fast HTTP, HTTP proxy, IP and SSL stream proxy. If you configure the protocol type as HTTP, system will create an HTTP virtual server. Any means any protocol.

Different types of virtual servers have different methods to process requests:

- For HTTP, HTTPS, TCP, UDP or fast HTTP virtual servers, the device will map the addresses of multiple real servers to a single virtual server address, and forward client requests to corresponding real servers according to the SLB rules or load balance algorithm configured for the virtual server.
    - For IP virtual servers, the device will perform matching on the destination address in a client request. When the destination address matches the IP of the virtual server, the device will forward the client request to a corresponding real server according to the SLB rules or load balance algorithm configured for the virtual server, so as to achieve link load balancing.
- For HTTP proxy or SSL stream proxy virtual servers, the device will function as a proxy server to directly forward client requests to target servers. HTTP virtual servers can only forward HTTP requests, so if you want to forward HTTPS requests, you need to enable the HTTP tunnel mode. While SSL stream proxy virtual servers can directly forward HTTPS requests.

Note:

- Option configurations for Layer 4 and Layer 7 virtual servers may vary depending on different protocols. For specific configurations, see the actual page.
- When a new connection is requested, the device will, according to the message information, match the connection request with a virtual server in the following order: HTTP, HTTPS, TCP, UDP, FTP, fast HTTP, SIP-TCP, SIP-UDP, HTTP proxy and SSL stream proxy virtual servers > Any virtual servers > Direct routing > IP virtual servers > Other routing.

To configure a virtual server, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Virtual Server**.
2. Click **New** and select a protocol type from the drop-down list. Configuration options may vary depending on different protocols.

In the Basic Configuration tab of the pop-up dialog box, configure the following options:

Option	Description
Name	Specify the name of the virtual server.
Status	Configure the status of the virtual server. For the running status of the virtual server, see Viewing Running Status of a Virtual Server. The status includes: • Enable - Client requests can be received normally. • Disable - The original connections and persistence table will be deleted. If there is a new client request, the connection timeout error will pop up. • Maintain - This status can only be configured for Layer 7 virtual servers. If Maintain is configured, the original connections and persistence table will be deleted. And if there is a new client request, system will display an error message page. For more information, see the Error option.
Default Virtual Server	If no domain names are matched, the virtual server will be matched first.
IP: Port	Specify the IP address and port number of the virtual server. Click **Add**, and you can add multiple virtual server addresses as needed. Port Any means all ports. You can configure the virtual server address as an IPv6 address or IPv6 address range.
IP Address	Specify the network segment for the IP virtual server, and click **Add**. You can add multiple segments as needed, and up to 32 segments are supported. Besides, the network segment can be IP/netmask or IPv6/prefix length.
Auto SNAT	• ------: Auto SNAT will not be enabled. If both SNAT rules and auto SNAT function are configured, the former shall prevail. • Egress Interface IP: System will automatically translate the source IP

Option	Description
	address passing through the virtual server to the egress interface IP address without configuring SNAT. • TOA: System will automatically translate the source IP address passing through the virtual server to the source IP resolved from the TOA in the TCP packet. • X-Forwarded-For: System will automatically translate the source IP address passing through the virtual server to the source IP resolved from the X-Forwarded-For field in the HTTP/HTTPS message header. • X-Real-IP: System will automatically translate the source IP address passing through the virtual server to the source IP resolved from the X-Real-IP field in the HTTP/HTTPS message header. • Real Source IP: System will automatically translate the source IP address passing through the virtual server to the source IP that actually initiated the request. The priority of obtaining a real source IP is as follows: X-Forwarded-For > X-Real-IP > the source IP carried in the message. If this option is selected, system will first search for the source IP in the X-Forwarded-For field, and the found source IP will be used as the source IP that actually initiated the request. If no result is found in the X-Forwarded-For field, the X-Real-IP field will be searched, and the found source IP will be used as the source IP that actually initiated the request. If no result is found either, the source IP that comes with the message will be used as the source IP that actually initiated the request. • Header Name: System will automatically translate the source IP address passing through the virtual server to the source IP resolved from the custom Name field in the HTTP/HTTPS message header.
Data Channel	The data channel port is a listen port used by a virtual FTP server to estab-

Option	Description
Port (For FTP)	lish a data channel with a client. The default value is 20. The port mainly refers to the source port from which the FTP server initiates data connection to the client in the active mode. If the port configured here has been occupied, system will allocate another source port.
PING	Specify whether the IP address of the virtual server can be pinged to verify network connectivity. • Enable - No matter what status the virtual server is in, its IP can be pinged. The function is enabled by default. • Disable - No matter what status the virtual server is in, its IP cannot be pinged. • Selective - After enabling the function, system will decide whether the virtual server IP can be pinged according to the virtual server status. If the virtual server is "Configured Down", its IP cannot be pinged. If the virtual server is "Up" or "Maintained", its IP can be pinged.
Status Code	After specifying the connect failure action, you need to type a status code to be returned into the **Status Code** text box. The value range is 200 to 599. The default value is 503.
Connection Reuse	Select the **Enable** check box to enable the TCP connection reuse function. The function is disabled by default, indicating that the TCP connection will be closed after each request/response. Then, the AX device will connect to a real server over the HTTP 1.0 protocol. After the function is enabled, the AX device will connect to a real server over the HTTP 1.1 protocol and will adopt the persistent connection mechanism. The maximum number of requests/responses that can be made on a single TCP connection is determined by the real server. Compared with the number of client requests, the number of connections between the AX device and the real server is lesser due to connection reuse, thereby reducing the burden on the real server.

Option	Description
Server pool	Specify the default "Server Pool" on Page 50. If no valid Layer 4 or Layer 7 switching rules match the client requests, system will allocate real servers in the specified default server pool according to the balance algorithm. Select the server pool from the drop-down list. "---" means that the default server pool will not be configured.
Backup Server Pool	Specify the name of the backup server pool. If there is no available real server in the default server pool, system will use real servers in the backup server pool.
SSL Profile	Specify the name of the client SSL profile. System will decrypt the data sent between the client and the ADC device. Only HTTPS virtual servers support this function.
Server SSL Profile	Specify the name of the server SSL profile. System will encrypt the data sent between the ADC device and the real server. Only HTTP or HTTPS virtual servers support this function.

3. In the Virtual Server Configuration dialog box, click the **Advanced Configuration** tab.

Configure the following options.

Option	Description
Domain Match	If the protocol type is HTTP or HTTPS, you can configure the domain match. That is to say, a unique virtual server will be determined based on the IP, port and domain name to forward client requests. After the domain match is configured for HTTP, if the virtual servers have the same IP and port, the device will determine which virtual server will handle the HTTP requests using the domain match. After the domain match is configured for HTTPS, the device will allocate the corresponding virtual server based on the domain name information in the SSL protocol, and obtain the corresponding certificate. System supports accurate match, matching of domain names with wildcards, and regular expression match. None means no domain match.

Option	Description
	Note: Priority of the domain match: accurate match > a domain name with a wildcard prefix > a domain name with a wildcard suffix > regular expression. If no domain names are matched, system will select the virtual server that matches the default domain name.
Default Virtual Server	If no domain names are matched, the virtual server will be matched first.
L7 Content Switching	Specify the Layer 7 content switching rule for the virtual server. If multiple Layer 7 content switching rules are bound, system will match the client requests with the rules in the rule list from top to down. After a rule is matched, system will stop matching.
Access Control List	Specify the access control rule for the virtual server. If multiple access control rules are bound, system will match the client requests with the rules in the rule list from top to down. After a rule is matched, system will stop matching.
Content Rewrite	Specify the content rewrite rule for the virtual server. If multiple content rewrite rules are bound, system will match the client requests with the rules in the rule list from top to down. In this case, all content rewrite rules need to be matched. That is to say, after a rule is matched, system will continue to match the requests with all other rules. You can only rewrite HTTP and HTTPS client requests.
Host Rewrite	To configure the host rewrite, you can enter required Host/Refer/Location fields in the **Original Content** and **New Content** text boxes separately as needed.
L4 Content Switching	Specify the Layer 4 content switching rule for the virtual server. If multiple Layer 4 content switching rules are bound, system will match the client requests with the rules in the rule list from top to down. After a rule is matched, system will stop matching.
App Profile	Binds "Application Profile" on Page 98. "---" means that the option will not

Option	Description
	be configured.
Max Connections	Specify the maximum number of concurrent connections allowed for the virtual server. If the value is exceeded, new connections will not be established. The value is an integer ranging from 0 to 10,000,000. The value of 0 indicates no limitation.

Connect Failure Action	For HTTP, HTTPS or HTTP proxy virtual servers, if the number of concurrent connections reaches the maximum number of connections, new connections will not be established, and system will perform the following connect failure actions according to your configuration:
	• ------ - No failure action will be specified.
	• Response Message - system will return the specified response message after failing to establish a new connection.
	  • Message - Type a user-defined response message into the **Message** text box. The value range is 1 to 255 characters.
	• Response Page - System will return the specified response page after failing to establish a new connection.
	  • Response Page - Select a predefined or user-defined response page from the **Response Page** drop-down list. To upload a user-defined response page, click **Upload**, and in the pop-up **Page Management** dialog box, upload your file. You can upload files in HTM/HTML/JPG/PNG format, whose size should be less than 128K. You can also upload, delete or export pages by clicking the Page Management in the virtual server page. For more information, see Page Management.
	• Redirect - System will redirect to the specified new page after failing to establish a new connection.

Option	Description
	• Redirect - Type the address (beginning with http:// or https://) of the new page to which you want to redirect into the **Redirect** text box.
Surge Protection Queue Limit	For HTTP, HTTPS or HTTP proxy virtual servers, after the **Connection Rate Limit** is configured, you can configure the queue limit to protect virtual servers from the effects of traffic surge. After a new connection is generated, it will be put in the queue until the number of connections in the queue has reached the configured limit. The value is an integer ranging from 0 to 10,000,0. The value of 0 indicates no limitation, which means there is no protection against traffic surge. When the new connections have been generated, if the number of concurrent connections in the queue does not reach the limit, system will put the new connections in the queue one by one. System will handlee the first request in the queue if the rate of connection does not reach the rate limit. If the total number of connections in the queue has reached the configured limit, system will perform **Timeout Connection Action** to the new connection. For example, if "1000" is set as the rate limit, "2000" as the queue limit, "----" as the action (means that system will block the client request and return "error:403"): A client accesses 2500 requests per second. After the first second, the 2000 requests reach ADC first will be put in the queue and the last 500 requests will be blocked. During the first second, the ADC device handles the first 1000 connections in the queue. The other 1000 connections in the queue will be handled in the next second, and so forth.
Error	If the status of the Layer 7 virtual server is "Health Check Down" or "Maintained", or all real servers are unavailable, the virtual server will prompt an error after receiving a client request. The error types include: sending an error message, returning to an error page, and redirecting to a new page.

Option	Description
	• **Sending an error message** - Select **Error Message** from the drop-down list behind the **Error** option, and then customize an error message in the text box. By default, system will send the error message "Service Unavailable" and the error code "503". • **Returning to an error page** - Select **Error Page** from the drop-down list behind the **Error** option, and select a predefined or user-defined error page from the corresponding drop-down list. To upload a user-defined error page, click **Upload**, and in the pop-up **Page Management** dialog box, upload your file. You can upload files in HTM/HTML/JPG/PNG format, whose size should be less than 128K. For more information on deleting, exporting, or adding error pages, see Error Page Management. • **Redirecting to a new page** - Select **Redirect** from the drop-down list behind the **Error** option, and enter the address (beginning with http:// or https://) of the new page to which you want to redirect in the text box.
Error Code	Specify the error code. The default value is 503.
DSR	Select the check box to enable the DSR mode. Only TCP/UDP/Any supports this function. In the DSR mode, a request sent by a client to a real server will be processed by the device first, and then forwarded to the real server. However, a response returned by the real server will be sent directly to the client instead of passing through the device.
Datagram	With the Enable check box selected, when a client initiates a request, the device will perform L7 load balancing, and allocate a server based on UDP datagrams, so that client requests with the same quintuple will be distributed to different servers.

Option	Description
	• Timeout: Specify the timeout value for the device to establish a connection with the real server. If the timeout expires, the device will disconnect the UDP connection from the real server. The value range is 1 to 60 seconds. The default value is 5 seconds. Note: With the function enabled, neither the virtual server nor the real servers in its bound server pool will support Port Any, and the ALG function will be invalid.
Route Advertisement	Distributing the virtual server IP address means that the device distributes the virtual server IP to the OSPF protocol to calculate routes. In this case, when switching between data centers in the network, the traffic to the virtual server can be automatically switched, thereby improving the reliability of load balance. This function needs to be used together with OSPF's Redistribute function to take effect. • Enable - Enable the distribution function. System will always distribute the virtual server IP. • Disable - Disable the distribution function. System will not distribute the virtual server IP. This function is disabled by default. • Selective - After the function is enabled, system will decide whether to distribute the virtual server IP according to the running status of the virtual server. If the running status of the virtual server is "Configured Down/Maintained/Health Check Down", system will not distribute the virtual server IP. If the running status of the virtual server is "Up" or "Unknown", system will always distribute the virtual server IP.
Reverse Route	Enable or disable reverse route as needed: Reverse route is used for forwarding the reverse path data. A reverse path is in the opposite direction in relation to the initial data flow direction. • Enable: Force to use a reverse route. If available, the reverse route

Option	Description
	will be used to send reverse packets; otherwise the packets will be dropped. • Close: Reverse route will not be used. When reaching the device, the reverse data stream will be returned to its original route without any reverse route check. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send reverse packets; otherwise the packets will be returned to its original route.
Detect Server	When another virtual server has enabled the IP Family Detect function, select the **Enable** check box to enable the virtual server as the detect server. And enter the URL path of of this detect server in the text box. For example, an HTTP virtual server VS1 has enabled the **IP Family Detect** function and specify "http://10.10.10.12:80/a/b.html" as the URL address of the detect server. In this address, the "10.10.10.12:80" part is the address the client can reach. Then you need to configure another HTTP virtual server VS2, whose IP address is "10.10.10.12" and port number is "80". Next, enable the **Detect Server** function of VS2 and specify the URL path as "a/b.html".
Mirror Traffic	After the function is enabled, system can mirror the HTTP traffic, or decrypt and mirror the HTTPS traffic, and then forward the mirrored traffic to other devices in monitoring modes, such as DLP and IDS. Select an egress interface for the mirrored traffic from the **Interface** drop-down list. Type the destination port number of the client request into the **Destination Port** text box. The destination port you entered will replace the destination port of the mirrored packet. Type the destination MAC address of the mirrored packet into the **Destination MAC** text box.

Option	Description
Log	Select the **Enable** check box to enable the load balance logging function. Select one of the following items from the **Logging Source** drop-down list: • Source IP - System will send logs using the source IP and source port carried in the message itself. • TOA - System will send logs using the source IP (and source port) resolved from the TOA in the TCP packet. If the resolution fails, the source IP and source port carried in the packet itself will be used. • X-Forwarded-For - System will send logs using the source IP (and source port) resolved from the X-Forwarded-For field in the HTTP/HTTPS message header. If there is no resolution result, the source IP and source port carried in the message itself will be used. • X-Real-IP - System will send logs using the source IP (and source port) resolved from the X-Real-IP field in the HTTP/HTTPS message header. If there is no resolution result, the source IP and source port carried in the message itself will be used. • Real Source IP - System will send logs using the source IP (and source port) resolved from the X-Forwarded-For or X-Real-IP field in the HTTP/HTTPS message header. • Header Name - System will send logs using the source IP (and source port) resolved from the custom Name field in the HTTP/HTTPS message header. If there is no resolution result, the source IP and source port carried in the message itself will be used. To avoid the number of load balance logs generated by the device per second is too many to be saved in the database, you can customize which logs do not need to be saved. Only HTTP and HTTPS virtual servers support this function.

Option	Description
	• Exclude Method - HTTP/HTTPS logs with methods of get/put/-head/post/delete will not be saved. • Exclude File - HTTP/HTTPS logs in css/js/image/media format will not be saved. Specifically, the image types include PNG/BMP/JPEG/GIF/JPE/JPG, and the media types include FLV/SWF/MP4/MP3/AVI.
TOA Type	Specify the TOA type required when sending packets, including IPv4 and IPv6. The value range is 2 to 255. This value is used for inserting TOA, logging, auto SNAT, and session persistence.
Insert TOA	• FIN - Insert TOA for TCP packets with the FIN flag. • RST - Insert TOA for TCP packets with the RST flag. • ACK - Insert TOA for TCP packets with the ACK flag. • SYN - Insert TOA for TCP packets with the SYN flag. • PSH - Insert TOA for TCP packets with the PSH flag. • URG - Insert TOA for TCP packets with the URG flag. • Select All - Insert TOA for TCP packets with all flags.
HTTP Tunnel Mode	If the protocol type is HTTP Proxy, the device can function as a proxy server to forward HTTP packets to the requested target server. If you want to forward HTTPS packets, you need to enable the HTTP tunnel mode. After the mode is enabled, the device will establish a tunnel connection between the client and the target server, and forward HTTPS packets via the tunnel.
DNS Server	If the protocol type is HTTP Proxy or SSL Stream Proxy, you can customize a DNS server with an IPv4 or IPv6 address. The maximum number of DNS servers you can customize is 6. By default, the DNS server configured in system will be used.

Option	Description
IPv6 DNS Query	For the HTTP proxy or SSL stream proxy virtual server, system supports to send DNS requests to query IPv6 addresses. The function is disabled by default.
DNS TTL	For the HTTP proxy or SSL stream proxy virtual server, you can specify the amount time that the DNS response will be cached on the device. After the specified TTL expires, system will reinitiate DNS requests. The value range is 0 to 3600 seconds. The default value is 0, which means that the TTL in the response is used as the cache time. Because the TTL is short, it is recommended to modify it to avoid frequently initiating DNS requests.

4. Select an HTTP/HTTPS/HTTP-Proxy virtual server from the virtual server list, and click **Edit**. In the Virtual Server Configuration dialog box, click the **External Link Rewrite** tab. For the HTTP/HTTPS virtual server, system can rewrite external links based on URL path and domain name. For the HTTP Proxy virtual server, system only can rewrite external links based on the URL path.

   Configure the following options for external link rewrite based on the URL path.

Option	Description
External Link Rewrite	Select the **Enable** check box to enable the external link rewrite function.
Rewrite Type	Select the **Path** option button, system will rewrite the URL path of external links.
Type	Specify the type of the virtual server used by the client to access external links. • Type of Virtual Server: The same virtual server type as the virtual server you are editing will be used. • HTTPS: An HTTPS virtual server will be used. • HTTP: An HTTP virtual server will be used.
External Link Prefix	Specify the link prefix for rewriting external links. The value range is 1 to 63 characters.

Option	Description
IP Family Detect	Select the **Enable** check box and enter the IPv4 address for detect URL to enable this function. After the function is enabled, the client accesses request to the specified website. According to the response returned by the website, the client will carry a cookie which marks whether the client can support both IPv4 and IPv6 when accessing request the next time. If the client supports both IPv6 and IPv4, system will not perform external link rewrite function; otherwise the external links(IPv4) will be rewriten. **Notes**: This function will not work if the specified website does not support cross-domain. Therefore, you can enable the Detect Server function of another virtual server and specify an IPv4 address and port number provided by the client. The client can access the virtual server which works as the detect website successfully so that the **IP Family Detect function** can work.
Recursive Rewrite	Select the **Enable** check box to enable the recursive rewrite function. With this function enabled, if the client accesses the rewritten external link, and the returned response still contains an external link (IPv4), the device will continue to rewrite the response.
Content Rewrite	Select the **Enable** check box to enable content rewrite for responses from external links. With a content rewrite rule configured for an HTTP/HTTPS/http-proxy virtual server, the device will match the response received from an external link with the rule, and return the rewritten response to the client.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Import External Link Detection</td><td>Click the button, and the External Link List dialog box will appear. Configure the following options.
<table>
<tr><td>Option</td><td>Description</td></tr>
<tr><td>Discovery Mode</td><td>Specify the mode for external link detection, including All URL and Hyper Link Only. All URL refers to external links starting with "http://, "https:// and "//, while Hyper Link Only refers to external links starting with href="http://, href="https:// and href="//.</td></tr>
<tr><td>Domain Name Filter</td><td>Type the domain name for filtering external links into the text box, click Query, and system will display the external links that contain the domain name in the list below. To restore the list to the status before filtering, click Clear Filters.</td></tr>
<tr><td>Enable External Link Discovery</td><td>Click the button to enable the external link discovery function. If enabled, when the real server returns a response page to the client, system will automatically detect whether the page contains external links (IPv4), and display the found external links in the list below. The list will be refreshed every 10 seconds, which will consume system resources. To disable the function, click Disable External Link Discovery.</td></tr>
<tr><td>Clear All</td><td>Click the button to clear the external links that have been added to the external link rewrite list and saved from the list below. When detected again, the cleared external links will no longer be displayed.</td></tr>
<tr><td>Add</td><td>Select one or more found external links from the list, and click Add to add it or them to the external link rewrite list.</td></tr>
<tr><td>Close</td><td>Click Close to close the External Link List dialog box.</td></tr>
</table></td></tr>
</table>

Option	Description
Save External Link Configuration	Click the button, and system will save the external link rewrite configuration.
External Link Rewrite list	The list contains external links added from the external link list. To delete an external link, select it and click -; to add an external link manually, click +. • Type: Specify the protocol type to which system will rewrite that of external links, including "-----", HTTP and HTTPS. "-----" means to stick to the original protocol type of the external links. • Domain: Specify the domain name for external links. System will rewrite the external links that contain the domain name. For example, if "HTTPS" is selected as the type, "www.baidu.com" as the domain name, "ax_proxy" as the external link prefix, and "HTTP" as the type of the virtual server for accessing external links: when a client requests to access the virtual server (http://[2000::8]:9999/index.com), the response returned by a real server to the client contains an external link (IPv4), and the external link address contains "www.baidu.com", system will rewrite the link to "http://[2000::8]:9999/ax_proxy.https.www.baidu.com/index.html".

Configure the following options for external link rewrite based on the domain name.

Option	Description
External Link Rewrite	Select the **Enable** check box to enable the external link rewrite function.
Rewrite Type	Select the **Domain** option button. Then you need to use the corresponding aRule scripts for the virtual server, so that system can rewrite the domain name of external links. You can configure the parameters when writing the scripts, such as the white list of external links. System provides predefined script files "external-link-domain-http.lua" and "external-link-domain-https.lua" for reference. You can edit and use the predefined script files as

Option	Description
	needed. For more information on scripts, refer to aRule.
Type	Specify the type of the virtual server used by the client to access external links. • Type of Virtual Server: The same virtual server type as the virtual server you are editing will be used. • HTTPS: An HTTPS virtual server will be used. • HTTP: An HTTP virtual server will be used.
External Link Prefix	Specify the link prefix for rewriting external links. The value range is 1 to 63 characters. The new domain name of the external link will consist of the configured domain, link prefix and the original domain name of the external link. And then system returns the external link with new domain names to clients.
IP Family Detect	Select the **Enable** check box and enter the IPv4 address whcih is the address of a detect servern. After the function is enabled, the client accesses detect requests to the detect server. According to the response returned by the website, the client will carry a cookie which marks whether the client can access IPv6 address or both IPv4 and IPv6 addresses when the client accesses request the next time. If the client supports both IPv6 and IPv4, system will not perform external link rewrite function; otherwise the external links(IPv4) will be rewriten.If the client can only access IPv6 addresses, system will perform the external link rewrite function. If the client can access both IPv6 and IPv4 addresses, system will not perform the external link rewrite function. **Notes**: This function will not work if the specified website does not support cross-domain access. Therefore, you can configure another virtual server according to the reachable IPv4 address and port number provided by the client, and then enable the Detect Server function of this virtual server.

Option	Description
Domain	Specify the domain name for the virtual server. If the client uses the HTTP virtual server to access external links, system will rewrite the domain name of external links to the following format: the original domain name.External Link Prefix. Domain. If the client uses the HTTPS virtual server to access external links, system will rewrite the domain name of external links to the following format: the original domain name - External Link Prefix - Domain, and meanwhile rewrite the "." in the original domain name to "-". For example, if "HTTPS" is selected as the type of the virtual server for accessing external links, "ax_proxy" as the external link prefix and "www.baidu.com" as the domain name. In the scenario, if a client requests to access the virtual server and the response returned by a real server to the client contains an IPv4 external link (IPv4) "https://www.baidu.com", system will rewrite this link to "http://www.baidu.-com.proxy.www.ax.com/?proxy_scheme=https&proxy_port=443".

5. Click **Save**.

Viewing Running Status of a Virtual Server

After completing the configuration, you can view the running status of a virtual server in the virtual server list. The running status of the virtual server is determined by the status of the server pool, backup server pool and SLB Layer 4/7 content switching rules, and the configured status of the virtual server, including:

- : Indicates that the running status is "Up".

  If the virtual server is assigned with an IP and configured as "Enable", and at least one of the configured server pool, backup server pool and Layer 4/7 content switching rules is in "Up" status, the running status of the virtual server will be "Up".

- : Indicates that the running status is "Health Check Down".

  If the virtual server is assigned with an IP and configured as "Enable", and the configured server pool, backup server pool and Layer 4/7 content switching rules are all in "Health Check Down" status, the running status of the virtual server will be "Health Check Down". Or if the virtual server is not assigned with an IP, or the default server pool, backup

server pool and Layer 4/7 content switching rules are not configured, the running status of the virtual server will be "Health Check Down" too.

- : Indicates that the running status is "Unknown".

  If the virtual server is assigned with an IP and configured as "Enable", none of the configured server pool, backup server pool and Layer 4/7 content switching rules is in "Up" status, and at least one of them is in "Unknown" status, the running status of the virtual server will be "Unknown".

- : Indicates that the running status is "Configured Down".

  If the virtual server is configured as "Disable", its running status will be "Configured Down".

- : Indicates that the running status is "Maintained".

  If the virtual server is configured as "Maintain", the running status of the virtual server will be "Maintained".

- : Indicates that the running status is "Manual Resume".

  If the virtual server is assigned with an IP and configured as "Enable", and the configured server pool is in "Manual Resume" status, the running status of the virtual server will be "Manual Resume".

Sorting Virtual Servers

To sort virtual servers, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Virtual Server**.
2. In the virtual server list, click the header "Name", "Protocol Type", "IP", "Port", "Server Pool", "Backup Server Pool" or "Running Status" as needed, the content in the corresponding column will be automatically sorted. means the ascending order, and means the descending order.

Note:

1. The sorting order from small to large is: special characters < numbers < uppercase letters < lower-case letters < Chinese characters.
2. Because the virtual server can be assigned with multiple IP addresses and port numbers, the smallest IP address of the virtual server will be used as the basis for sorting. When sorting by IP address segments, the order from small to large is: No IP assigned < IPv4 address < IPv6 address. For

example, if vs1 is assigned with two IPs of 2.1.1.1 and 2001::5, while vs2 is assigned with two IPs of 11.1.1.1 and 1.1.1.1. Then, the two virtual servers will be sorted by their respective smallest IP, that is, 2.1.1.1 for vs1, and 1.1.1.1 for vs2, so the order is vs2 < vs1.

3. The empty value means that it is the smallest when sorting.

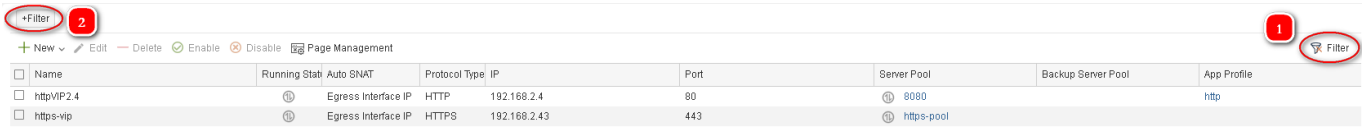
Searching Virtual Servers

You can search for virtual servers by the set filter conditions. The filter conditions include the name, protocol type, IP and port.

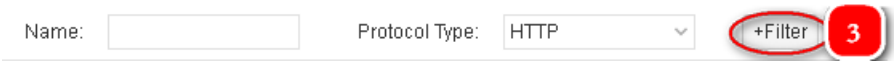
To search virtual servers, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Virtual Server**.

2. In the virtual server list, click Filter at the top-right corner, and then click **+Filter**.



3. In the pop-up drop-down list, select the filter condition you want to apply, such as Name. If you need to select multiple filter conditions, continue to click **+Filter** to add a filter condition.



4. The virtual servers met the condition(s) will be displayed in the virtual server list.

Page Management

If the running status of the virtual server is "Health Check Down" or "Maintained", or all real servers are unavailable, the virtual server will return an page according to your configuration after receiving a client request. There are 14 pages predefined in system, including 200-zh.html, 200-en.html, 301-zh.html, 301-en.html, 302-zh.html, 302-en.html, 403-zh.html, 403-en.html, 404-zh.html, 404-en.html, 50x-zh.html, 50x-en.html, maintain-zh.html and maintain-en.html. Among them, those with -en in the name are English pages, and those with -zh in the name are Chinese pages. The predefined pages cannot be deleted. You can also create pages as needed, which can be in HTM/HTML/JPG/PNG format.

To manage pages, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Virtual Server**.
2. In the virtual server page, click **Page Management**, and the **Page Management** dialog box will appear.
3. Then, you can do the following:
   - **Upload a user-defined page**: Click **Browse**, select the file in HTML/HTM/JPG/PNG format in your PC, and click **Upload**. You can only upload files less than 128K. After uploading successfully, the new page will be displayed in the page list.
   - **Export the created error page(s)**: In the page list, select one or more pages, and click **Export** to export the selected page(s) to your PC.
   - **Delete the error page(s)**: In the page list, select one or more pages, and click **Delete** to delete the selected page(s).
4. Click **Close**.

Server Pool

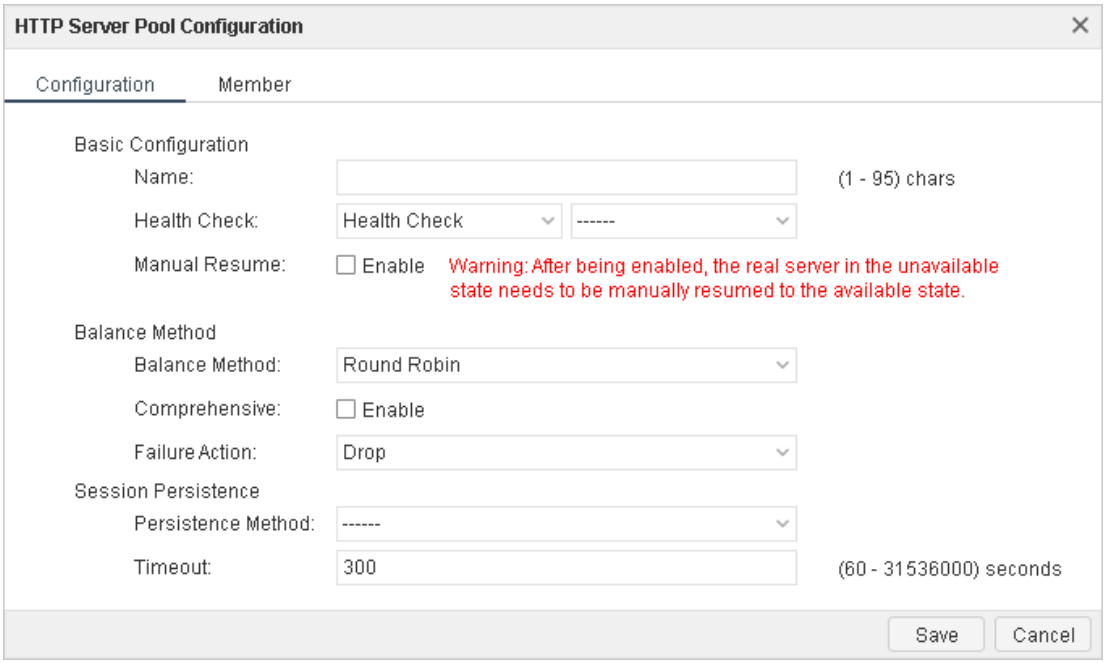
A server pool is a group of real servers provide the same services. Load balance refers to the process of balancing multiple real servers in the server pool by using different load balance algorithms.

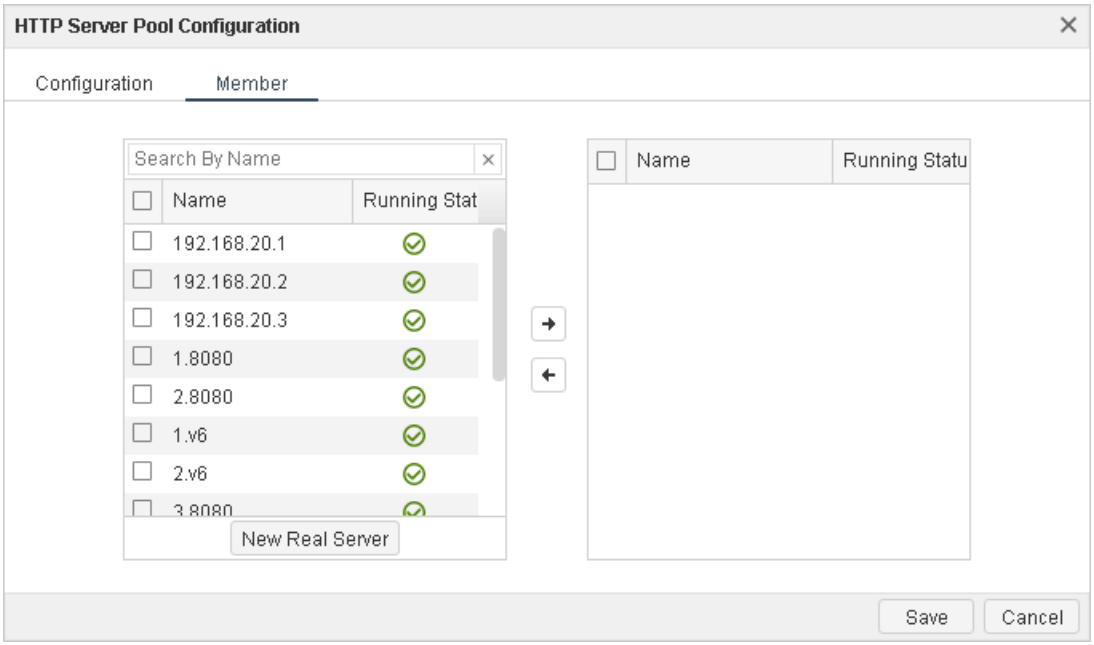
The server pool supports binding IPv4 real servers, IPv6 real servers, or a mixture of the two types of real servers.

Configuring a Server Pool

To configure a server pool, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Server Pool**.
2. Click **New**, and select a protocol type from the drop-down list. A server pool configuration dialog box will appear. For example, if you specify HTTP as the protocol type, the server pool will distribute HTTP requests. Option configurations for Layer 4 and Layer 7 server pools may vary depending on different protocols. For specific configurations, see the actual page.





In the Configuration tab of the pop-up dialog box, configure the following options:

Option	Description
Name	Specify the name of the server pool.
Health Check	Select a health check or health check group.

Option	Description
Manual Resume	Select the **Enable** check box to enable the manual resume function. With this function enabled, if the health check status changes from "Unavailable" to "Available", the running status of the server pool will be "Manual Resume". **Note**: • The real server in the unavailable state in the server pool needs to be manually resumed to the available state. For the method of manually resuming the running status, see Manually Resuming the Running Status. • If the running status of the server pool is "Manual Resume", the status of the configured virtual server, backup server pool and L4/L7 content switching rules will change to "Manual Resume" too.
Balance Method	Specify a load balance algorithm. After the parameter is configured, system will distribute the requests across the server pool according to the specified algorithm. For more information on load balance algorithms, see Load Balance Algorithm. If the specified algorithm is IP Hash, Weighted IP Hash, IP-Port Hash, or Weighted IP-Port Hash, specify how many first bits of the Source IP or the Real Source IP obtained from a client request will be hashed in the **Hash Bits** text box. The value range is 0 to 128. The default value is 128. The value of 0 means no load balance. This option is only effective for HTTP, HTTPS or Fast HTTP server pools. Note: If the specified algorithm is IP Hash, the load balance can be performed based on the source IPv4 or IPv6 addresses.
Comprehensive	Select the **Enable** check box to enable the Comprehensive function. With this function enabled, if the specified algorithm is Round Robin or Weighted Round Robin, system will perform load balancing based on the scheduling results of real servers by scripts, L7 Content Switching, L4 Content Switch-

Option	Description
	ing, Session Persistence and other balance methods. System will determine the performance of each real server according to its current capacity. Then, after receiving new client requests, the device will first distribute the requests to the real servers with better performance in turn.
Failure Action	After the client initiates a request, if the real server does not respond, system will perform the following failure actions: • Drop - Drops the client request and does not respond. • Retry - System will retry to initiate a connection to the real server until the specified retry times is reached. • Retry and reselect - System will retry to initiate a connection to the real server until the specified retry times is reached. If retrying fails, a real server will be reselected. • Reselect - Reselects a real server.
Persistence Method	To maintain the continuity and consistency of a session, the device supports the session persistence function. By configuring a session persistence method, the device will always distribute client requests carrying the specified persistence feature to the same server as that of the client accessed for the first time instead of multiple servers, thereby ensuring session persistence. According to different applications, you can configure different session persistence methods, including: • ---: Session persistence will not be enabled. • **Source IP**: Sends client requests (including all subsequent connection requests) from the same source IP address to the same real server. Both IPv4 and IPv6 addresses are supported. • IPv4 Granularity: Specify the granularity (i.e., netmask) of the IPv4 address. The value range is 1 to 32. The default value is

Option	Description
	32. • IPv6 Granularity: Specify the granularity (i.e., prefix length) of the IPv6 address. The value range is 1 to 128. The default value is 128. • **URL Hash**: Obtains a string from the HTTP URL path or URL parameter value in a client request for hashing. The request carrying the string will be distributed to the same server as that of the client accessed for the first time. Type the URL parameter name into the **URL Param** text box, and system will obtain a string from the parameter value. If the parameter not specified, a string will be obtained from the URL path. Click , and type values into the **Start** and **End** text boxes respectively to specify the position for the string in the URL path or URL parameter. • **Header Hash**: Obtains a string from the HTTP header of a client request for hashing. The request carrying the string will be distributed to the same server as that of the client accessed for the first time. Type the name of the header into the **Header Name** text box. Click , and type values into the **Start** and **End** text boxes respectively to specify the position for the header string. • **Cookie Hash**: Obtains a string from the HTTP cookie of a client request for hashing. The request carrying the string will be distributed to the same server as that of the client accessed for the first time: • Cookie Name: Specify the name of the HTTP cookie. Then, system will obtain the specified HTTP cookie from a client request. The request carrying the cookie will be distributed to the same server as that of the client accessed for the first time. • Encryption: Select the **Enable** check box to enable cookie

Option	Description
	encryption, and specify a password which will be encrypted by AES. Then, system will encrypt the specified cookie in the client request. When the client initiates a request again, system will decrypt the cookie: if the decryption is successful, the request will be distributed to the same server as that of the client accessed for the first time; if the decryption fails, the session will be non-persistent. • Accept Plaintext: Select the **Enable** check box to enable the accept plaintext function. With this function enabled, after failing to decrypt the cookie, system will consider the encrypted cookie as plaintext and use it to ensure session persistence. • **Insert Cookie**: For an HTTP request passing through the device, the device will insert a cookie into the response. The request carrying the cookie will be distributed to the same server as that of the client accessed for the first time. • Cookie Name: Specify the name of the HTTP cookie. If the name is not specified, system will use the ID (such as SLBServerPool3) of the current address pool as the default cookie and insert it into the request. • Domain: Specify a domain name to be matched. The client request that matches with it will be inserted with the cookie, and the session will be persistent. • Path: Specify a URL path to be matched. The client request that matches with it will be inserted with the cookie, and the session will be persistent. • Session Cookie: Select the **Enable** check box to enable the session cookie function. With this function enabled, the inserted

Option	Description
	cookie will not be stored on the client's disk and does not contain an expiration date. As long as the browser is open, the session will be persistent. However, when the browser is closed, the cookie will be permanently lost. If the function is not enabled, the inserted cookie will be stored on the client's disk. In this case, closing the browser does not close the session, and the session will only be removed from the client's disk when the cookie times out. • Cookie Expiration: If the session cookie is not enabled, you need to specify the cookie timeout. The value range is 1 to 31536000 seconds. The default value is 300. If the timeout expires, the cookie will be removed from the client's disk. Then the client will no longer carry the cookie when sending messages, and the session will be non-persistent. • No Pass To Real Server: With the **Enable** check box selected, the inserted cookie will not be passed through to the real server. • Encryption: Select the **Enable** check box to enable cookie encryption, and specify a password which will be encrypted by AES. Then, system will encrypt the inserted cookie. When the client initiates a request again, system will decrypt the cookie: if the decryption is successful, the request will be distributed to the same server as that of the client accessed for the first time; if the decryption fails, the session will not be non-persistent. • Accept Plaintext: Select the **Enable** check box to enable the accept plaintext function. With this function enabled, after failing to decrypt the cookie, system will consider the encrypted cookie as plaintext and use it to ensure session persistence. • **SSL ID**: Obtains an SSL ID from an HTTPS client request. The

Option	Description

	request carrying the ID will be distributed to the same server as that of the client accessed for the first time.
	• **Request Method**: Obtains the request method from a client request. The request carrying the method will be distributed to the same server as that of the client accessed for the first time.
	• **HTTP Version**: Obtains the HTTP version number from a client request. The request carrying the number will be distributed to the same server as that of the client accessed for the first time.
	• **Real Source IP**: Obtains the real source IP from a client request. The request carrying the source IP will be distributed to the same server as that of the client accessed for the first time. The priority of obtaining a real source IP is as follows: X-Forwarded-For > X-Real-IP > the source IP carried in the message. If this option is selected, system will first search for the source IP in the X-Forwarded-For field, and the found source IP will be used as the source IP that actually initiated the request. If no result is found in the X-Forwarded-For field, the X-Real-IP field will be searched, and the found source IP will be used as the source IP that actually initiated the request. If no result is found either, the source IP that comes with the message will be used as the source IP that actually initiated the request.
	  • IPv4 Granularity: Specify the granularity (i.e., netmask) of the IPv4 address. The value range is 1 to 32. The default value is 32.
	  • IPv6 Granularity: Specify the granularity (i.e., prefix length) of the IPv6 address. The value range is 1 to 128. The default value is 128.
	• **TOA**: Obtains the TOA from a TCP request of a client. The request

Option	Description
	carrying the TOA value will be distributed to the same server as that of the client accessed for the first time. • IPv4 Granularity: Specify the granularity (i.e., netmask) of the IPv4 address. The value range is 1 to 32. The default value is 32. • IPv6 Granularity: Specify the granularity (i.e., prefix length) of the IPv6 address. The value range is 1 to 128. The default value is 128. • **TOA or Source IP (TOA First)**: Obtains the TOA or source IP from a TCP request of a client, of which the TOA will be obtained first. The request carrying the value will be distributed to the same server as that of the client accessed for the first time. • IPv4 Granularity: Specify the granularity (i.e., netmask) of the IPv4 address. The value range is 1 to 32. The default value is 32. • IPv6 Granularity: Specify the granularity (i.e., prefix length) of the IPv6 address. The value range is 1 to 128. The default value is 128. • **URL** : Obtains a string from the HTTP URL path or URL parameter value in a client request. The request carrying the string will be distributed to the same server as that of the client accessed for the first time. Type the URL parameter name into the **URL Param** text box, and system will obtain a string from the parameter value. If the parameter not specified, a string will be obtained from the URL path. Click ▲, and type values into the **Start** and **End** text boxes respectively to specify the position for the string in the URL path or URL parameter.

Option	Description

	• **Header**: Obtains a string from the HTTP header of a client request. The request carrying the string will be distributed to the same server as that of the client accessed for the first time. Type the name of the header into the **Header Name** text box. Click , and type values into the **Start** and **End** text boxes respectively to specify the position for the header string.
	• **Cookie**: Obtains a string from the HTTP cookie of a client request. The request carrying the string will be distributed to the same server as that of the client accessed for the first time:
	  • Cookie Name: Specify the name of the HTTP cookie. Then, system will obtain the specified HTTP cookie from a client request. The request carrying the cookie will be distributed to the same server as that of the client accessed for the first time.
	  • Encryption: Select the **Enable** check box to enable cookie encryption, and specify a password which will be encrypted by AES. Then, system will encrypt the specified cookie in the client request. When the client initiates a request again, system will decrypt the cookie: if the decryption is successful, the request will be distributed to the same server as that of the client accessed for the first time; if the decryption fails, the session will be non-persistent.
	  • Accept Plaintext: Select the **Enable** check box to enable the accept plaintext function. With this function enabled, after failing to decrypt the cookie, system will consider the encrypted cookie as plaintext and use it to ensure session persistence.
	• SIP Call-ID: Obtains the Call-ID from a SIP request of a client. Requests carrying the Call-ID will be distributed to the same server as that of the client accessed for the first time.

Option	Description
	Note: After a client request enters the server pool, it will be matched with an entry in the session persistence table first. If an entry is matched, the device will directly allocate a real server. Otherwise, a real server will be selected according to the load balance algorithm configured in the server pool.
Match Across Virtual Server	Select the **Enable** check box to enable the match across virtual server function. With this function enabled, the session persistence table will be shared with other virtual servers. **Note**: The Insert Cookie, TOA, TOA or Source IP, and SSL ID-based session persistence methods do not support this function.
Timeout	Specify the timeout value for the session. If the timeout expires, the device will clear the session information of the client.

3. In the Member tab, add a real server to the server pool. In the member list, select the real server you want to add, and then click  to add it to the selected list. If you want to remove a real server from the server pool, select the real server from the selected list, and then click  . You can also click **New Real Server** to create a new real server as needed. Then, the newly created real server will be automatically added to the selected list.

Note: To add a real server to an IP virtual server pool, you should ensure that the IP address of the server is on the same network segment as that of the device.

4. Click **Save**.

Viewing Running Status of a Server Pool

After completing the configuration, you can view the running status of each server pool in the server pool list. The server pool status is determined by the Running Status of Real Servers in the Server Pool, including:

-  : Indicates that the running status is "Up". If the running status of at least one real server in the server pool is "Up", the server pool status will be "Up".

- : Indicates that the running status is "Health Check Down". If the running status of all real servers in the server pool is "Health Check Down" or "Configured Down", the server pool status will be "Health Check Down".
- : Indicates that the running status is "Unknown". If the running status of all real servers in the server pool is not "Up", and at least one of them is in "Unknown" or "Going Down" status, the server pool status will be "Unknown".
- : Indicates that the running status is "Manual Resume". If the Manual Resume function is enabled and the health check status changes from "Unavailable" to "Available", the server pool status will be "Manual Resume".

Running Status of Real Servers in the Server Pool

The status of a server pool is determined by the running status of real servers in the pool, which is different from that of the real servers (see Viewing Running Status of a Real Server). The running status of the real servers in the pool is related to their configured status and health check status, including Up, Unknown, Configured Down, Health Check Down, Going Down and Manual Resume:

- When a real server is configured as "Enable":
  - If no health check is configured, the status of the real server in the server pool will be "Unknown";
  - If the health check status is "Available", the status of the real server in the server pool will be "Up";
  - If the health check status is "Unavailable", the status of the real server in the server pool will be "Health Check Down";
  - If the health check status changes from "Unavailable" to "Available" and the Manual Resume function is enabled for the server pool, the status of the real server in the server pool will be "Manual Resume".
- When a real server is configured as "Disable", no health check instance of the real server will be generated regardless of whether the real server or the server pool to which it belongs is configured with a health check. In this case, the status of the real server in the server pool will be "Configured Down".
  - When a real server is configured as "Waiting Down (Clear Persistence)", no health check instance of the real server will be generated regardless of whether the real server or the server pool to which it belongs is configured with a health check. In this case, the status of the real server in the server pool includes:
    - "Going Down" before all sessions related to the real server are closed.
    - "Configured Down" after all sessions related to the real server are closed.

- When a real server is configured as "Waiting Down (Wait For Persistence To Be Aged Out)", no health check instance of the real server will be generated regardless of whether the real server or the server pool to which it belongs is configured with a health check. In this case, the status of the real server in the server pool includes:
    - "Going Down" before all sessions related to the real server are closed and all persistence tables are aged.
    - "Configured Down" after all sessions related to the real server are closed and all persistence tables are aged.

Manually Resuming the Running Status

To manually resume the running status, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Server Pool**.
2. In the server pool list, select the server pool whose running status is displayed as , and click in the Restore column. Then the running status of the server pool will change according to the current health check status, and the status of all real servers in the server pool will be changed accordingly:
    - If the health check status is "Available", the running status of the server pool will change from "Manual Resume" to "Up".
    - If the health check status is "Unavailable", the running status of the server pool will change from "Manual Resume" to "Health Check Down".
3. To manually resume the running status of a real server in the server pool, click "+" in front of the server pool, select the real server that needs to be manually resumed in the expanded list, and click in the Restore column. Then the running status of the real server will change according to the current health check status:
    - If the health check status is "Available", the running status of the real server in the server pool will change from "Manual Resume" to "Up";
    - If the health check status is "Unavailable", the running status of the real server in the server pool will change from "Manual Resume" to "Health Check Down".

Viewing Status Statistics of Real Servers in the Server Pool

To view the status statistics of real servers in the server pool, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Server Pool**.

2. In the server pool list, click the "+" in front of the server pool you want to view its statistics, the status statistics of the real servers in the server pool will be expanded. The page is shown as below:

3. Click the "-" in front of the server pool, the statistics will be collapsed.

Sorting Server Pools

To sort server pools, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Server Pool**.

2. In the server pool list, click the header "Name", "Protocol Type", "Balance Method", "Session Persistence", "Health Check" or "Running Status" as needed, the content in the corresponding column will be automatically sorted. ▲ means the ascending order, and ▼ means the descending order.

Note:

1. The sorting order from small to large is: special characters < numbers < uppercase letters < lower-case letters < Chinese characters.

2. The empty value means that it is the smallest when sorting.

Searching Server Pools

You can search for server pools by the set filter conditions, including the name, protocol type, real server and balance method. The method of searching server pools is the same as that of virtual servers, see "Searching Virtual Servers" on Page 49.

Load Balance Algorithm

System supports multiple load balance algorithms, including:

Algorithm	Description
Round Robin	Client requests will be distributed to each real server in a queue in turn.
Weighted Round Robin	According to their performance, real servers will be given different weights. The device will distribute client requests in proportion to weights of real servers. The real server with higher weight will receive a higher proportion of requests.
IP Hash	First, the source address of a client will be hashed. Then, the client will be allocated to a real server according to the hash value. If the server list remains unchanged, clients on the same IP address will be allocated to the same real server every time.
Weighted IP Hash	Based on the IP Hash algorithm, the device will distribute client requests in proportion to weights of real servers. The real server with higher weight will receive a higher proportion of requests.
IP-Port Hash	First, the IP address and port number of the client will be hashed. Then, the client will be allocated to a real server according to the hash value.
Weighted IP-Port Hash	Based on the IP-Port Hash algorithm, the device will distribute client requests in proportion to weights of real servers. The real server with higher weight will receive a higher proportion of requests.
Consistent IP Hash	First, the source address of a client will be hashed. Then, the client will be allocated to a real server according to the hash value. If a real server fails to function due to a fault or other reasons, the requests originally sent to the failed real server will be redistributed to other available real servers; and the requests (from the same source IP or the same client) originally sent to the real servers without failure will not be redistributed.
Least Connection	The device will record the number of connections on each real server or port. After a new connection is generated, the device will distribute it to the real server with the fewest active connections.
Weighted Least Connection	Based on the least connection algorithm, each real server will be given a weight according to its performance. The weight indicates the performance of each real server. After a new connection is generated, the latest request will be distributed to the real server with the smallest ratio of the number of active connections to the weight (Calculation

Algorithm	Description
	method: dividing the current number of connections by the weight).
Fastest Response	The device will record the number of connections on each real server or port. After a new connection is generated, the device will distribute it to the real server with the fastest response time.
Priority	Requests will be distributed to a real server with the highest priority. The smaller the priority value is, the higher the priority of the real server will be. If there are multiple real servers with the same highest priority, resources will be allocated by round robin among these real servers.
Dynamic Ratio	According to the different processing capabilities of real servers, the device calculates different dynamic weights. The device will distribute client requests in proportion to dynamic weights of real servers. The real server with higher dynamic weight will receive a higher proportion of requests. If the dynamic weight is 0, the real server will not be distributed with requests. In general, the dynamic weight value is calculated by the SNMP health check; in other cases, the value of 1 means that the real server can provide services, while 0 means it is unavailable.
Least Bandwidth	The device will record the sum of upstream and downstream bandwidth on each real server or port. When a new connection is requested, the device will distribute it to the real server with the least sum.
Weighted Least Bandwidth	Based on the least bandwidth algorithm, each real server will be given a weight according to its performance. The weight indicates the performance of each real server. When a new connection is requested, the latest request will be distributed to the real server with the smallest ratio of the sum to the weight (Calculation method: dividing the sum by the weight).

Real Server

A real server is a dedicated physical server which is deployed in the user's network environment and responsible for processing client requests.

You can configure an IP address or a domain name for a real server, and both IPv4 and IPv6 are supported.

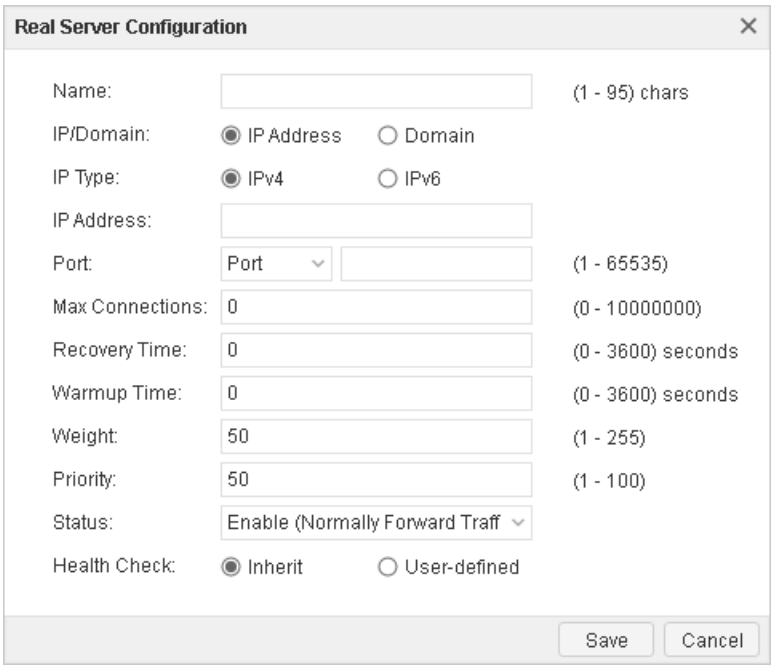
If a domain name is specified, system will create a real server (i.e., the parent real server), and will use the IP address(es) resolved from the domain name to create one or more sibling real server(s) (usually named "--IP of the sibling real server-@name of the parent real server"). You can choose to resolve the first IP or all IPs to create one or more sibling real server (s). If the IP(s) resolved from the domain name change(s), system will automatically update the sibling real server(s). For a non-existent IP, its corresponding sibling real server will be deleted; for a newly resolved IP, system will automatically create a sibling real server, thereby eliminating frequent configuration changes caused by IP changes of the real server.

Note: For the specified domain name, the device will resolve it using the DNS server in system, so you need to configure the DNS server in advance. For more information, refer to Object > DNS > DNS Server.

Configuring a Real Server

To configure a real server, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Real Server**.
2. Click **New**, and the Real Server Configuration dialog box will appear.



Configure the following options.

Option	Description
Name	Specify the name of the real server.
IP/Domain	Select **IP Address** or **Domain**, and then configure the specific IP or domain name in the options below.
IP Type	If IP Address is selected, specify the IP type for the real server. Both IPv4 and IPv6 are supported.
IP Address	If IP Address is selected, specify the IP Address for the real server.
Domain Type	If Domain is selected, specify the domain name type for the real server. Both IPv4 and IPv6 are supported. If IPv4 is selected, system will resolve the A record for the specified domain name, and create one or more sibling real server(s) according to the resolution result; if IPv6 is selected, system will resolve the AAAA record for the specified domain name, and create one or more sibling real server(s) according to the resolution result.
Domain	If Domain is selected, specify the domain name for the real server. The length range is 1 to 254 characters.
Port	Specify the number of the port on which the real server listens for client requests. The value range is 1 to 65535.
Auto Populate	If Domain is selected, you can choose to automatically resolve All IP or First IP to create one or more sibling real server(s). If All IP is selected, system will create sibling real servers using all resolved IPs, and each real server supports to create up to 16 sibling real servers; if First IP is selected, system will create a sibling real server using the first resolved IP.
Max Connections	Specify the maximum number of concurrent connections allowed for the real server. The value is an integer ranging from 0 to 10,000,000. You can set the value of the maximum connections according to the performance of the real server. If the value is exceeded, connections between the excess requests and the real server will not be established. The value of 0 indicates no limitation.
Recovery Time	Specify the recovery period of the real server. After the health check is

Option	Description
	configured, and when the running status of the real server changes from down to up, the real server will immediately enter the recovery period. Within the recovery period, the real server will not receive client requests. After the recovery period ends, the real server will enter the warmup period. You can set the recovery period according to the performance of the server. The value range is 0 to 3600 seconds. The default value is 0 seconds, which means that the real server does not need the warmup period and will directly enter the warmup period.
Warmup Time	After the recovery period ends, the ADC device will enter the warmup period. Within the specified warmup period, the real server will respond to part of client requests. After the warmup period ends, the real server will respond to all the client requests until the maximum number of connections is reached. You can set the warmup period according to the performance of the server. The value range is 0 to 3600 seconds. The default value is 300 seconds. The value of 0 means that system does not need the warmup period, and will respond to the client requests immediately after the recovery period ends until the maximum number of connections is reached.
Weight	Specify the weight of the real server. You can assign different weights to real servers, so that they can receive client requests in proportion to their respective weights. For example, servers with low-end configuration and high loads should be given lower weights to reduce their loads.
Priority	Specify the priority of the real server. The value range is 1 to 100. The default value is 50. The smaller the value is, the higher the priority of the real server will be.
Status	Configure the status of the real server. For the running status of the real server, see Viewing Running Status of a Real Server. The status includes:

Option	Description
	• Enable (Normally Forward Traffic) - If the real server is enabled, client requests can be received normally. • Disable (Drop All Traffic) - If the real server is disabled, the original connections will be deleted and cannot function anymore, and no new connection requests from clients will be received. • Waiting Down (Clear Persistence) - If the real server is in this status, the original connections will remain available. System will immediately delete the persistence table, and no longer receive new requests. • Waiting Down (Wait For Persistence To Be Aged Out) - If the real server is in this status, the original connections and session persistence will remain available. When the persistence table is aging, and if a new client request matches the persistence table, the request will be forwarded to the real server. System will no longer receive new connection requests that do not match the persistence table to ensure that ongoing services will not be interrupted.
Health Check	• Inherit - Inherit the health check configuration of the server pool. • User-defined - Select a health check or health check group.

3. Click **Save**.

Note:

- When creating a real server, you cannot specify the IP and domain name for a real server at the same time. Besides, "@" cannot be included in the real server name.
- When configuring a domain name for a real server, if the status of the parent real server is "Configured Down", system will still perform resolution and create a sibling real server.

- A sibling real server has a separate running status and health check status, while shares other attributes with the parent real server, including health check, port, weight, priority, etc.
- You cannot edit and delete a sibling real server.
- For Layer 4 and Layer 7 content switching rules, you cannot specify a parent real server.
- A parent real server will not generate a health check instance, but the sibling real server will.

Viewing Running Status of a Real Server

After completing the configuration, you can view the running status of the real server in the real server list, including:

- : Indicates that the running status is "Up". If the real server is configured as "Enable" and assigned with an IP, its running status will be "Up".
- : Indicates that the running status is "Configured Down". If the real server is configured as "Disable", or if the real server is configured as "Enable" but not assigned with an IP, its running status will be "Configured Down".
- : Indicates that the running status is "Going Down". If the real server is configured as "Waiting Down (Clear Persistence)" or "Waiting Down (Wait For Persistence To Be Aged Out)", and when the original connections have not been closed or the persistence table has not been aged, its running status will be "Going Down". After the original connections are closed normally or the persistence table is aged, its running status will be "Configured Down".

Sorting Real Servers

To sort real servers, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Real Server**.
2. In the real server list, click the header "Name", "IP/Domain", "Port", "Max Connections", "Weight", "Health Check" or "Running Status" as needed, the content in the corresponding column will be automatically sorted. means the ascending order, and means the descending order.

Note:

1. The sorting order from small to large is: special characters < numbers < uppercase letters < lower-case letters < Chinese characters.
2. For IP/Domain, which can only be sorted by IP address segments, the order from small to large is: No IP assigned < IPv4 address < IPv6 address.
3. The empty value means that it is the smallest when sorting.

Searching Real Servers

You can search for real servers by the set filter conditions, including the name, IP and port. The method of searching real servers is the same as that of virtual servers, see "Searching Virtual Servers" on Page 49.

SLB Rule

The virtual server distributes client requests according to SLB rules, including HTTP content rewrite rules, Layer 4 content switching rules and Layer 7 content switching rules.

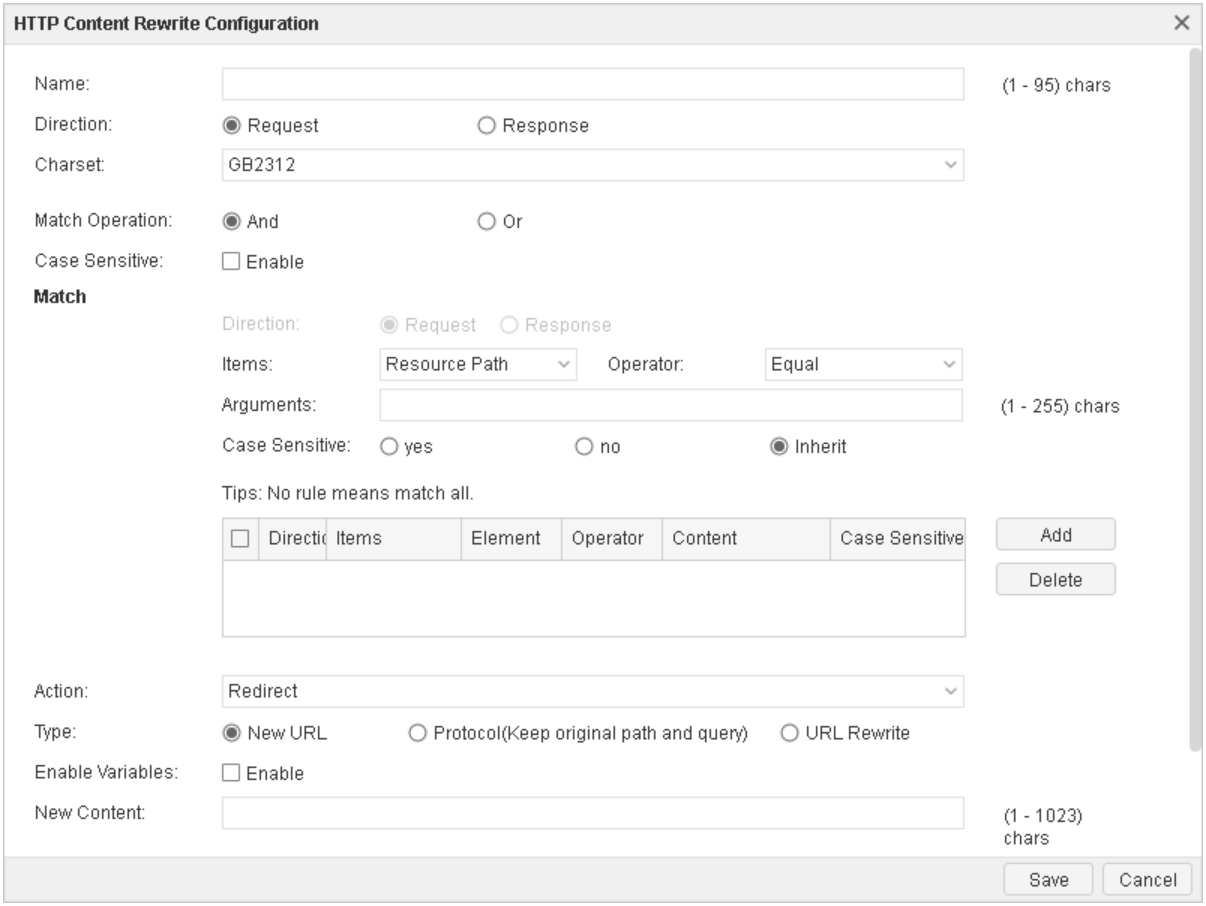
Configuring HTTP Content Rewrite Rules

System supports to rewrite the HTTP content, including the content of client requests and server responses. You can configure 16 matching conditions for a content rewrite rule. When multiple matching conditions are configured, the relationship among the conditions is "AND", i.e., all the conditions should be met before being matched.

To configure an HTTP content rewrite rule, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Rule** > **HTTP Content Rewrite**.

2. Click **New**, and the HTTP Content Rewrite Configuration dialog box will appear.



Configure the following options.

Option	Description
Name	Specify the name of the HTTP content rewrite rule.
Direction	• Request: Rewrites the content of client requests. • Response: Rewrites the response returned by real servers.
Charset	Specify the encoding method for the input characters, including GB2312, UTF-8, GBK and GB18030.
Match Operation	Specify an operator for matching conditions, including And and Or. "And" is the default option, indicating that all matching conditions need to be met;

Option	Description
	"Or" indicates that only one matching condition needs to be met.
Case Sensitive	With this check box selected, system will perform matching in a case-sensitive manner.

Match	After configuring a matching condition, click **Add**. If the configured matching condition is met, the device will rewrite the HTTP content.
	Note:
	• When the direction is "Response", the matching conditions can be applied to the content of requests or responses; and when the direction is "Request", the matching conditions can only be applied to the content of requests.
	• You can configure the Match and Action as needed to send client certificate information to the server. After a matching condition is configured with certificate information, if the condition is met by a client certificate, system will perform content rewrite.
	  • Select **X509 Cert** from the **Items** drop-down list, and then specify an element, including Issuer, Issuer Country, Issuer Organization, Issuer Organization Unit, etc.
	  • Select **SSL/TLS** from the **Items** drop-down list, and then specify an element, including Protocol, Client Verify Result, SNI, Cipher Suite, etc.

Action	System will perform an action on the HTTP content that meets a matching condition. You can select an action from the drop-down list, including: • **Redirect** - Select a radio button behind the **Type** option as needed, including: • **New URL** - Type the URL address you want to redirect to into the **New Content** text box, and type the status code returned by

Option	Description
	the device to the client into the **Status Code** text box. System will redirect the HTTP content to the specified URL address. • **Protocol (Keep original path and query)** - Modify the original protocol and port as needed, i.e., select the HTTP or HTTPS radio button, and type the port number into the **Port** text box. System will keep the original URL during an HTTP/HTTPS redirect. • **URL Rewrite** - Specify the original content and new content for the URL rewrite. System will replace the original content with the new content according to your configuration. • **Replace URL (Only path)** - Specify the address range, original content and new content for the URL rewrite. • **Replace Header** - Specify the name, value range, original content and new content of the header. System will replace the original content with the new content according to the configuration. • **Replace Body** - Specify the value range, original content and new content of the message body. System will replace the original content with the new content according to the configuration. For the rewriting of message bodies of responses, only the bodies in text format can be rewritten. • **Replace Cookie** - Specify the name, value range, original content and new content of the cookie. System will replace the original content with the new content according to the configuration. • **Delete Header** - Specify the name of the header. System will delete the specified header field. • **Delete Cookie** - Specify the name of the cookie. System will delete

Option	Description
	the specified cookie. • **Insert Header** - Specify the name and content of the header. System will insert the header field into requests or responses. • **Insert Cookie** - Specify the name and content of the cookie. System will insert the cookie field into requests or responses. • **Insert IP Family Prompt** - Modify the IPv4 text content/IPv6 text content, text position, text size, font color and background color in HTTP responses. The option takes effect only when the matching-condition direction is "Response". **Note:** For the HTTP content rewrite rules configured with the action "Insert IP Family Prompt", you can only reference one of them in the virtual server.
Enable Variables	Select the **Enable** check box to enable this function. With this function enabled, system will replace the predefined variables specified in the **New Content** text box with corresponding information, and send the replaced content to a real server.
New Content	You can add new content using predefined variables, which should follow the format of "${}" and can be combinations of letters, numbers, "." and "_ ". For more information about variables, refer to HTTP Content Rewrite_ Variable Instructions.
Description	Specify the description for the rule.

3. Click **Save**.

Note: If the Enable Variables function is enabled:

- System will perform URI encoding on the new content to avoid any unsafe characters.
- The new content for Replace Body will not be URI-encoded.

HTTP Content Rewrite_ Variable Instructions

The following table shows the variable Instructions for HTTP content rewrite.

Variable Instructions.

Variable	Description
${X509.version}	Version of the client certificate.
${X509.serial_num}	Serial number of the client certificate.
${X509.signature_algorithm}	Signature algorithm of the client certificate.
${X509.not_valid_before}	The date and time when the client certificate becomes valid.
${X509.not_valid_after}	The date and time when the client certificate is no longer considered valid.
${X509.public_key}	Public key of the client certificate.
${X509.public_key_type}	Public key type of the client certificate.
${X509.public_key_bits}	Public key length of the client certificate.
${X509.md5}	MD5 hash of the client certificate.
${X509.whole}	The client certificate itself (PEM format).
${X509.subject_dn}	Subject of the client certificate (each field should be separated by ",").
${X509.subject_dn_r}	Subject fields of the client certificate displayed in reverse order (each field should be separated by ",").
${X509.subject_dn_cn}	Common name of the client certificate subject.
${X509.subject_dn_e}	Email address included in the subject of the client certificate.

Variable	Description
${X509.subject_dn_o}	Organization name included in the subject of the client certificate.
${X509.subject_dn_ou}	Organization unit name included in the subject of the client certificate.
${X509.subject_dn_c}	Country name included in the subject of the client certificate.
${X509.subject_dn_st}	State/province name included in the subject of the client certificate.
${X509.subject_dn_l}	Town/city name included in the subject of the client certificate.
${X509.issuer_dn}	Issuer of the client certificate (each field should be separated by ",").
${X509.issuer_dn_r}	Issuer fields of the client certificate displayed in reverse order (each field should be separated by ",").
${X509.issuer_dn_cn}	Common name of the client certificate issuer.
${X509.issuer_dn_e}	Email address of the client certificate issuer.
${X509.issuer_dn_o}	Organization to which the client certificate issuer belongs.
${X509.issuer_dn_ou}	Organization unit to which the client certificate issuer belongs.
${X509.issuer_dn_c}	Country in which the client certificate issuer is located.
${X509.issuer_dn_st}	State/province in which the client certificate issuer is located.
${X509.issuer_dn_l}	Town/City in which the client certificate issuer is located.
${SSL.version}	SSL/TLS protocol version.
${SSL.cipher_id}	Negotiation algorithm ID of the SSL/TLS protocol.
${SSL.cipher_name}	Negotiation algorithm name of the SSL/TLS protocol.
${SSL.client_verify_result_code}	Error code for the client certificate verification.

Variable	Description
${SSL.client_verify_result_string}	Result of the client certificate verification.
${SSL.session_id}	SSL/TLS session ID.
${SSL.tlsext_sni}	SNI extension field of the TLS protocol.
${SSL.session_ticket_id}	SSL/TLS session ticket ID.

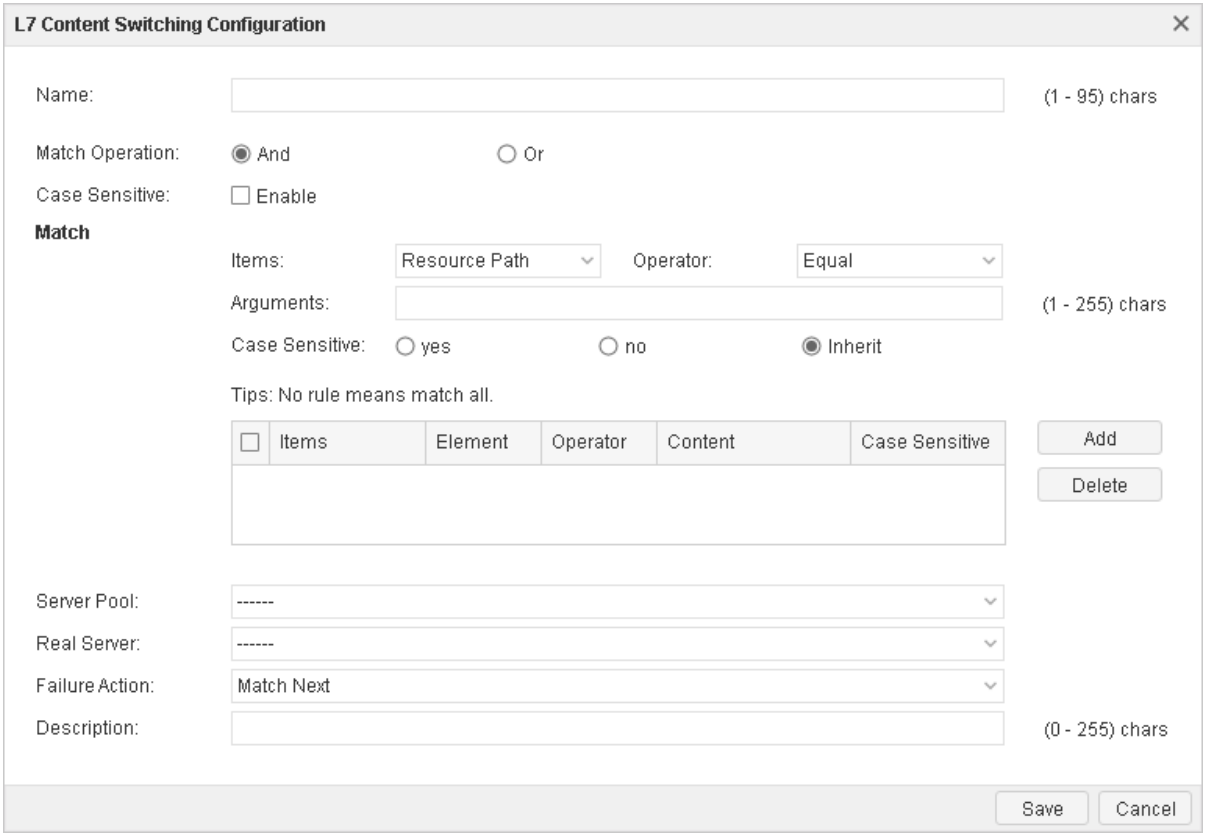
Configuring Layer 7 Content Switching Rules

For client requests accessing the same virtual server, you can configure Layer 7 content switching rules for the device. Then, the device will determine which server pool or real server will receive the requests based on the source and content attributes of the requests. You can configure 16 matching conditions for a Layer 7 content switching rule. When multiple matching conditions are configured, the relationship among the conditions is "AND", i.e., all the conditions should be met before being matched. If multiple Layer 7 content switching rules are configured, system will match the client requests with the rules in the rule list from top to down. Currently, only HTTP and HTTPS virtual servers support this function.

To configure a Layer 7 content switching rule, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Rule** > **L7 Content Switching**.

2. Click **New**, and the L7 Content Switching Configuration dialog box will appear.



Configure the following options.

Option	Description
Name	Specify the name of the Layer 7 content switching rule.
Match Operation	Specify an operator for matching conditions, including And and Or. "And" is the default option, indicating that all matching conditions need to be met; "Or" indicates that only one matching condition needs to be met.
Case Sensitive	With this check box selected, system will perform matching in a case-sensitive manner.
Match	After configuring a matching condition, click **Add**. If a client request meets the configured matching condition, the device will forward the request to the server pool or real server.

Option	Description

	Note:
	• You can configure the Match and Action as needed to send client certificate information to the server. After a matching condition is configured with certificate information, if the condition is met by a client certificate, system will forward the client request to a server pool or real server.
	  • Select **X509 Cert** from the **Items** drop-down list, and then specify an element, including Issuer, Issuer Country, Issuer Organization, Issuer Organization Unit, etc.
	  • Select **SSL/TLS** from the **Items** drop-down list, and then specify an element, including Protocol, Client Verify Result, SNI, Cipher Suite, etc.

Server Pool	Specify the name of the server pool. The client request that meets a matching condition will be distributed to the specified server pool.
Real Server	Specify the name of the real server as needed. If the parameter is specified, the device will directly distribute the matched client requests to the real server instead of distributing them to the server pool. If the parameter is not specified, the client requests will be load balanced across the server pool, and then they will be distributed to real servers according to the load balance algorithm.
Failure Action	When both the server pool and real server configured for the Layer 7 content switching rule are unavailable: if the real server is specified, system will perform a failure action as long as the real server is unavailable; and if no real server is specified, and the server pool is unavailable, system will perform a failure action too. • **Match Next** - System will continue to match the client request with the next Layer 7 content switching rule in the rule list. • **Drop** - System will drop the client request that meets a matching con-

Option	Description
	dition.
Description	Specify the description for the rule.

3. Click **Save**.

Configuring Layer 4 Content Switching Rules

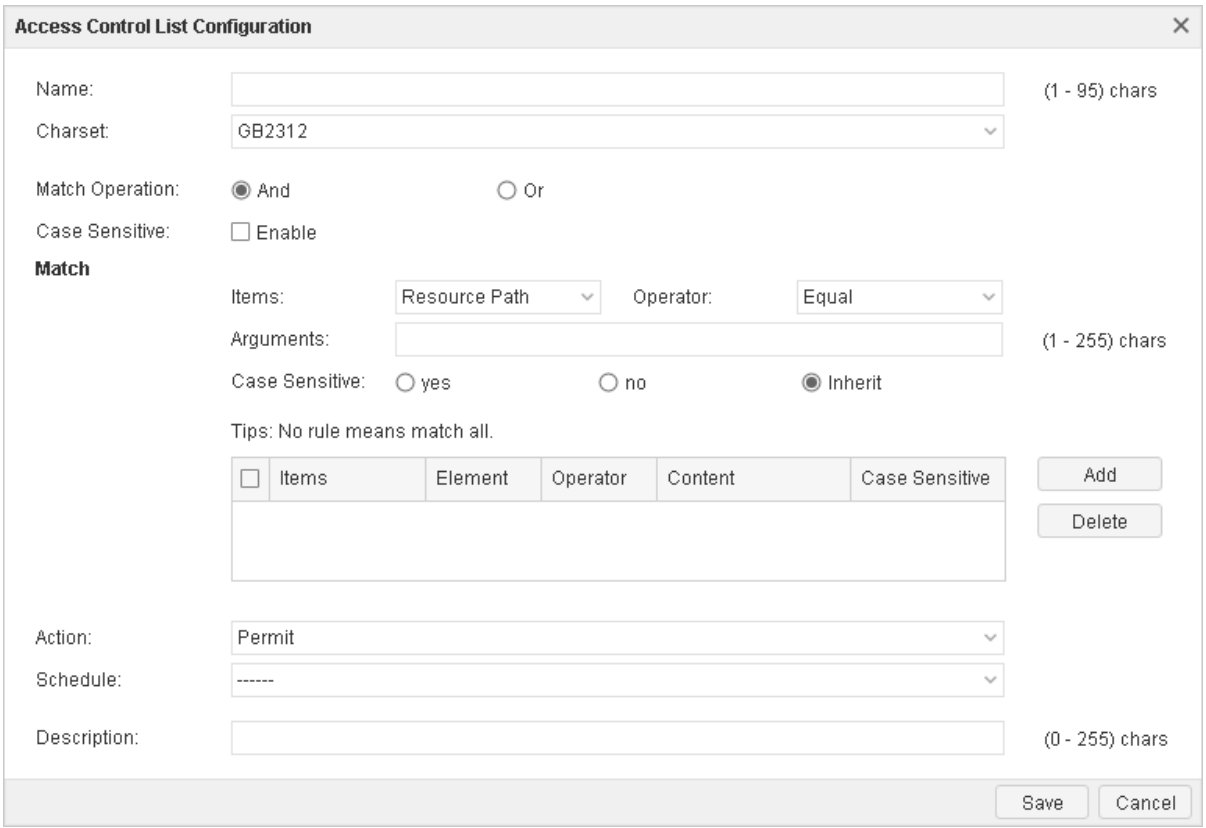
You can configure multiple Layer 4 content switching rules for a virtual server. System will match the client requests with the rules in the Layer 4 content switching rule list from top to down.

The Layer 4 SLB function supports IPv4 and IPv6 addresses.

To configure a Layer 4 content switching rule, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Rule** > **L4 Content Switching**.

2. Click **New**, and the L4 Content Switching Configuration dialog box will appear.



Configure the following options.

Option	Description
Name	Specify the name of the Layer 4 content switching rule.
Protocol	Select the protocol type supported by the Layer 4 content switching.
IP Type	Specify the IP type, including IPv4 and IPv6.
Source IP	Specify the source IP address of the client. You can select the IP address or IP range. Both IPv4 and IPv6 addresses are supported.
Source Port	Specify the source port of the client. You can select the port or port range.
Destination IP	Specify the destination IP of the client request, i.e., the IP address of the virtual server. Both IPv4 and IPv6 addresses are supported.
Destination Port	Specify the destination port of the client request, i.e., the port of the virtual server.
Server Pool	Specify the server pool. The client request that meets a matching condition will be distributed to the specified server pool.
Real Server	Specify the real server as needed. If the parameter is specified, the device will directly distribute the matched client requests to the real server instead of distributing them to the server pool. If the parameter is not specified, the client requests will be load balanced across the server pool, and then they will be distributed to real servers according to the load balance algorithm.
Failure Action	When both the server pool and real server configured for the Layer 4 content switching rule are unavailable: if a real server is specified, system will perform a failure action as long as the real server is unavailable; and if no real server is specified, and the server pool is unavailable, system will perform a failure action too. • **Match Next** - System will continue to match the client requests with the next Layer 4 content switching rule in the rule list. • **Drop** - System will drop the client request that meets a matching condition.
Description	Specify the description for the rule.

3. Click **Save**.

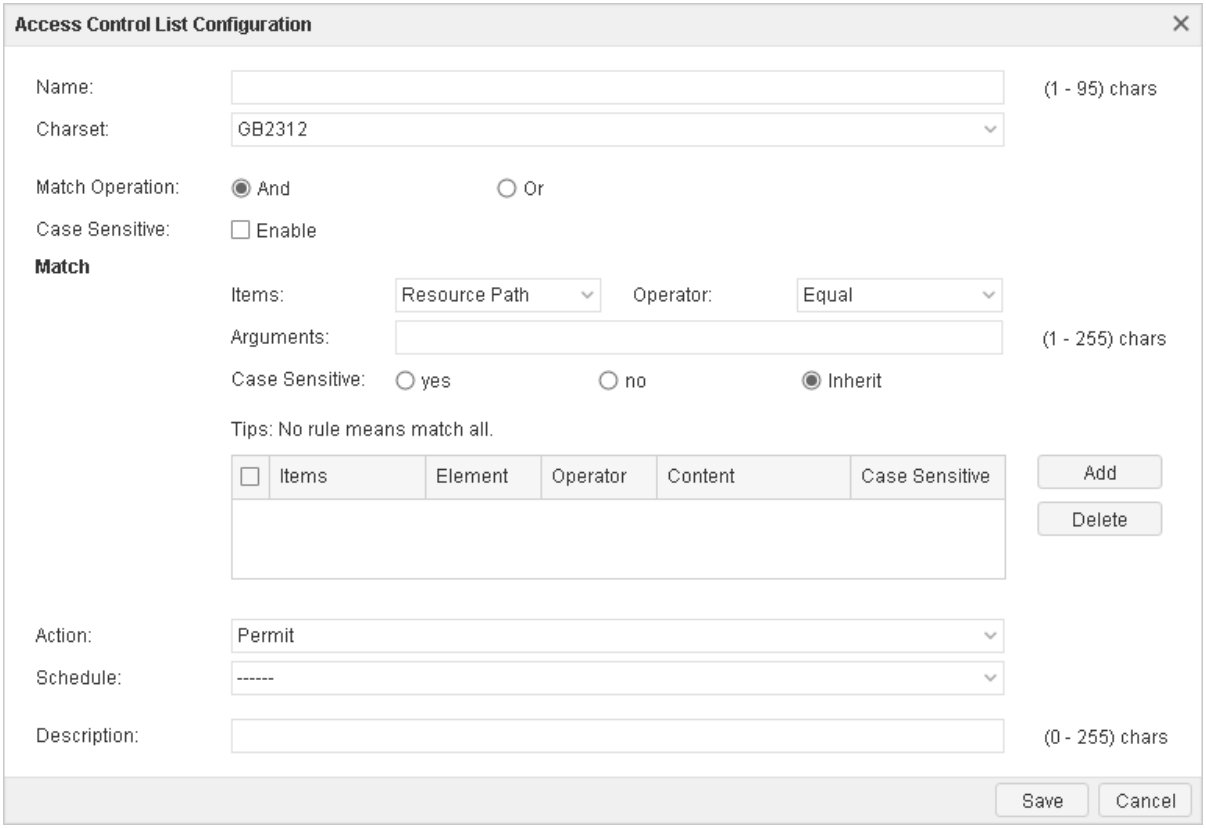
Access Control List

According to an access control rule you create, system will perform a Permit, Deny, Redirect or Response action on the traffic that meets a matching condition. After the configuration is complete, you need to bind the access control rule to a virtual server make it take effect. Currently, you can only bind access control rules to HTTP, HTTPS and HTTP proxy virtual servers.

To configure an access control rule, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **Rule** > **Access Control List**.

2. Click **New**, and the Access Control List Configuration dialog box will appear.



3. Configure the following options.

Option	Description
Name	Specify the name of the access control rule.
Charset	Specify the encoding method for the input characters, including GB2312, UTF-8, GBK and GB18030.

Option	Description
Match Operation	Specify an operator for matching conditions, including And and Or. "And" is the default option, indicating that all matching conditions need to be met; "Or" indicates that only one matching condition needs to be met.
Case Sensitive	With this check box selected, system will perform matching in a case-sensitive manner.

Match	After configuring a matching condition, click **Add**. If a client request meets the configured matching condition, the device will perform the corresponding action on the request to control its access.
	Note:
	• You can configure the Match and Action as needed to send client certificate information to the server. After a matching condition is configured with certificate information, if the condition is met by a client certificate, system will perform the corresponding action.
	  • Select **X509 Cert** from the **Items** drop-down list, and then specify an element, including Issuer, Issuer Country, Issuer Organization, Issuer Organization Unit, etc.
	  • Select **SSL/TLS** from the **Items** drop-down list, and then specify an element, including Protocol, Client Verify Result, SNI, Cipher Suite, etc.

Action	Specify the action to be executed by system. System will perform the corresponding action on the request that meets the matching conditions. • Permit - Permits the traffic to pass through. • Deny - Denies the traffic. • Redirect - Redirects the traffic to the specified URL address. Type the URL address into the **Redirect** text box, and then select a status code from the **Status Code** drop-down list.

Option	Description
	• Response - Returns the specified page or message. Select **Message** or **Page** as the Response Type, and type the message content into the **Message** text box or select a page from the **Response Page** drop-down list accordingly, and then type a status code into the **Status Code** text box.
Schedule	Specify the schedule.
Description	Specify the description for the rule.

4. Click **Save**.

Viewing the SLB Rule Status

After configuring a Layer 4 or Layer 7 content switching rule, you can view its running status in the rule list, including:

-  : Indicates that the running status is "Up".
-  : Indicates that the running status is "Health Check Down".
-  : Indicates that the running status is "Unknown".

If a Layer 4 or Layer 7 content switching rule is only configured with a server pool, the running status of the rule will be consistent with that of the server pool. If a Layer 4 or Layer 7 content switching rule is configured with both a server pool and a real server, the running status of the rule will be consistent with that of the real server, namely:

- If the running status of the specified real server is "Up", the rule status will be "Up".
- If the running status of the specified real server is "Unknown" or "Going Down", the rule status will be "Unknown".
- If the running status of the specified real server is "Health Check Down" or "Configured Down", the rule status will be "Health Check Down".

Client SSL Profile

After receiving the HTTPS traffic from a client, the device will decrypt the data, and then send the decrypted data to a real server in clear text; at the same time, the device will encrypt the data sent by the real server to the client, and then send the

encrypted data to the client. By encrypting and decrypting the HTTPS traffic, the burden on the real server is reduced, and the speed of users' access to the server is increased.

After configuring a client SSL profile, you can directly reference the profile when creating an HTTPS virtual server to implement SSL offloading. If you want to encrypt the data sending from the ADC device to the real server, you can configure a server SSL profile (see Server SSL-Profile).

Configuring Client SSL Profiles

To configure a client SSL profile, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **SSL Profile** > **Client SSL Profile**.
2. Click **New**, and the Client SSL Profile Configuration dialog box will appear.

In the Configuration tab, configure the following options.

Option	Description
Name	Type the name of the SSL Profile.
SSL/TLS Configuration	
Cipher Suite	Specify the SSL/TLS cipher suite for data transmission between a client and the device. You can either select a predefined or user-defined cipher suite. • Predefined: You can select or unselect a predefined encryption algorithm as needed. • User-defined: You can customize a cipher suite according to OpenSSL syntax.
Server Cipher Suite Preferred	
SSL Version	Specify the SSL/TLS protocol version for data transmission between a client and the device. You can select one or more protocol versions as needed. TLSv1.0, TLSv1.1 and TLSv1.2 are supported by default.
RSA Cert-chain	Specify the certificate chain for the RSA algorithm required when a client and the device establish an SSL connection. You need to create the certificate chain in advance in **System** > **PKI** > **Cert-chain**. The SSL certificate chain should include a Web server certificate and a key pair. For more information about creating a certificate chain, see Certificate Chain.
ECC Cert-chain	Specify the certificate chain for the ECC algorithm required when a client and the device

Option	Description
	establish an SSL connection. You need to create the certificate chain in advance in **System** > **PKI** > **Cert-chain**. The certificate chain should include a Web server certificate and a key pair. For more information about creating a certificate chain, see Certificate Chain.
Session Reuse	Select the **Enable** check box to enable the session reuse function. After the function is enabled, when an SSL connection is established between a client and a server for the first time, the symmetric key and other status information generated during the TLS handshake will be stored in the cache of the ADC device. When the client initiates the SSL connection request again (or initiates the connection request again after disconnection), the ADC device will continue to use the key and status information in the cache to encrypt and decrypt data without recalculation, thereby reducing the time consumed during the TLS handshake and the certificate transmission.
Timeout	Specify the timeout value of the session reuse. Within the timeout period, if the client initiates the SSL connection again, the ADC device will continue to use the key and status information in the cache for data transmission without recalculation. If this timeout expires, when establishing the SSL connection, the device needs to renegotiate with the client, and calculate the key and other status information.
Session Ticket	Select the **Enable** check box to enable the session ticket function. After the function is enabled, when an SSL connection is established between a client and a server for the first time, the symmetric key and other status information will be encrypted and sent to the corresponding client instead of being stored in the cache of the ADC device. When the client initiates the SSL connection again, the encrypted key and other status information will first be sent to the ADC device for decryption. Then, the ADC device will use the decrypted key and other status information to establish the SSL connection with the client.
GMSSL Configuration	
Cipher Suite	Specify the cipher suite supported by GMSSL. Currently, GMSSL supports the ECC-SM4-SM3 cipher suites.
Signature Cert-Chain	Specify the signature certificate chain supported by GMSSL. You need to create the sig-

Option	Description
	nature certificate chain in advance in **System** > **PKI** > **Cert-chain**. For more information about creating a certificate chain, see Certificate Chain.
Encryption Cert-Chain	Specify the encryption certificate chain supported by GMSSL. You need to create the encryption certificate chain in advance in **System** > **PKI** > **Cert-chain**. For more information about creating a certificate chain, see Certificate Chain.

Note: For the client SSL profile, you can configure SSL/TLS Configuration and GMSSL Configuration simultaneously.

In the Verification Configuration tab, configure the following options.

Option	Description
Verify Client	Specify the method for verifying the client certificate, including: • Disable: Indicates that a client does not need to provide an SSL certificate for verification when an SSL connection is established. • Optional: Indicates that a client may not provide an SSL certificate when an SSL connection is established. If the client provides the certificate, system will verify it. • Force: Indicates that system will verify SSL certificates of all clients when SSL connections are established.
Cert-chain	Specify one or more complete CA certificate(s) or certificate chain(s) to be verified. You need to create a certificate chain in advance in **System** > **PKI** > **Cert-chain**. The certificate chain should include a Web server certificate and a key pair. For more information about creating a certificate chain, see Certificate Chain.
CA Certificate Auto Advertisement	Select the **Enable** check box to enable the CA certificate auto advertisement function. After the function is enabled, system will send the relevant information of all selected CA certificates to a client. If it is not enabled, you can specify a CA certificate or certificate chain which needs to be advertised in Cert-chain Advertisement.
Cert-chain Advertisement	Specify one or more CA certificate(s) or certificate chain(s) to be advertised. You need to

Option	Description
	create a certificate chain in advance in **System** > **PKI** > **Cert-chain**. The certificate chain should include a Web server certificate and a key pair. For more information about creating a certificate chain, see Certificate Chain.
Min Key Length	Specify the minimum key length for the RSA and ECC algorithm used by a client certificate. The length has no limit by default. If a client key length is less than the specified length, the verification will fail, and then system will perform the corresponding action according to the verification rule.
Max Verify Depth	Specify the maximum verification depth for the root CA of a client certificate. The value range is 1 to 32. The default value is 9. If the depth of the root CA exceeds the specified depth, the verification will fail.
Verification Rule	You can configure different processing actions for results of the client certificate verification. After configuring the Verification Result and Action, click **Add** to generate a verification rule. System has 7 predefined client verification results and each result has a default action. If not configured otherwise, system will process a verification result according to the default action. Meanwhile, you can change the action for a verification result as needed to create a new rule, and then system will process the result according to the rule you create.
Verify URL Rule	After configuring Operator, Mode, Match URL, Case Sensitive and Element, click **Add** to generate a rule. If a client accesses a specified URL, system will perform Optional or Force verification on the client certificate according to the rule; if the client accesses an unspecified URL, system will perform verification according to the verification method you set. System will match with the rules in the list from top to down, and you can adjust the position of a rule in the list as needed. To adjust the position, click **Move**.

Configuring OCSP

The device allows you to configure Online Certificate Status Protocol (OSCP) to verify the validity of client certificates. OSCP and CRL are the main methods to query the status of CA certificates. Compared with downloading CRL files, the OSCP method is used by taking different steps. First, the ADC device sends a request to the OCSP server to query the

revoking status of a certain or multiple client certificates in real time. After the response is returned, the device obtains the status of the certificates from the response and processes the access request on the client. You can reduce network costs and save network resources when you use the OCSP method to verify the revoking status of client certificates.

The device allows you to configure OCSP stapling. This way, the browser used by the client can enable the OCSP stapling function. When the client establishes a TLS handshake with the virtual server for the first time, the device sends an OCSP request to query the status of the virtual server certificate. After the status information is obtained from the OCSP response, the device sends the virtual server certificate and its status information to the client. The browser used by the client determine whether to continue to access the virtual server based on its certificate status information and the policy of the browser.

To configure OCSP and OCSP stapling, take the following steps:

1. Select Load Balancing > Server Load Balancing > SSL Profile, and click the Client SSL Profile tab.
2. Click New, and the Client SSL Profile Configuration dialog box will appear.

In the Verification Configuration tab, configure the following options:

Option	Description
OCSP	Select the Enable check box to enable the OCSP function.
Responder Verify	Select the Enable check box to enable the function for verifying the OCSP response. After the function is enabled, the system verifies the signature of the OCSP response. If the verification is successful, the system obtains the verification result of the client certificate from the response. If the verification fails and the corresponding action is configured when the Verification Result parameter is set to OCSP Verify Failed, the system processes the signature by taking this action. If the verification fails and no action is configured, the system processes the signature by taking the default action. Note: If this function is disabled, the system directly obtains the verification result of the client certificate from the OCSP response and takes the corresponding action.
Request Method	Specify the request method used by the device to send an OCSP request. By default, the GET method is used.
Responder URL	Specify the URL of the OCSP server, which starts with "http://". In one of the following cases, the system determines the Verification Result parameter as OCSP Cert Unknown, and then processes the certificate based on the configuration in the Verification Rule section. • The connection from the device to the OCSP server times out. • The device fails to parse the URL of the OCSP server. • The URL of the OCSP server is not configured and the system cannot obtain the URL of the OCSP server from the client certificate.
Request Timeout	Specify the timeout period for the device to connect to the OCSP server. If the connection time exceeds the specified value, the device disconnects from the OCSP server. Valid values: 3 to 10. Default value: 5. Unit: seconds.
Cache	Select the Enable check box to enable the OCSP cache function. After the function is enabled, the system stores the status of the client certificate that is obtained from the OCSP response in the cache of the ADC device. When a new request from the client is received, the system directly queries the revoking status of the certificate in the cache. If the certificate status fails to be queried, the system sends a request to the

Option	Description
	OCSP server to query the status and store the query result in the cache of the ADC device. You can manually clear the OCSP cache in the device. For more information, see Clearing the OCSP cache.
Cache Timeout	Specify the timeout period for the device to store the OCSP cache. If the retention time exceeds the specified value, the system clears the status of the corresponding certificate in the cache. Valid values: 300 to 608400. Default value: 86400. Unit: seconds.

In the OCSP Stapling tab, configure the following options:

Option	Description
OCSP Stapling	Select the Enable check box to enable the OCSP stapling function.
Cert Issuer	Specify the certificate of the authority that issued the virtual server certificate. If the RSA or ECC certificate chain specified when the client establishes an SSL connection with the device contains the issuer certificate, you can ignore this parameter. Otherwise, you need to set this parameter. A maximum of 2 issuer certificates can be configured. You need to create a certificate chain in advance in System > PKI > Cert-chain. For more information about how to create a certificate chain, see Certificate Chain.
Responder Verify Cert	Specify the CA certificate used for verifying the OCSP response. A maximum of 2 CA certificates can be configured. You need to create a certificate chain in advance in System > PKI > Cert-chain. For more information about how to create a certificate chain, see Certificate Chain.
Responder Verify	Select the Enable check box to enable the function for verifying the OCSP response. After the function is enabled, the system verifies the signature of the OCSP response. If the verification fails, the browser used by the client cannot receive the verification result of the status of the virtual server certificate. If the function is disabled, the system directly obtains the status of the virtual server certificate from the OCSP response, and then sends the status information to the client.
Request Method	Specify the request method used by the device to send an OCSP request. By default, the GET method is used.
Responder URL	Specify the URL of the OCSP server, which starts with "http://". In one of the following

Option	Description
	cases, the browser used by the client cannot receive the verification result of the status of the virtual server certificate. • The connection from the device to the OCSP server times out. • The device fails to parse the URL of the OCSP server. • The URL of the OCSP server is not configured and the system cannot obtain the URL of the OCSP server from the client certificate.
Request Timeout	Specify the timeout period for the device to connect to the OCSP server. If the connection time exceeds the specified value, the device disconnects from the OCSP server. Valid values: 3 to 10. Default value: 5. Unit: seconds.
Responder Cache Timeout	Specify the timeout period for the device to store the status of the virtual server certificate. If the retention time exceeds the specified value, the system clears the status of the certificate in the cache. • Valid Cert: Specify the timeout period to store the status of the virtual server certificate when the status obtained from the OCSP response is normal. Valid values: 300 to 604800. Default value: 86400. Unit: seconds. • Others: Specify the timeout period to store the status of the virtual server certificate when the status obtained from the OCSP response is abnormal. Valid values: 300 to 604800. Default value: 86400. Unit: seconds.
Response All Status	Select the Enable check box to enable this function. After the function is enabled, the system returns the verification result to the client regardless of the status of the virtual server certificate. If the function is disabled, the system returns the verification result of the status of the virtual server certificate to the client only when the status is normal.

3. Click Save.

Clearing the OCSP cache

After the OCSP function is enabled, you can clear the status information of the client certificate that is stored in the device as needed. To clear the OCSP cache, take the following steps:

1. Select Load Balancing > Server Load Balancing > SSL Profile, and click the Client SSL Profile tab.
2. Select the client SSL profile whose OCSP cache you want to clear.
3. Click Clear OCSP Cache to clear the status of the client certificate corresponding to the client SSL profile.
4. Click Clear All OCSP cache to clear the status information of all client certificates.

SSL Accelerator Card

The SSL accelerator card uses a special hardware accelerator card to perform encryption and decryption operations required by the SSL communication, which can reduce the burden on the CPU and improve the overall SSL processing capability of system. The SSL accelerator card supports SSLv3, TLSv1.0, TLSv1.1 and TLSv1.2 protocols. Currently, SG-6000-AX1000S/SG-6000-AX2000S supports the SSL accelerator card.

Commands Related to SSL Accelerator Card

In any mode, use the following command to view the driver version number and running status of the accelerator card.

show ssl-hardware version

Example:

```
hostname# show ssl-hardware version
Version : 1.1-04
Status : SSL accelerator device OK
```

Description:

As above, the driver version number and status of the SSL accelerator card will be returned.

If `Status` returns OK, it indicates that the SSL accelerator card is working normally. For devices that do not support the accelerator card, "`NO SUPPORT SSL ACCELERATE DEVICE`" will be returned. If Status returns "`SSL driver init error`", it indicates that an error is occurred during the initialization of the SSL accelerator card.

In any mode, use the following command to view the statistics of the accelerator card. (Currently, you can only view the statistics related to the Record protocol in SSL.)

show ssl-hardware statistics

Example:

```
hostname# show ssl-hardware statistics

Encrypt : 180765

Decrypt : 76518

Encrypt IN Bytes : 2178310307

Encrypt OUT Bytes : 2174050298

Decrypt IN Bytes : 70211572

Decrypt OUT Bytes : 67150740
```

In the execution mode, use the following command to test the function of the accelerator card, such as testing the encryption and decryption functions.

exec ssl-hardware check { 3des | aes | hash }

3des - Tests whether the 3DES encryption function of the accelerator card is normal.

aes - Tests whether the AES encryption function of the accelerator card is normal.

hash - Tests whether the hash function of the accelerator card is normal.

Example:

```
hostname# exec ssl-hardware check 3des:

3DES: Devices detected: 1

dma mode: DIRECT Mode

Starting on device: 0

Encrypting data

Decrypting data

Comparing decrypted data with original

Device id: 0 - SUCCESS
```

Description:

As above, if SUCCESS is returned, it indicates that the test is successful. For devices that do not support the SSL accelerator card, "`NO SUPPORT SSL ACCELERATE DEVICE`" will be returned. If "`3DES_TEST: Failed to open`

`device file`" is returned, it indicates that an error is occurred during the device initialization. To obtain the running status, re-execute the `show ssl-hardware version` command.

In any mode, use the following command to clear the statistics of the accelerator card.

```
clear ssl-hardware statistics
```

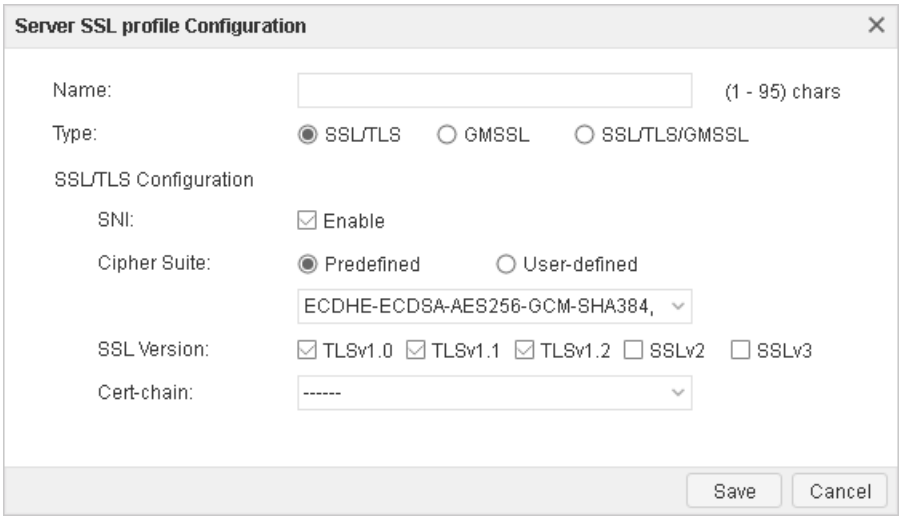
Server SSL Profile

By configuring a server SSL profile, the ADC device can encrypt the data from the client, and distribute the encrypted data to a real server with the SSL function. After configuring a server SSL profile, you can directly reference the profile when creating an HTTP or HTTPS virtual server to establish an HTTPS connection between the device and a real server.

Configuring Server SSL Profiles

To configure a server SSL profile, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **SSL Profile** > **Server SSL Profile**.
2. Click **New**, and the Server SSL Profile Configuration dialog box will appear.



Configure the following options.

Option	Description
Name	Type the name of the SSL Profile.
Type	Specify the type of the SSL profile, including SSL/TLS, GMSSL and SSL/TLS/GMSSL.

Option	Description
If SSL/TLS is selected, you need to configure the following:	
SSL/TLS Configuration	
SNI	After SNI is enabled, when the device forwards client requests to real servers with the same IP/port but different domain names, the client requests will carry the SNI field when accessing using domain names. Then, the servers will return corresponding certificates according to the SNI field.
Cipher Suite	Specify the SSL/TLS cipher suite for data transmission between the device and the real server. You can either select a predefined or user-defined cipher suite. • Predefined: You can select or unselect a predefined encryption algorithm as needed. • User-defined: You can customize a cipher suite according to OpenSSL syntax.
SSL Version	Specify the SSL/TLS protocol version for data transmission between the client and the real server. You can select one or more protocol versions as needed. TLSv1.0, TLSv1.1 and TLSv1.2 are supported by default.
Cert-chain	Specify the certificate chain required by the device to establish an SSL connection with the real server. The real server will verify certificates of the device. You need to create a certificate chain in advance in **System** > **PKI** > **Cert-chain**. The SSL certificate chain should include a Web server certificate and a key pair. For more information about creating a certificate chain, see Certificate Chain.
If GMSSL is selected, you need to configure the following:	
GMSSL Configuration	
Cipher Suite	Specify the cipher suite supported by GMSSL. Currently, GMSSL supports the ECC-SM4-SM3 cipher suites.
Signature Cert-Chain	Specify the signature certificate chain supported by GMSSL. You need to create the signature certificate chain in advance in **System** > **PKI** > **Cert-**

Option	Description
	chain. For more information about creating a certificate chain, see Certificate Chain.
Encryption Cert-Chain	Specify the encryption certificate chain supported by GMSSL. You need to create the encryption certificate chain in advance in **System** > **PKI** > **Cert-chain**. For more information about creating a certificate chain, see Certificate Chain.
If SSL/TLS/GMSSL is selected, you can configure SSL/TLS Configuration and GMSSL Configuration simultaneously. For specific configurations, refer to the above SSL/TLS Configuration and GMSSL Configuration.	

Application Profile

Application profiles include HTTP profiles, fast HTTP profiles, HTTP proxy profiles and SSL stream proxy profiles.

HTTP Profile

HTTP profiles allow you to configure parameters related to the HTTP protocol. The AX device supports the HTTP 1.0, 1.1 and 2.0 protocols, and the WebSocket protocol. Because the AX device is deployed between the HTTP client and the HTTP server, i.e., the AX device functions both as the HTTP client and the HTTP server during data forwarding, the configured HTTP protocol parameters will affect the way how the AX device processes HTTP requests.

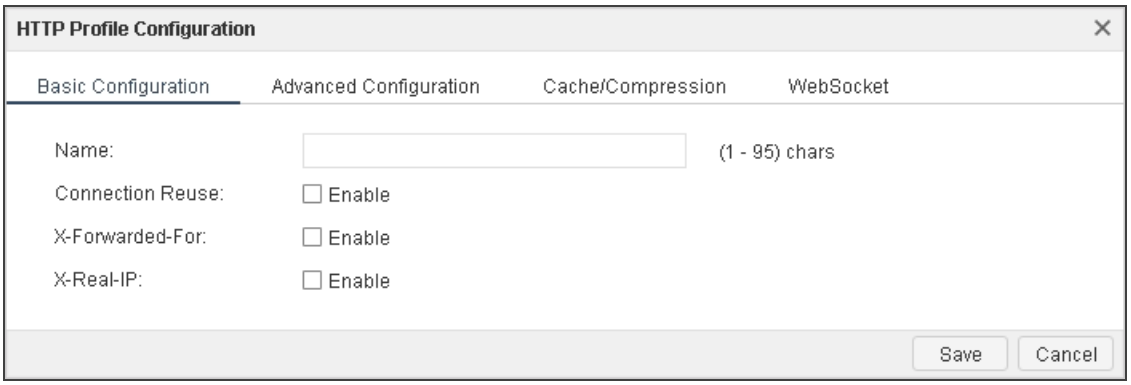
HTTP profiles support both HTTP and HTTPS protocols, wherein profiles for HTTP can only be configured on HTTP virtual servers, and profiles for HTTPS can only be configured on HTTPS virtual servers.

Configuring HTTP/HTTPS Profiles

HTTP profiles and HTTPS profiles have the same configuration steps. To configure an HTTP profile, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **App Profile** > **HTTP Profile**.

2. Click **New**, and the HTTP Profile Configuration dialog box will appear.

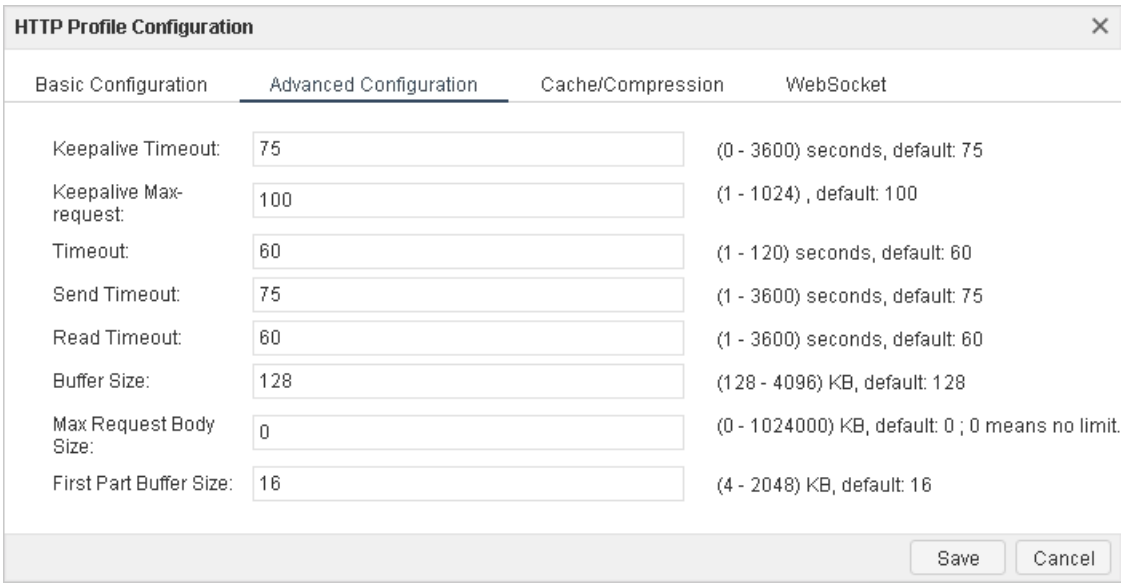


In the Basic Configuration tab, configure the following options.

Option	Description
Name	Type the profile name. You can enter 1 to 95 characters.
Connection Reuse	Select the **Enable** check box to enable the TCP Connection Reuse function. The function is disabled by default, indicating that the TCP connection will be closed after each request/response. Then, the AX device will connect to a real server over the HTTP 1.0 protocol. After the function is enabled, the AX device will connect to a real server over the HTTP 1.1 protocol and will adopt the persistent connection mechanism. The maximum number of requests/responses that can be made on a single TCP connection is determined by the real server. Compared with the number of client requests, the number of connections between the AX device and the real server is lesser due to connection reuse, thereby reducing the burden on the real server.
Connection Pool Size	Specify the maximum number of idle TCP connections between the AX device and all real servers. After enabling the Connection Reuse function, you need to specify the value. The value range is 0 to 10240. The default value is 1024.
X-Forwarded-For	Select the **Enable** check box to enable the X-Forwarded-For function. After the function is enabled, the device will insert the X-Forwarded-For

Option	Description
	field into an HTTP/HTTPS message when forwarding the message. If there are multiple proxies, each proxy server will insert the originating IP of the request into the X-Forwarded-For field to make it visible to the real server.
X-Real-IP	Select the **Enable** check box to enable the X-Real-IP function. After the function is enabled, the device will only record the IP of the client that actually sent the request when forwarding the message.

3. Click the **Advanced Configuration** tab.



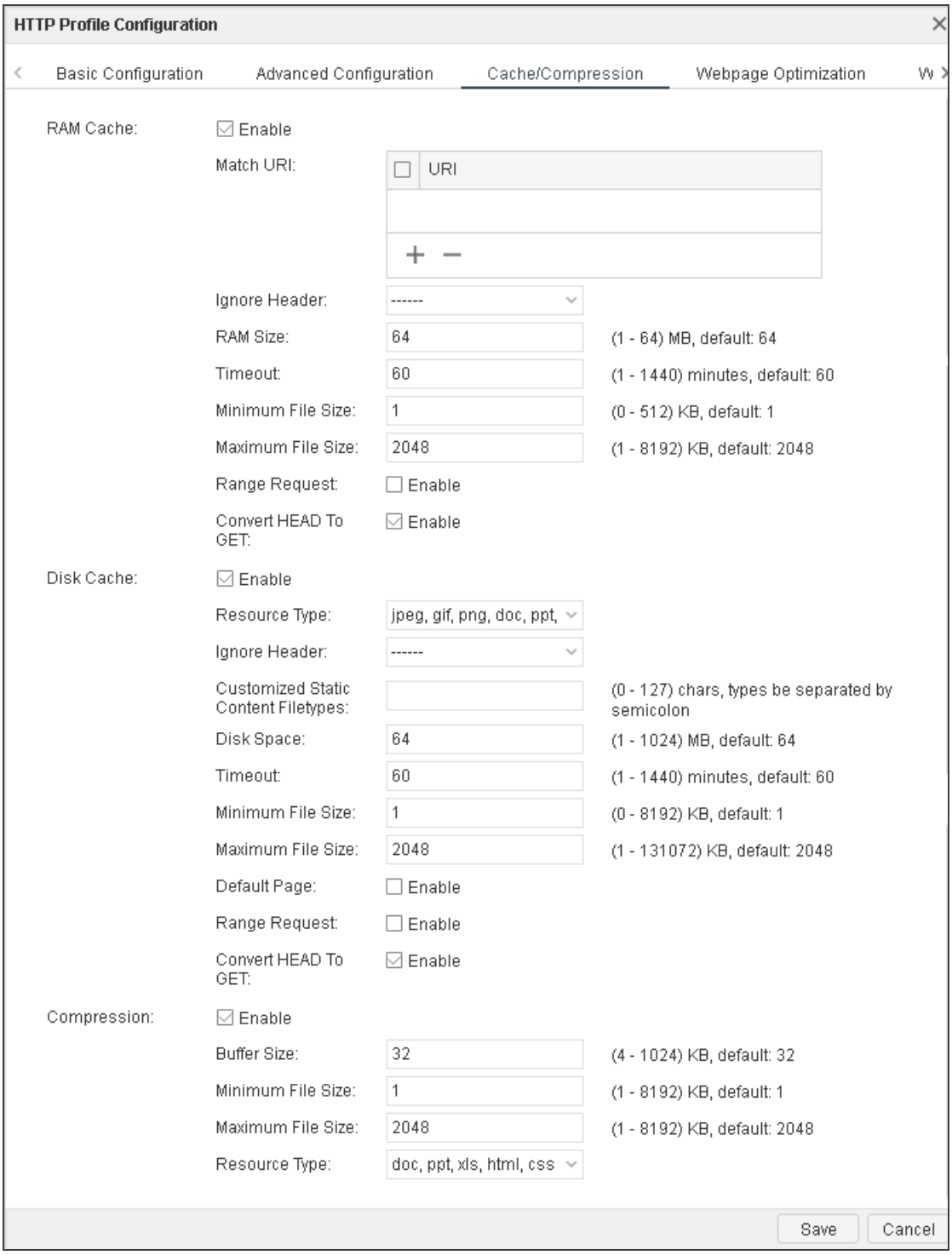
Configure the following options.

Option	Description
Keepalive Timeout	Specify the keepalive time between the device and the client (i.e., the TCP persistent connection timeout period). The value range is 0 to 3600 seconds. The default value is 75. The value of 0 indicates that the persistent connection mechanism is disabled. Because the HTTP 1.1 protocol introduces the persistent connection mechanism, the keepalive timeout period is the same as the timeout period of the persistent connection mechanism of HTTP 1.1. After the client establishes

Option	Description
	a TCP connection with the AX device over the HTTP 1.1 protocol, if the device has not received an HTTP request from the client within the keepalive timeout period, the TCP connection will be closed. Otherwise, if the device receives an HTTP request again, the Keepalive Timeout will be reset after the request being processed. This function is often used together with Keepalive Max-request. (For detailed information, refer to RFC2068)
Keepalive Max-request	Specify the maximum number of requests/responses that can be sent between the device and the client (based on the HTTP 1.1 keepalive mechanism). The value range is 0 to 1024. The default value is 100. The client establishes a TCP connection with the AX device over the HTTP 1.1 protocol. If the number of client requests responded by the AX device has reached the value, the device will close the TCP connection. (For detailed information, refer to RFC2068)
Timeout	Specify the timeout value for the device to establish a TCP connection with the real server. If this timeout expires, the TCP connection will fail. The value range is 0 to 120 seconds. The default value is 60.
Send Timeout	Specify the timeout value for sending a piece of data between the device and the real server. If this timeout expires, the device will disconnect the TCP connection. The value range is 1 to 3600 seconds. The default value is 75.
Read Timeout	Specify the timeout value for the device to read the HTTP/HTTPS response returned by the real server. That is to say, after the device sends an HTTP/HTTPS request, and has not received any data returned by the real server within the read timeout period, it is considered as timeout. Then, the device will pop up the "504 Gateway Timeout" error to ensure that the maximum waiting time for each request is fixed and not too long. The value range is 1 to 3600 seconds. The default value is 60.
Buffer Size	Specify the size of the buffer of the HTTP/HTTPS response to be returned by the real server. The value range is 128 to 4096KB. The default

Option	Description
	value is 128KB.
Max Request Body Size	Specify the size of the uploaded file in the HTTP/HTTPS request. The value range is 0 to 1024000KB. The default value is 0 KB.
First Part Buffer Size	Specify the size of the first fragment buffer of the HTTP/HTTPS response to be returned by the real server. The value range is 4 to 2048KB. The default value is 16KB.

4. Click the **Cache/Compression**4 tab.



Configure the following options.

Option	Description
RAM Cache: Select the **Enable** check box to enable the function of caching HTTP static resources in ADC RAM. After the function is enabled, when the URI path in a client request matches the matching rules of **RAM Cache**, system will cache the static resources (such as CSS files, pictures and other resources with a large number of accesses but small changes) returned by the real server to the client in ADC RAM. In this way, when the client accesses the same static resources again, the device can directly return the cached content to the client, thereby saving time of subsequent communication with the real server, and reducing the load burden on the real server. Notes: System supports to cache HTTP static resources in the device disk or RAM. System reads HTTP static resources from the RAM faster than the disk, and thus when a client request matches both	
URL	Click **+** to add a URI matching rule. Enter the URI information in the text box, system supports regular expression match. If the path in a client request matches the configured URI matching rules, system will cache the static resources returned by the real server to the client in RAM. You can add up to 8 matching rules. Click **-** to delete a selected URI matching rule. **Notes**: If you do not configure any URI matching rules, system will not cache any static resources in RAM.
Ignore Header	Select the header names which may be carried in responses from the drop-down list, the impact of them on caching will be ignored. In the list, select the headers you want to add, and then cilck → to add it to the selected list. If you want to remove a header in the selected list, select the headers in the list, and then click ←.
RAM Size	Specify the maximum size of RAM that the virtual server referencing the HTTP/HTTPS profile can provide for the Web cache. If the value is exceeded, system will clear some of the original cache to cache new HTTP static resources. The value range is 1 to 64 MB. The default value is 64 MB.
Timeout	Specify the amount of time that HTTP static resources will be cached in the

Option	Description
	device RAM. The value range is 5 to 1440 minutes. The default value is 60. After the value is specified, when the client accesses a static resource on the real server for the first time, system will cache the static resource returned by the real server to the client: • If the client accesses the static resource again within the timeout period, system will directly send the cached resource to the client, thereby saving communication time. After the timeout period is exceeded, system will request the resource from the real server again to refresh the cache. • If the client has not accessed the static resource within the timeout period, system will clear the static resource after the timeout period is exceeded. For example: With the timeout period set to 10 minutes, if system has cached the static resource A. The client accesses the resource A again at the 5th minute, system will directly send the cached resource to it. System will clear the cache 10th minute later. If the client accesses 10 minutes later, system will request the resource from the real server again to refresh the cache and send the new cache content to the client, and so forth.
Minimum File Size	Specify the minimum length of the file that can be cached by system. The value range is 0 to 512 KB. The default value is 1 KB. System will perform the cache operation only when the length of the file is between the minimum length and the maximum length.
Maximum File Size	Specify the maximum length of the file that can be cached by system. The value range is 1 to 8192 KB. The default value is 2048 KB. System will perform the cache operation only when the length of the file is between the minimum length and the maximum length.
Range Request	Select the **Enable** check box to enable this funciton. After the function is enabled, when the client accesses an HTTP Range Request to a URL, the device will access the complete request to the real server, and then cache the

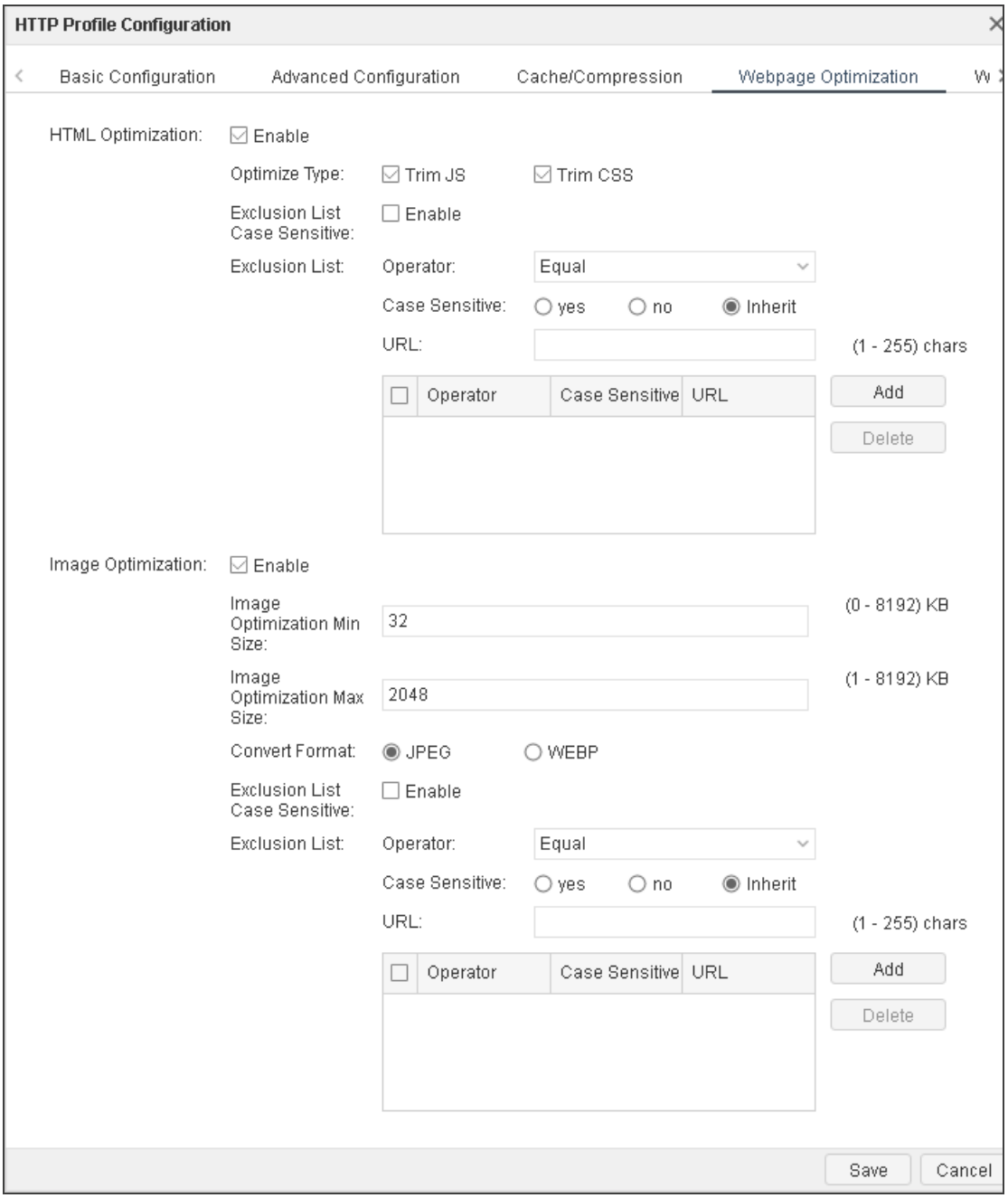
Option	Description
	responses in RAM. In this way, when the client accesses HTTP Range Request to the same URL, the ADC device will directly send corresponding cached responses to the client.
Convert HEAD To GET	Select the **Enable** check box to enable this funciton . After the function is enabled, when the client accesses an HEAD request, system will automatically convert it to a GET request. Then system accesses the GET request to the real server and caches responses in RAM. In this way, system can directly send cached resource to the client the next time whether the client accesses an HEAD request or a GET request. This function is enabled by default. If this function is disabled, system will directly forward request which the client accesses to the real server and cache corresponding responses. In this way, only when the client uses the request method same as that the client used for the first time, system can return cached resource to the client.
Disk Cache[1]: Select the **Enable** check box to enable the function of caching HTTP static resources on the device disk. After the function is enabled, system will cache the static resource (such as CSS files, pictures and other resources with a large number of accesses but small changes) returned by the real server to the client. In this way, when the client accesses the same static resource again, the device can directly return the cached content to the client, thereby saving time of subsequent communication with the real server, and reducing the load burden on the real server.	
Resource Type	Specify the type of the static resource that will be cached by the HTTP cache. You can either select a predefined type or customize one. System will only cache static resources of specified types.
Ignore Header	Select the header names which may be carried in responses from the drop-down list, the impact of them on caching will be ignored. In the list, select the headers you want to add, and then cilck → to add it to the selected list. If you want to remove a header in the selected list, select the headers in the list, and then click ←.

Option	Description
Customized Static Content Filetypes	Specify your own user-defined static resource types. Different types should be separated by the semicolon ";". System will only cache static resources of specified types.
Disk Space	Specify the maximum disk space that the virtual server referencing the HTTP/HTTPS profile can provide for the Web cache. If the value is exceeded, system will clear some of the original cache to cache new HTTP static resources. The value range is 1 to 1024MB. The default value is 64MB.
Timeout	Specify the amount of time that HTTP static resources will be cached on the device disk. The value range is 5 to 1440 minutes. The default value is 60. After the value is specified, when the client accesses a static resource on the real server for the first time, system will cache the static resource returned by the real server to the client: • If the client accesses the static resource again within the timeout period, system will directly send the cached resource to the client, thereby saving communication time. After the timeout period is exceeded, system will request the resource from the real server again to refresh the cache. • If the client has not accessed the static resource within the timeout period, system will clear the static resource after the timeout period is exceeded. For example: With the timeout period set to 10 minutes, if system has cached the static resource A. The client accesses the resource A again at the 5th minute, system will directly send the cached resource to it. System will clear the cache 10th minute later. If the client accesses 10 minutes later, system will request the resource from the real server again to refresh the cache and send the new cache content to the client, and so forth.
Minimum File Size	Specify the minimum length of the file that can be cached by system. The

Option	Description
	value range is 1 to 8192KB. The default value is 1KB. System will perform the cache operation only when the length of the file is between the minimum length and the maximum length.
Maximum File Size	Specify the maximum length of the file that can be cached by system. The value range is 1 to 8192KB. The default value is 2048KB. System will perform the cache operation only when the length of the file is between the minimum length and the maximum length.
Defalut Page	Select the **Enable** check box to enable this function. After the function is enabled, if there is not any URI information in the client request, system will still cache the static resources returned by the real server on the device disk.
Range Request	Select the **Enable** check box to enable this funciton. After the function is enabled, when the client accesses an HTTP Range Request , the device will access the complete request to the real server, and then cache the responses in RAM. In this way, when the client accesses HTTP Range Request to the URL same as that the client accessed for the first time, the ADC device will directly send corresponding cached responses to the client.
Convert HEAD To GET	Select the **Enable** check box to enable this funciton . After the function is enabled, when the client accesses an HEAD request, system will automatically convert it to a GET request. Then system accesses the GET request to the real server and caches responses in the device disk. In this way, system can directly send cached resource to the client the next time whether the client accesses an HEAD request or a GET request. This function is enabled by default. If this function is disabled, system will directly forward request which the client accesses to the real server and cache corresponding responses. In this way, only when the client uses the request method same as that the client used for the first time, system can return cached resource to the client.
Compression[2,3]: Select the **Enable** check box to enable the function of compressing HTTP static resources. After the function is enabled, if the client can receive and decompress com-	

Option	Description
pressed files, the device will first compress uncompressed files returned by the server, and then send them to the client, thereby reducing the transmission load and shortening the transmission time to accelerate the communication.	
Buffer Size	Specify the size of the compressed buffer that can be provided by the virtual server referencing the HTTP profile. If the value is exceeded, system will clear some of the original cache to cache new HTTP static resources. The value range is 4 to 1024KB. The default value is 32KB.
Minimum File Size	Specify the minimum length of the file that can be compressed by system. The value range is 1 to 8192KB. The default value is 1KB. System will perform the compression operation only when the length of the file is between the minimum length and the maximum length.
Maximum File Size	Specify the maximum length of the file that can be compressed by system. The value range is 1 to 8192KB. The default value is 2048KB. System will perform the compression operation only when the length of the file is between the minimum length and the maximum length.
Resource Type	Specify the type of the static resource that will be compressed by system. You can select a predefined resource type as needed. System will only compress static resources of specified types.

5. Click the **Webpage Optimization** tab.



Configure the following options.

Option	Description
HTML Optimize: Select the **Enable** check box to enable the function of HTML optimization. After the function is enabled, when the client accesses a URL address which is not specified in	

Option	Description
the **Exclusion List**, system will perform HTML optimization of webpages returned by the real server so that to reduce the size of webpage resources and increase the speed of users' access to the server.	
Optimize Type	• Trim JS - If you select the check box, system will optimize the JS code of an HTML webpage. • Trim CSS - If you select the check box, system will optimize the CSS code of an HTML webpage. **Notes**: Both **Trim JS** and **Trim CSS** are selected by default. If either of them is selected, system will only optimize the HTML code of webpage.
Exclusion List Case Sensitive	Select the **Enable** check box, system will perform matching the rules which are configured in Exclusion List in a case-sensitive manner. This function is disabled by default.
Exclusion List	After configuring Operator, Case Sensitive and URL, click **Add** to generate a rule. If a client accesses an unspecified URL address, system will perform HTML Optimization on the webpage returned by the real server. System supports accurate match and regular expression match. You can configure Case Sensitive for each matching rule as needed, if not, system will do the manner to this rule according to the Exclusion List Case Sensitive configuration.
Image Optimize: Select the **Enable** check box to enable the function of images optimization in the webpage. After the function is enabled, when the client accesses a URL address which is not specified in the **Exclusion List**, system will convert the format of images in webpages returned by the real server so that to reduce the traffic and increase the speed of users' access to the	

Option	Description
server.	
Image Optimization Min Size	Specify the minimum size of the image which format will be converted by system. The value range is 0 to 8192KB. The default value is 32KB. When the size of a image is less than the specified value, system will not perform format conversion on it.
Image Optimization Max Size	Specify the maximum size of the image which format will be converted by system. The value range is 1 to 8192KB. The default value is 2048KB. When the size of a image is more than the specified value, system will not perform format conversion on it.
Convert Format	• JPEG - If specified, system will convert images in PNG/GIF/WEBP format to images in JPEG format. • WEBP - If specified, system will convert images in PNG/JPEG format to images in WEBP format.
Exclusion List Case Sensitive	Select the **Enable** check box, system will perform matching the rules which are configured in Exclusion List in a case-sensitive manner. This function is disabled by default.
Exclusion List	After configuring Operator, Case Sensitive and URL, click **Add** to generate a rule. If a client accesses an unspecified URL address, system will perform HTML Optimization on the webpage returned by the real server. System supports accurate match and regular expression match. You can configure Case Sensitive for each matching rule as needed, if not, system will do the man-

Option	Description
	ner to this rule according to the Exclusion List Case Sensitive configuration.

6. Select the **WebSocket** tab, and select the **Enable** check box. After the function is enabled, a persistent connection based on bidirectional communication over TCP will be established between the server and client.

7. Click **Save**.

HTTP 2.0 Protocol

If the protocol type is HTTPS, the device supports HTTP 2.0 services. In this case, ADC can function as an HTTP 2.0 gateway enabling protocol conversion from HTTP 1.0/1.1 to HTTP 2.0 (and vice versa) between the client and server. Currently, system supports protocol conversion between the HTTP 2.0 client and HTTP 1.0/1.1 server.

To configure the HTTP 2.0, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **App Profile** > **HTTPS Profile**.

2. Click **New**, and the HTTPS Profile Configuration dialog box will appear.

3. In the Basic Configuration tab, select the **HTTP/2** check box to enable HTTP 2.0. The function is disabled by default.

4. Configure the following options.

Option	Description
Idle Timeout	Specify the timeout value for closing idle connections.
Max Concurrent Streams	Specify the maximum number of concurrent streams in each connection.
Receive Window Size	Specify the number of bytes that can be received without sending an acknowledgment.
Frame Size	Specify the size of the data frame sent to the client.
Table Size	Specify the maximum value of the compressed request header field.
Header X-HTTP/2	Select the **Enable** check box to enable the function. System will insert the Header information into the request from the source Web server.

5. Click **Save**.

Note:

1. The device will determine whether to cache static resources according to the HTTP response information (such as the Cache-Control and Expired fields in the HTTP response header) returned by the real server and the device configuration. For example, if the Expired time is exceeded, even if the device enables the cache function, the static resources of the HTTP response will not be cached.
2. If there is no Content-Length field in the HTTP response, system will not compress the HTTP static resources.
3. If the client cannot receive and decompress compressed files, even if the HTTP compression function is enabled, the device will not compress the static resources returned by the real server.
4. If both the HTTP cache and HTTP compression functions are enabled, system will first cache the static resources returned by the real server, and then compress them before sending them to the client.

Fast HTTP Profile

A fast HTTP profile can only be referenced by a fast HTTP virtual server. To configure a fast HTTP profile, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **App Profile** > **Fast HTTP Profile**.
2. Click **New**, and the Fast HTTP Profile Configuration dialog box will appear.

   Configure the following options.

Option	Description
Name	Type the profile name. You can enter 1 to 95 characters.
Maximum Segment Size	Specify the maximum segment size of the TCP packet.

3. Click **Save**.

Configuring HTTP Proxy Profiles

An HTTP proxy profile can only be referenced by an HTTP proxy virtual server. To configure an HTTP proxy profile, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **App Profile** > **HTTP Proxy Profile**.
2. Click **New**, and the HTTP Proxy Profile Configuration dialog box will appear.

In the Basic Configuration tab, configure the following options.

Option	Description
Name	Type the profile name. You can enter 1 to 95 characters.
X-Forwarded-For	Select the **Enable** check box to enable the X-Forwarded-For function. After the function is enabled, the device will insert the X-Forwarded-For field into a message when forwarding the message. The field contains the real IP of the client, which is visible to the real server.

3. Click the Advanced Configuration tab, and configure the following options.

Option	Description
Keepalive Timeout	Specify the keepalive time between the device and the client (i.e., the TCP persistent connection timeout period). The value range is 0 to 3600 seconds. The default value is 75. The value of 0 indicates that the persistent connection mechanism is disabled. Because the HTTP 1.1 protocol introduces the persistent connection mechanism, the keepalive timeout period is the same as the timeout period of the persistent connection mechanism of HTTP 1.1. After the client establishes a TCP connection with the AX device over the HTTP 1.1 protocol, if the device has not received an HTTP request from the client within the keepalive timeout period, the TCP connection will be closed; otherwise, if the device receives an HTTP request again, the Keepalive Timeout will be reset after the request being processed. This function is often used together with the Keepalive Max-request. (For detailed information, refer to RFC2068)
Keepalive Max-request	Specify the maximum number of requests/responses that can be sent between the device and the client (based on the HTTP 1.1 keepalive mechanism). The value range is 0 to 1024. The default value is 100. The client establishes a TCP connection with the AX device over the HTTP 1.1 protocol. If the number of client requests responded by the AX device has reached the value, the device will close the TCP connection. (For detailed information, refer to RFC2068)
Timeout	Specify the timeout value for the device to establish a TCP connection with the real server. If this timeout expires, the TCP connection will fail. The value range is 0 to 120 seconds. The default value is 60.
Send Timeout	Specify the timeout value for sending a piece of data between the device and the real server. If this timeout expires, the device will disconnect the TCP connection. The value range is 1 to 3600 seconds. The default value is 75.

Option	Description
Read Timeout	Specify the timeout value for the device to read the response returned by the real server. That is to say, after the device sends a request, and has not received any data returned by the real server within the read timeout period, it is considered as timeout. Then, the device will pop up the "504 Gateway Timeout" error to ensure that the maximum waiting time for each request is fixed and not too long. The value range is 1 to 3600 seconds. The default value is 60 seconds.
Buffer Size	Specify the size of the buffer of the response to be returned by the real server. The value range is 128 to 4096KB. The default value is 128KB.
Max Request Body Size	Specify the size of the uploaded file in the request. The value range is 128 to 1024000KB. The default value is 8192KB.
First Part Buffer Size	Specify the size of the first fragment buffer of the response to be returned by the real server. The value range is 4 to 2048KB. The default value is 16KB.

4. Click **Save**.

Configuring SSL Stream Proxy Profiles

A SSL stream proxy profile can only be referenced by a SSL stream proxy virtual server. To configure a SSL stream proxy profile, take the following steps:

1. Select **Load Balance** > **Server Load Balance** > **App Profile** > **SSL Stream Proxy Profile**.
2. Click **New**, and the SSL Stream Proxy Profile Configuration dialog box will appear.

   Configure the following options.

Option	Description
Name	Type the profile name. You can enter 1 to 95 characters.
Timeout	Specify the timeout value for the device to establish a TCP connection with the real server. If this timeout expires, the TCP connection will fail. The value range is 0 to 120 seconds. The default value is 60.

Option	Description
Read and Write Timeout	Specify the timeout value for the device to send the request to the target server and to read the response returned by the target server. The two timeout periods share the same value. If the time taken by the device to forward the HTTPS request to the target server exceeds the value, the device will disconnect itself from the target server; and if the request has been successfully sent to the target server, but no response is received from the target server within the specified timeout period, the device will disconnect itself from the target server. The value range is 1 to 3600 seconds. The default value is 600.
Buffer Size	Specify the size of the buffer of the HTTPS response to be returned by the real server. The value range is 128 to 4096KB. The default value is 128KB.

3. Click **Save**.

Chapter 4 Link Load Balance

For multi-ISP links, the system distributes and forwards traffic to different links based on the ISP of its destination IP address. The system can also distribute and forward traffic to different links by using load balancing algorithms such as real-time monitoring and dynamic link detection. This reduces the delay, jitter, and packet loss rate on each link, and thus balances the bandwidth utilization.

Related Topics:

- "Outbound Link Load Balancing" on Page 119: Enable the LLB function for outbound traffic.

Outbound Link Load Balancing

The system provides the LLB function for outbound traffic. For traffic from outbound links, the system monitors the delay, jitter, packet loss rate, and bandwidth utilization of each link in real time based on a specified load balancing algorithm. This way, the system can intelligently route and dynamically adjust the traffic load of each link. You can configure a flexible LLB profile and bind the LLB profile to a route by configuring LLB rules (the current system supports only the DBR and PBR routes). This allows you to control the traffic from outbound links and balance the load of these links.

The device balances the traffic load of outbound links based on the following process:

1. Session persistence and load balancing algorithms are matched in sequence.
2. If session persistence is matched, the device directly selects the link in session persistence.
3. If the ISP algorithm is matched, the device selects a route for the traffic based on the ISP of its destination IP address. If multiple available ISP links are matched, the device selects a route based on the secondary algorithm. If all matched ISP links exceed the threshold of bandwidth utilization or no ISP link is matched, the device selects a route based on a specified alternative balancing algorithm.
4. If an algorithm other than ISP is matched, the device selects a route based on this algorithm.
5. The device forwards the traffic to the selected link based on the result of the link selection.

Note:

- When you select a link for outbound traffic, session persistence is preferentially matched. If the link selected in session persistence is busy, the device selects another link based on the specified balancing algorithm. If all links are busy, the link selected in session persistence continues to be served as the outbound link.
- If all the links selected based on load balancing algorithms are busy, the system forwards the traffic to the default route.

Load Balancing Algorithms

The following table describes the load balancing algorithms for outbound traffic supported by the system.

Algorithm	Description
Dynamic Proximity	The device monitors the delay, jitter, packet loss rate, and bandwidth utilization of each link in real time. If the bandwidth utilization of each link is lower than the specified threshold, the system analyzes the link quality only based on the delay, jitter, and packet loss rate. Then, the system selects the link with the highest quality. If the bandwidth utilization of each link is greater than the specified threshold, the system analyzes the link quality based on the delay, jitter, packet loss rate, and bandwidth utilization. Then, the system selects the link with the highest quality.
Destination IP Hash	The system calculates the hash value of the destination IP address of traffic, and then selects a route for the traffic based on the hash value.
Source IP Hash	The system calculates the hash value of the source IP address of traffic, and then selects a route for the traffic based on the hash value.
Source IP Port Hash	The system calculates the hash value of the source IP address and port of traffic, and then selects a route for the traffic based on the hash value.
ISP	The system matches the destination IP address of traffic with its ISP information, and then selects a route for the traffic based on the matched result.
Least Bandwidth	The device records the upstream bandwidth, downstream bandwidth, or sum of the upstream and downstream bandwidth on each interface. After new outbound traffic is generated, the device forwards it to the interface with the minimum record value.

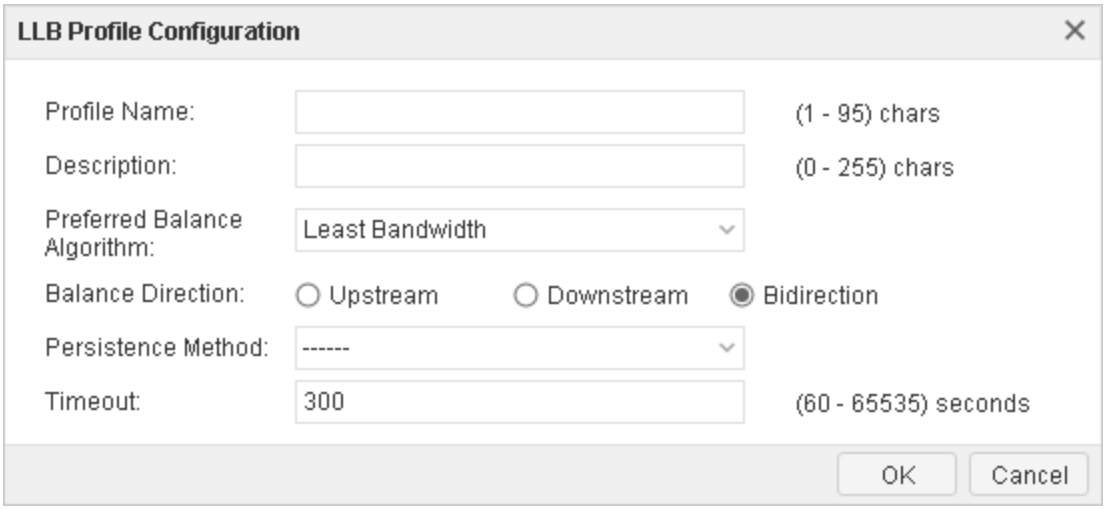
Algorithm	Description
Least Connection	The device records the number of connections on each interface. After new outbound traffic is generated, the device forwards it to the interface with the minimum record value.
Round Robin	The device forwards the traffic to each outbound link in a rotating sequential manner.
Weighted Source IP Hash	Based on the Source IP Hash algorithm, the device forwards the traffic in proportion to the weights of the routes bound with LLB rules. The route with a higher weight receives more traffic from outbound links.
Weighted Least Bandwidth	Based on the Least Bandwidth algorithm, the device forwards traffic in proportion to the weight of each route bound with LLB rules. After new traffic is generated, the device selects the link with the minimum bandwidth ratio. The bandwidth ratio of a link is calculated based on the following formula: The upstream bandwidth, downstream bandwidth, or sum of the upstream and downstream bandwidth on the interface/The route weight.
Weighted Round Robin	Based on the Round Robin algorithm, the device forwards the traffic in proportion to the weight of each route bound with LLB rules. The route with a higher weight receives more traffic from outbound links.

Configuring LLB Profile

The LLB profile contains the parameters of the load balancing algorithm, such as Preferred Balance Algorithm, Balance Direction, and Persistence Method. To configure an LLB profile, take the following steps :

1. Select **Load Balance** > **Link Load Balancing** > **Profile**.

2. Click **New**.



In the LLB Profile Configuration dialog box, configure as follows:

Option	Description
Profile Name	Specify the Profile name, whose length range is 1-95 characters.
Description	Configure additional details for the LLB profile.
Preferred Balance Algorithm	Specify the preferred balancing algorithm. After you set the parameter, the system selects a route for outbound traffic based on the specified algorithm. For more information about load balancing algorithms, see the Load Balancing Algorithms section.
Balance Direction	This parameter is available when you set the Preferred Balance Algorithm parameter to Least Bandwidth or Weighted Least Bandwidth. You can use this parameter to specify the balancing direction of traffic load. The system calculates the bandwidth of links based on the specified balancing direction. Valid values: • Upstream: The system calculates the outbound bandwidth of data traffic, and then adjusts the routing method. • Downstream:The system calculates the inbound bandwidth of data traffic, and then adjusts the routing method.

Option	Description
	• Bidirection: The system calculates the sum of the inbound and outbound bandwidth of data traffic, and then adjusts the routing method. This is the default value.
Secondary Algorithm	This parameter is available when you set the Preferred Balance Algorithm parameter to ISP. You can use this parameter to specify the secondary algorithm of LLB. If multiple links are matched with the ISP of the destination IP address of the traffic, the system needs to select another route from these links based on the secondary algorithm.
Alternative Balance Algorithm	This parameter is available when you set the Preferred Balance Algorithm parameter to ISP. You can use this parameter to specify the alternative balancing algorithm. If all the links selected based on the ISP algorithm are busy, or no ISP link is matched, the system needs to select another route based on the alternative balancing algorithm.
Persistence Method	Specify the session persistence method of LLB. The system forwards the traffic that meets the specified condition to the same outbound link. Valid values: • --- : No session persistence is configured. • Source IP and Destination IP: The traffic that is from the same client and shares the same destination IP address is forwarded to the same link. • Source IP: The traffic that is from the same client is forwarded to the same link. • Destination IP: The traffic that shares the same destination IP address is forwarded to the same link. **Note**: If the link selected in session persistence is busy, the system selects another link based on the specified balancing algorithm. If all links are busy, the link selected in session persistence continues to be served as the outbound link.

Option	Description
Timeout	Specify the timeout period of session persistence. If the actual timeout period exceeds the specified threshold, the device clears the information of the corresponding data traffic. The value of this parameter ranges from 60 to 65535 and defaults to 300. Unit: seconds.
Balance Direction	Specify the direction of data traffic when the link bandwidth utilization is calculated. Valid values: • Upstream: The system compares the outbound bandwidth utilization of data traffic with the bandwidth utilization threshold of the interface, and then adjusts the routing method. • Downstream: The system compares the inbound bandwidth utilization of data traffic with the bandwidth utilization threshold of the interface, and then adjusts the routing method. • Bidirection: The system compares the larger of the inbound and outbound bandwidth utilization of data traffic with the bandwidth utilization threshold of the interface, and then adjusts the routing method.
Description	Configure additional details for the LLB profile.

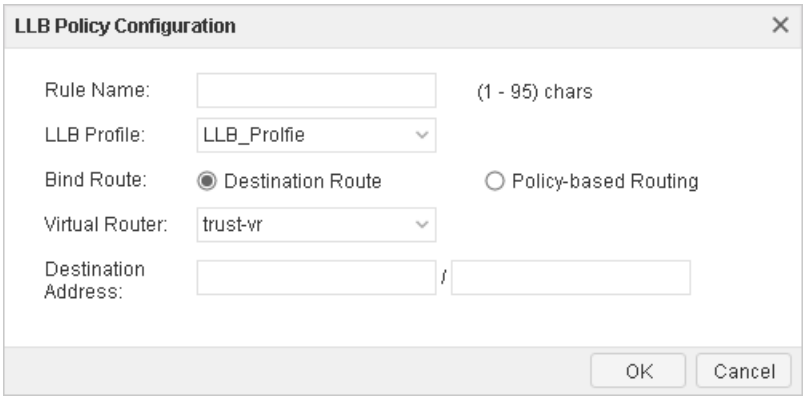
3. Click **OK**.

Configuring LLB Rule

The LLB Profile and the route is bound by the formation of LLB rules that currently support binding destination routing (DBR) and policy-based routing (PBR).

1. Select **Load Balance** > **Link Load Balancing** > **Rule**.

2. Click **New**.



In the LLB Policy Configuration dialog box, configure as follows:

Option	Description
Rule Name	Specify the rule name, whose length range is 1-95 characters.
LLB Profile	Specify the profile to be bound in the rule.
Bind Route	Specify the route to be bound in the rule: Destination Route or Policy-based Routing. • Destination Route - Select this option to specify the virtual router and destination address of the destination route. The destination network segment of the route should be consistent with the network segment of the LLB rule. • Policy-based Routing - Select this option to specify the name and ID of the policy-based route.

3. Click **OK**.

Chapter 5 Global Server Load Balance

Global Server Load Balance (GSLB) is implemented based on DNS services. In a multi-data center environment, when a client initiates a DNS query, GSLB will resolve the query based on the location, operator and other information of the client, and return the optimal resolution record to direct the traffic intelligently, so that users in different locations or with different operators can access the nearest server to obtain the service in the optimal path.

To enable GSLB, you need to install the GSLB license and ensure the license is not expired.

This section includes the following topics:

- Implementing GSLB and configuring Smart DNS. See Load Balance > Global Server Load Balance > Smart DNS.
- Configuring a DNS server, including configuration view, master zone, forward zone, recursive query, etc. See Load Balance > Global Server Load Balance > DNS Server.
- GSLB will continuously monitor the health status of all servers and perform health checks on them. See Load Balance > Health Check.
- GSLB will obtain the system load status of the devices in its zone, and monitor the memory utilization and CPU utilization of system. See Load Balance > System Load Detection.

DNS Server

This section includes the following topics:

Implementation Process

This section takes the view with all configuration being enabled as an example to illustrate the implementation of the DNS server module. You can refer to the following process.

When a domain name requested by a client reaches the ADC, the device will first find the matched DNS view according to source and destination addresses of the client. Then, the device will perform DNS resolution according to the view configuration.

1. After a view is matched, system will, according to the longest domain matching algorithm, match the domain name requested by the client with domain names of master zones configured in the view.

2. If a master zone is matched, the domain name will be resolved by it. The process is as follows:
   2.1) The domain name will first be resolved by Smart DNS of the master zone. If resolved successfully, the result will be returned to the client.
   2.2) If the resolution fails, system will continue to query for resource records. If resolved successfully, the result will be returned to the client.
   If all profiles of the master zone fail to resolve the domain name, system will return a corresponding status code to the client, which means the resolution fails.

3. If no master zone is matched,
   3.1) The domain name will first be resolved by the Smart DNS configured in the view. If resolved successfully, the result will be returned to the client.
   3.2) If the resolution fails, system will continue to query for resource records cached in the view. If resolved successfully, the result will be returned to the client.
   3.3) If the resolution fails, system will continue to match forward zones configured in the view according to the longest domain matching algorithm.
   3.3.1) If a forward zone is matched, the query will be performed according to the configured forward destination

address, and the query result will be cached and returned to the client. If there is no match, a matching failure will be returned to the client.

3.3.2) If no forward zone is matched, the domain name will continue to be resolved by the Recursion and Forward in the view. The Forward takes priority over the Recursion.

Configuring the DNS Server

The DNS server configuration includes:

- Configuring DNS Views
- Configuring Zones
- Global Configuration

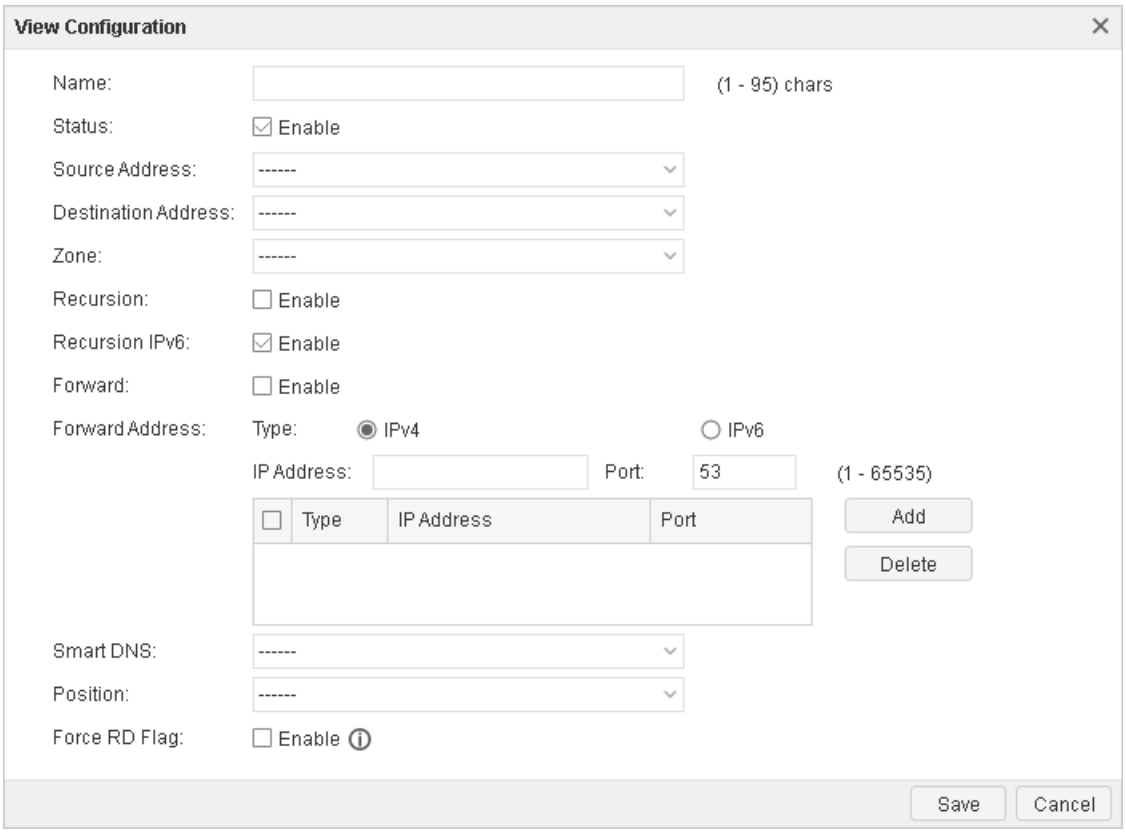
Configuring DNS Views

If the source IP and destination IP of the client match the source IP and destination IP configured in the DNS view respectively, system considers that the client request matches the DNS view. Only the client matching the view can access the associated resources in the view, such as the defined master zone, forward zone, Smart DNS, recursion and forwarding. You can create multiple DNS views, while the resources in each view cannot be shared. After the client request reaches system, system will match the client request with the rules in the DNS view from top to down.

To configure a DNS view, take the following steps:

1. Select **Load Balance** > **Global Server Load Balance** > **DNS Server**.
2. Click the **View** tab.

3. Click **New**, and the View Configuration dialog box will appear.



Configure the following options.

Option	Description
Name	Specify the name of the DNS view.
Status	Specify the status of the DNS view. You can enable or disable it.
Source Address Destination Address	Specify the source and destination IPs. Only if the client request matches the source and destination IPs configured in the view, the resources of the view can be accessed. If source and destination IPs are not configured in the view, system will select the default address **Any**, i.e., all addresses of requests will be matched.
Zone	Specify the name of the zone. For the request that matches a view, system will match it with master zones according to the longest domain name matching algorithm. If a master zone is successfully matched, the resources in the zone can be accessed. This option is optional.

Option	Description
Recursion	If the function is enabled, a DNS query will be performed by using the built-in DNS root server addresses. The cached record only belongs to its DNS view and cannot be shared with other views.
Forward	After the function is enabled, if the DNS server cannot resolve a DNS query, system will forward the query to other DNS servers, and return the query result to the client.  **Note:** If a forward zone is configured, system will first perform matching in the forward zone before forwarding. If matched successfully, the profile in the forward zone will be used for DNS resolution. Otherwise, the forward destination address configured in the DNS view will be used.
Forward Address	Specify the IP address of the DNS server. After the Forward Profile is enabled, if system cannot resolve a DNS query, it will be performed by the DNS server on this address. If multiple addresses are configured, the query will be performed regardless of the order you configured them. If no result is returned from one address, the query will be forwarded to the next address.
Smart DNS	Specify the host name of Smart DNS. "---" means no configuration.
Position	Specify the position of the rule in the DNS view list. After selecting **Before ID** or **After ID**, you need to type an ID number into the text box. Then, the selected rule will be put before or after the specified rule.

4. Click **OK**.

Configuring Zones

You can manage the resource records in the zone by configuring the zone and its domain name information. DNS zones include master zones and forward zones:

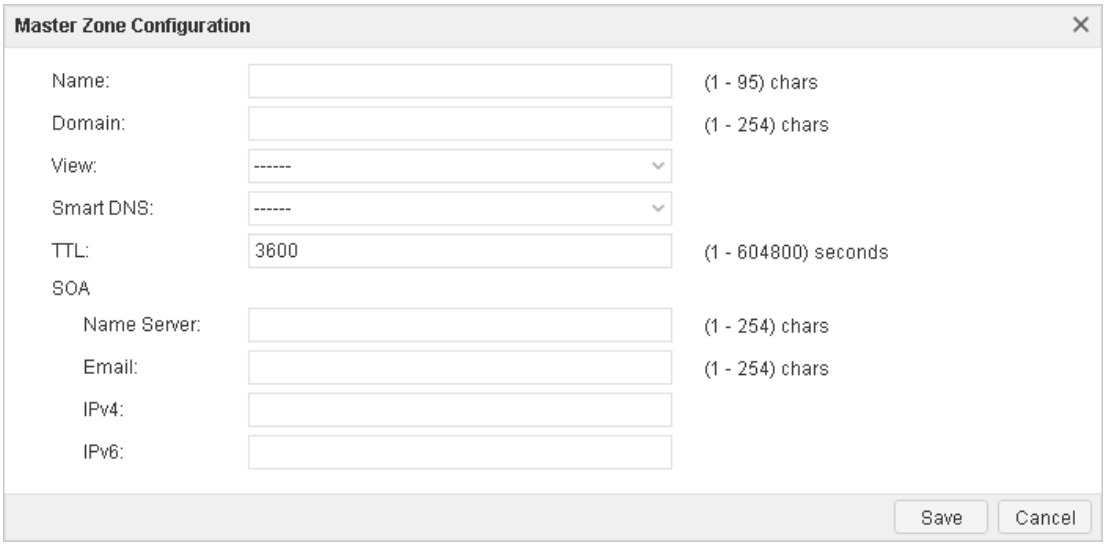
- Master Zone: An authoritative DNS server for processing client requests.
- Forward Zone: Forwards client requests with specified domain names. System will perform a query according to the configured forward destination address, and then cache the query result and return it to the client.

Note: A domain name configured in a zone should comply with the host/domain name specification, i.e., the name should include uppercase and lowercase letters, numbers, and "-". Each label (the string between two ".") of the host name cannot be blank, and the total length cannot exceed 63 bytes. The length of the domain name cannot exceed 254 bytes.

Configuring DNS Master Zones

To configure a DNS master zone, take the following steps:

1. Select **Load Balance** > **Global Server Load Balance** > **DNS Server**.
2. Click the **Zone** tab.
3. Click **New** > **Master Zone**, and the Master Zone Configuration dialog box will appear.



Configure the following options.

Option	Description
Name	Specify the name of the master zone.

Option	Description
Domain	Specify the domain name of the master zone. After being configured, neither the domain name nor name can be changed. By configuring the same domain name in different zones, you can get different results of resolving the same resource record in different views.
Smart DNS	Specify the host name of Smart DNS. "---" means no configuration.
TTL	Specify the amount of time that the domain name resolution information will be cached in the DNS. The value range is 1 to 604800 seconds. The default value is 3600 seconds, which will be used by system if no TTL has been specified for a resource record.
Name Server	Specify the name of the server that manages the master zone. You can configure a host name or a fully qualified domain name (FQDN), and the total length cannot exceed 254 bytes. After being configured, a domain name will be resolved by the authoritative DNS server. Note: 1) The name cannot be the same as the host name of CNAME. 2) If a host name is configured, the total length of the host name and the domain name in the Zone cannot exceed 254 bytes. (Each label should be separated by ".". If the domain name does not end with ".", system will automatically add one at the end.)
Email	Specify the email address of the administrator who is responsible for managing the zone, and the length should not exceed 254 bytes. Note: The email address format is "uername.domain.com". "." is used for separating instead of "@".
IPv4	Specify the IPv4 address of the name server.
IPv6	Specify the IPv6 address of the name server.

4. Click **Save**.

Configuring Resource Records

The resource record types include:

- A - Used to specify an IP address of a domain name.
- AAAA - Used to specify an IPv6 address of a domain name.
- CNAME - Used to specify an alias of a domain name. Multiple domain names can be mapped to one host.
- NS - A record of the name server information that is used to specify which DNS server to resolve a domain name.
- MX - A mail exchanger record that is used to map an email from a domain name to a corresponding mail server.
- PTR - A reverse DNS record that is used to perform a reverse DNS lookup during email sending.
- TXT - A text information record that is used to save the information related to a domain name.
- SRV - A server resource record that is used to record available services of a server.

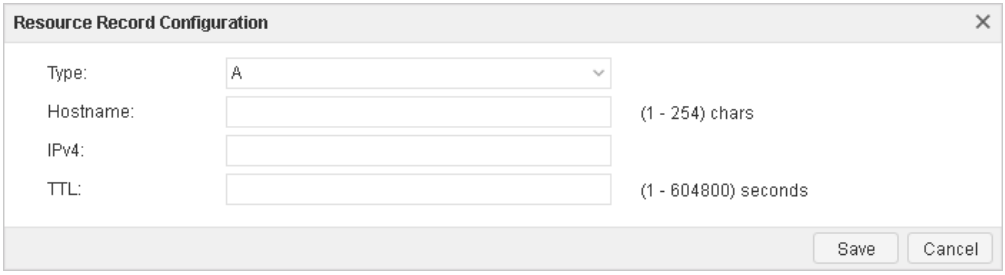
Note:

- The number of resource records in a zone is limited, and may vary depending on different platforms.
- The name of a resource record can only be configured with a host name, and cannot end with ".". The total length of the resource record name and the domain name configured in the Zone cannot exceed 254 bytes. The domain name should end with ".". If not, system will automatically add a "." at the end of the name.
- The host name should comply with the host/domain name specification, i.e., the name should include uppercase and lowercase letters, numbers, and "-". Each label (the string between two ".") of the host name cannot be blank, and the total length cannot exceed 63 bytes.

After a resource record is configured, system will automatically generate an ID. To configure a resource record, take the following steps:

1. Select **Load Balance** > **Global Server Load Balance** > **DNS Server**.
2. Click the **Zone** tab, and click the **Configuration** button under the Resource Record column in the zone list to configure the resource record for the master zone.

3. On the Resource Record page, click **New** to add a resource record; or click **Back** to return to the Zone tab.



4. In the Resource Record Configuration dialog box, configure the following options. Configuration options will vary depending on different resource records.

Option	Description
A Record: Used to specify an IP address of a domain name.	
Hostname	Specify the host name corresponding to the domain name of the DNS record.
IPv4	Specify the IPv4 address of the domain name.
TTL	Specify the amount of time that the record will be cached in the DNS server. When the TTL expires, the DNS server will update the information in its cache.
AAAA Record: Used to specify an IPv6 address of a domain name.	
Hostname	Specify the host name corresponding to the domain name of the DNS record.
IPv6	Specify the IPv6 address of the domain name.
TTL	Specify the amount of time that the record will be cached in the DNS server. When the TTL expires, the DNS server will update the information in its cache.
NS Record: A record of the name server information that is used to specify which DNS server to resolve a domain name.	
Hostname	Specify the host name corresponding to the domain name of the DNS record.
Name Server	Specify the name of the authoritative DNS server.

Option	Description
IPv4	Specify the IPv4 address of the name server.
IPv6	Specify the IPv6 address of the name server.
TTL	Specify the amount of time that the record will be cached in the DNS server. When the TTL expires, the DNS server will update the information in its cache.
MX Record: A mail exchanger record that is used to map an email from a domain name to a corresponding mail server.	
Hostname	Specify the host name corresponding to the domain name of the DNS record.
Mail Exchange	Specify the domain name of the email address of the recipient.
Priority	Specify the priority value of the MX record. The smaller the value is, the higher the priority will be. System will select the server with higher priority to send emails.
TTL	Specify the amount of time that the record will be cached in the DNS server. When the TTL expires, the DNS server will update the information in its cache.
CNAME Record: An alias record that is used to map multiple domain names to one host.	
Hostname	Specify the host name corresponding to the domain name of the DNS record.
Alias	Specify the alias of the domain name of the DNS record.
TTL	Specify the amount of time that the record will be cached in the DNS server. When the TTL expires, the DNS server will update the information in its cache.
PTR Record: A pointer record that is used to perform a reverse DNS lookup.	
Hostname	Specify the host name corresponding to the domain name of the DNS record.
Record	Specify the PTR record information, which is usually the domain name corresponding to the MX record.

Option	Description
TTL	Specify the amount of time that the record will be cached in the DNS server. When the TTL expires, the DNS server will update the information in its cache.
TXT Record: A text information record.	
Hostname	Specify the host name corresponding to the domain name of the DNS record.
Record	Specify the text information of the domain name.
TTL	Specify the amount of time that the record will be cached in the DNS server. When the TTL expires, the DNS server will update the information in its cache.
SRV Record: A server resource record that is used to record available services of a server.	
Hostname	Specify the host name corresponding to the domain name of the DNS record.
Priority	Specify the priority value of the server if there are multiple servers that can provide same services. The smaller the value is, the higher the priority will be.
Port	Specify the port that provides services.
Weight	Specify the priority value of the SRV record. The smaller the value is, the higher the priority will be.
Record	Specify the SRV record information.
TTL	Specify the amount of time that the record will be cached in the DNS server. When the TTL expires, the DNS server will update the information in its cache.

5. Click **Save**.

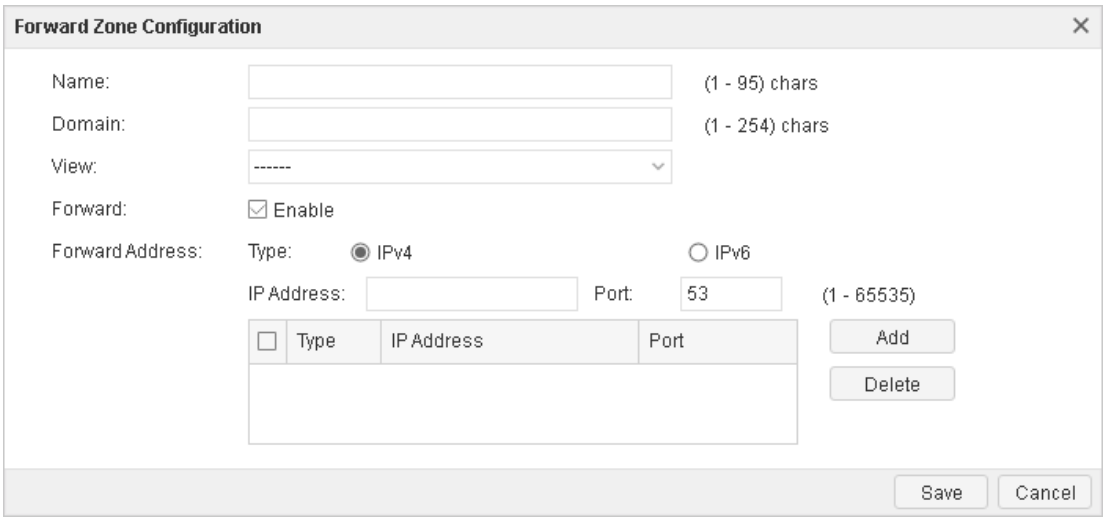
Configuring DNS Forward Zones

To configure a DNS forward zone, take the following steps:

1. Select **Load Balance** > **Global Server Load Balance** > **DNS Server**.

2. Click the **Zone** tab.

3. Click **New** > **Forward Zone**, and the Forward Zone Configuration dialog box will appear.



Configure the following options.

Option	Description
Name	Specify the name of the forward zone.
Domain	Specify the domain name of the forward zone.
Forward	After the function is enabled, if the DNS server cannot resolve a DNS query, system will forward the query to other DNS servers, and return the query result to the client.
Forward Address	Specify the IP address of the DNS server. After the Forward Profile is enabled, if system cannot resolve a DNS query, it will be performed by the DNS server on this address.

4. Click **Save**.

Configuring the Global Configuration

The global configuration can function as a DNS view too, i.e., a view in which source and destination addresses of client requests are both **Any**. The view of global configuration is independent of other user-defined views, and it will not be

displayed in the view list. When a client request reaches the device, the global configuration will be the last view to be matched.

To configure the global configuration, take the following steps:

1. Select **Load Balance** > **Global Server Load Balance** > **DNS Server**.

2. In the Global Configuration tab, configure the following options.

Option	Description
Listen Address	Configure the IP address on which the DNS server will provide services. IPv4 or IPv6 addresses are supported. Type the listen address into the **IP Address** text box, and then click **Add** to add an IP address to be listened. Click **Delete** to cancel the listening on

Option	Description
	the selected server.
Listen Port	Configure the TCP and UDP port on which the DNS will provide services. The default port is 53. The port is effective for both TCP and UDP.
Smart DNS	Select the host name of Smart DNS. "---" means no configuration.
Recursion	If the function is enabled, a DNS query will be performed using the built-in DNS root server addresses. Only IPv4 root servers can be queried.
Recursion IPv6	If the function is enabled, a DNS query will be performed according to the built-in DNS root server addresses, and IPv6 root servers can be queried.
Forward	After the function is enabled, if the DNS server cannot resolve a DNS query, system will forward the query to other DNS servers, and return the query result to the client.  **Note:** If a forward zone is configured, system will first perform matching in the forward zone before forwarding. If matched successfully, the profile in the forward zone will be used for DNS query. Otherwise, the forward destination address configured in the DNS view will be used.
Forward Address	Specify the IP address of the DNS server. You can assign an IPv4 or IPv6 address. After the Forward Profile is enabled, if system cannot resolve a DNS query, it will be performed by the DNS server on this address. If multiple addresses are configured, the query will be performed regardless of the configured order. If no result is returned from one address, the query will be forwarded to the next address.
Cache	Specify the cache size of each DNS view. The DNS resolution results obtained through the recursive query will be stored in the view cache, and each view is independent of the others.
Log	Select the **Enable** check box to record GSLB logs.

Option	Description
Statistics	Select the **Enable** check box to collect statistics on GSLB.
UDP Session Timeout	Configure the UDP timeout setting. • Select the **Timeout** radio button, and specify the UDP timeout value. If no server response has been received within the timeout period, system will delete the UDP packet request. • Select the **Invalid after Answering** radio button. System will delete the UDP packet request after the server answers the request.

3. Click **OK**.

Configuring Smart DNS

System can not only resolve a domain name to an IP address closest to the source geographic location of the DNS request, but also resolve DNS requests of different ISP users to the IP addresses for corresponding ISPs, which can reduce the cross-region and cross-ISP access. Such resolution method is known as Smart DNS.

Smart DNS can be referenced by the DNS global configuration, view and master zone, and has the highest search priority. However, it can only resolve A or AAAA DNS records.

Configuring Smart DNS

The Smart DNS configuration includes:

1. Configuring the ISP
2. Configuring Regions
3. Configuring Servers and Server Pools
4. Configuring DNS Hosts

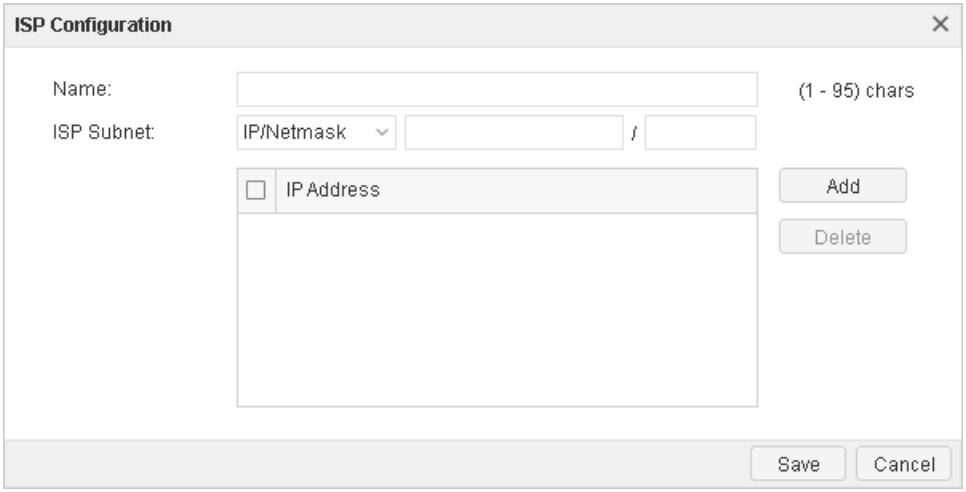
Configuring the ISP

System has four predefined ISPs: China Telecom, China Unicom, China Mobile and CERNET, which cannot be deleted or renamed.

To customize an ISP, take the following steps:

1. Select **Load Balance** > **Global Server Load Balance** > **ISP**.

2. Click **New**, and the ISP Configuration dialog box will appear.



Configure the following options.

Option	Description
Name	Specify the name of the ISP you want to create.
ISP Subnet	Specify an IP subnet for the ISP.

3. Click **Save**.

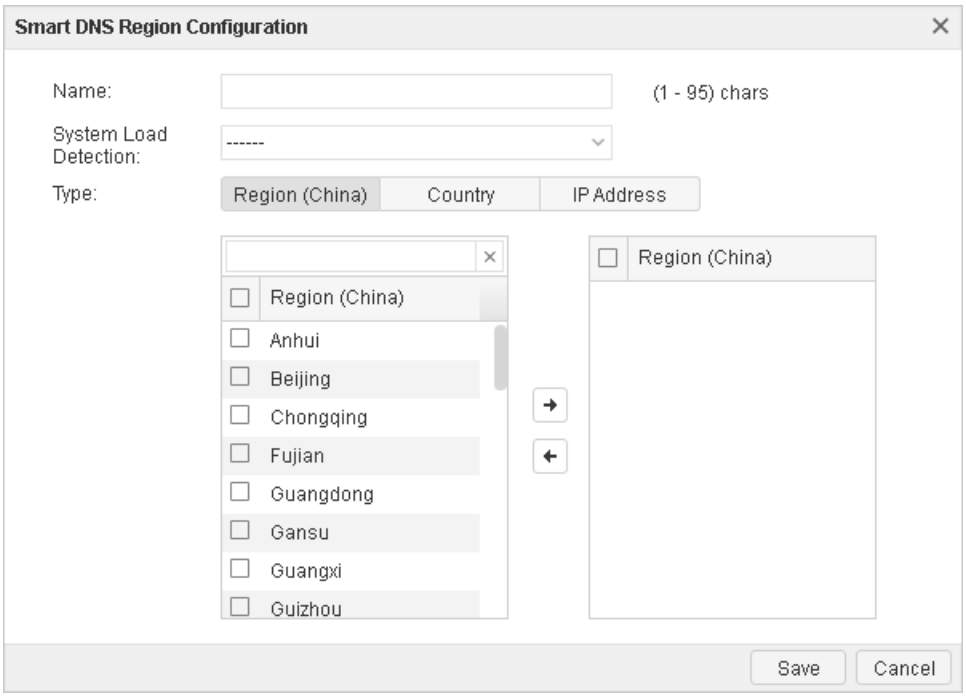
Note: Predefined and user-defined ISPs can be referenced in the Region.

Configuring Regions

To create a region, take the following steps:

1. Select **Load Balance** > **Global Server Load Balance** > **Region**.

2. Click **New**, and the Smart DNS Region Configuration dialog box will appear.



Configure the following options.

Option	Description
Name	Specify the name of the region you want to create.
Type	Add a province/region, a country, an ISP or an IP subnet under the "Region (China)", "Country", "IP Address" or "ISP" types accordingly. If you add multiple types at the same time, the matching priority of the client source address is: user-defined IP subnet > user-defined ISP > predefined ISP > province/region > country. If multiple items are configured under the same type, as long as the client source address matches any of them, the region is matched.

3. Click **Save**.

Configuring Servers and Server Pools

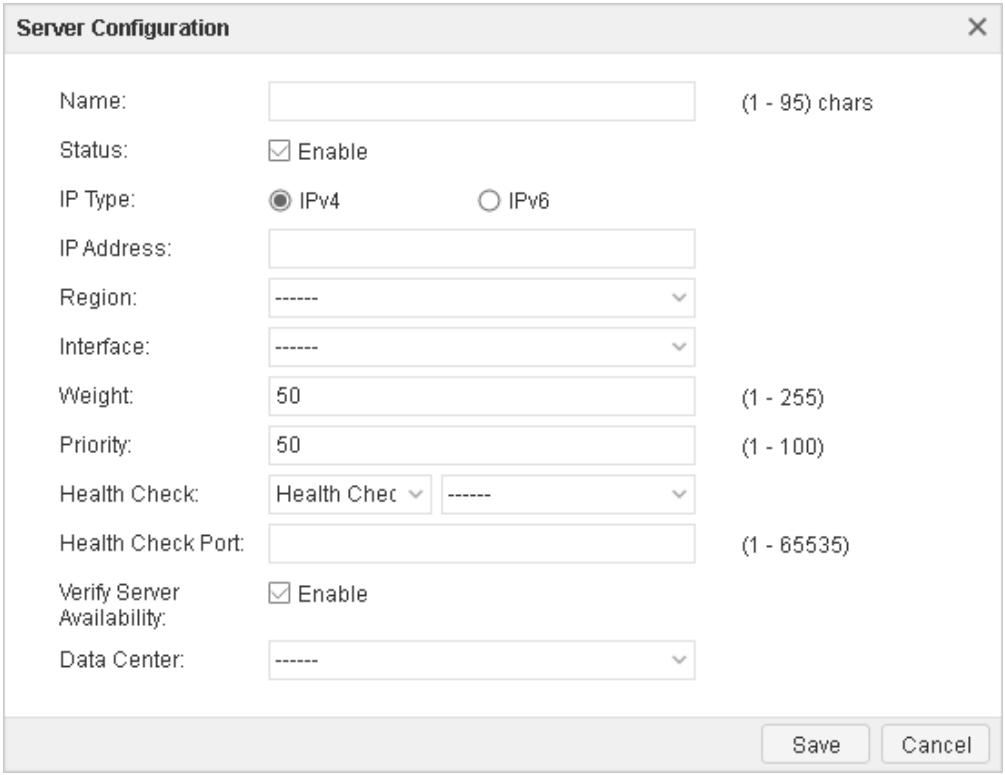
A server provides services to DNS hosts, while a server pool is a group of servers.

To create a server, take the following steps:

1. Select **Load Balance** > **Global Server Load Balance** > **Smart DNS**.

2. Select the **Server** tab.

3. Click **New**, and the **Server Configuration** dialog box will appear.



Configure the following options.

Option	Description
Name	Specify the name of the server that provides services.
Status	Enable or disable the server. The disabled server will be unavailable.
IP Type	Specify the IP address type of the server. You can select the IPv4 or IPv6.
IP Address	Specify the IP address of the server.
Region	Specify the region to which the server belongs. If the server pool is configured with the typology algorithm, servers will be categorized according to regions. After that, when the client source address matches a certain region,

Option	Description
	the servers in the region can be accessed.
Interface	Select an interface for the server from the drop-down list. When server pool to which the server belongs enables the Busy Protect function, whether the server is busy is determined by the bandwidth utilization of its bound interface . If the bandwidth utilization of interface reaches configured threshold, the server is considered as busy and system will not distribute client requests to it. When server pool to which the server belongs selects "Dynamic Promixity" as load balance algorithm, system will record the sum of upstream and downstream bandwidth utilization of the interface bound to each server in this server pool. Then system will distribute client requests to the server with the least sum.
Weight	Specify the weight of the server. When the server pool is configured with the weighted round robin algorithm, system will return the server's IP according to the weight.
Priority	Specify the priority value of the server. The value range is 1 to 100. The default value is 50. The smaller the value is, the higher the priority of the server will be.
Health Check	Select a health check or health check group to check the availability of various servers. Note: When the server member or its server pool is not configured with health checks, the availability of the server member is determined by the health check result of the corresponding device configured in the local data center. For more information about data centers, see Data Center.
Health Check Port	Specify the port for the health check.
Verify Server Availability	Select Enable to enable the Verify Server Availability function. After the function is enabled, the system determines whether the server can be used based on the availability of physical devices in the corresponding data center.

Option	Description
Data Center	Specify the data center of the server.

4. Click **Save**.

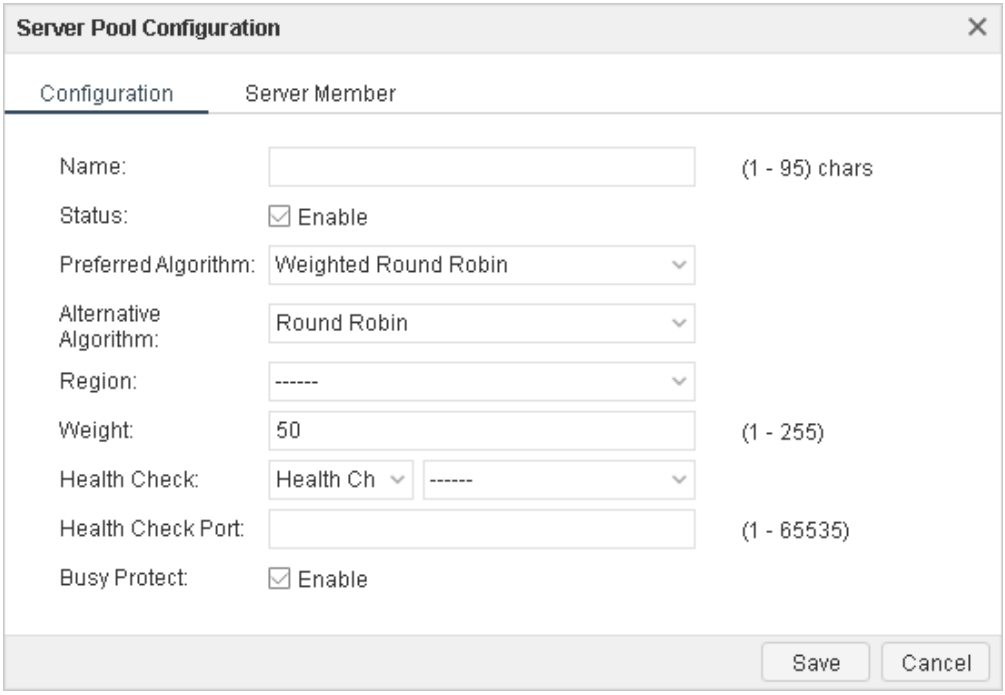
Note: For the device with IPv4-only firmware, if you configure an IPv6 address for a server member, the member's availability cannot be determined through health check.

To create a server pool, take the following steps:

1. Select **Load Balance** > **Global Server Load Balance** > **Smart DNS**.

2. Select the **Server Pool** tab.

3. Click **New**, and the Server Pool Configuration dialog box will appear.



Configure the following options.

Option	Description
Name	Specify the name of the server pool that provides services.

Option	Description
Status	Enable or disable the server pool. The disabled server pool will be unavailable.
Preferred Algorithm	Select a preferred load balance algorithm, including: • Round Robin: Client requests will be distributed to each server in turn. • Weighted Round Robin (Default): According to their performance, servers will be given different weights. The device will distribute client requests in proportion to weights of servers. The server with higher weight will receive a higher proportion of requests. • IP Hash: The source address of a client will be hashed, and then the client will be allocated with a server according to the hash value. If the server list remains unchanged, clients on the same IP address will be allocated with the same server every time. • Topology: A server will be allocated according to the region to which the client source address belongs. If there are multiple servers configured for the same region, the server IP with higher weight will be returned. • All: If the option is selected, the number of server IPs returned (up to 16 IPs) can be configured. • Priority: A server will be allocated according to the priority value. The server with higher priority will receive a higher proportion of requests. The smaller the priority value is, the higher the priority of the server will be. • Dynamic Ratio: According to the different processing capabilities of servers, the device calculates different dynamic weights. The device will distribute client requests in proportion to dynamic weights of servers. The server with higher dynamic weight will receive a higher pro-

Option	Description
	portion of requests. If the dynamic weight is 0, the server will not be distributed with requests. In general, the dynamic weight value is calculated by the SNMP health check; in other cases, the value of 1 means that the server can provide services, while 0 means it is unavailable. • Dynamic Promixity： System will record the sum of upstream and downstream bandwidth utilization of the interface binding to servers. When a new connection is requested , system will distribute the latest request to the server with the least sum.
Alternative Algorithm	Select an alternative load balance algorithm, including: • Drop: Client requests will be dropped and server resources will no longer be allocated. • Round Robin (Client): Client requests will be distributed to each server in turn. • Weighted Round Robin: According to their performance, servers will be given different weights. The device will distribute client requests in proportion to weights of servers. The server with higher weight will receive a higher proportion of requests. • IP Hash: The source address of a client will be hashed, and then the client will be allocated with a server according to the hash value. If the server list remains unchanged, clients on the same IP address will be allocated with the same server every time. • Topology: A server will be allocated according to the region to which the client source address belongs. If there are multiple servers configured for the same region, the server IP with higher weight will be returned. • All: If the option is selected, the number of server IPs returned (up to

Option	Description
	16 IPs) can be configured. • Priority: A server will be allocated according to the priority value. The server with higher priority will receive a higher proportion of requests. The smaller the priority value is, the higher the priority of the server will be. • Dynamic Ratio: According to the different processing capabilities of servers, the device calculates different dynamic weights. The device will distribute client requests in proportion to dynamic weights of servers. The server with higher dynamic weight will receive a higher proportion of requests. If the dynamic weight is 0, the server will not be distributed with requests. In general, the dynamic weight value is calculated by the SNMP health check; in other cases, the value of 1 means that the server can provide services, while 0 means it is unavailable. • Dynamic Proximity： System will record the sum of upstream and downstream bandwidth utilization of the interface binding to servers. When a new connection is requested , system will distribute the latest request to the server with the least sum.
Region	Specify the region to which the server pool belongs. If the DNS host is configured with the typology algorithm, server pools will be categorized according to regions. After that, when the client source address matches a certain region, the servers in pools in the region can be accessed.
Weight	Specify the weight of the server pool. When the DNS host is configured with the weighted round robin algorithm, system will select a server pool according to the weight.
Health Check	Select a health check or health check group to check the availability of various servers.
Health Check	Specify the port for the health check.

Option	Description
Port	
Busy Protect	Select the **Enable** check box to enable the busy protect function of server members. After the function is enabled, when the bandwidth utilization of interface bound to a server member reaches configured threshold, system will consider the server is busy. If the server selected based on preferred algorithm is busy, system will continue to select another server through alternative algorithm. If servers selected based on both preferred algorithm and alternative algorithm are busy, system will ignore the busy protect function and select a server through algorithm again.
Server Member	In the Server Member tab, select a server you have created. After being saved, the selected server will be included in the server pool.

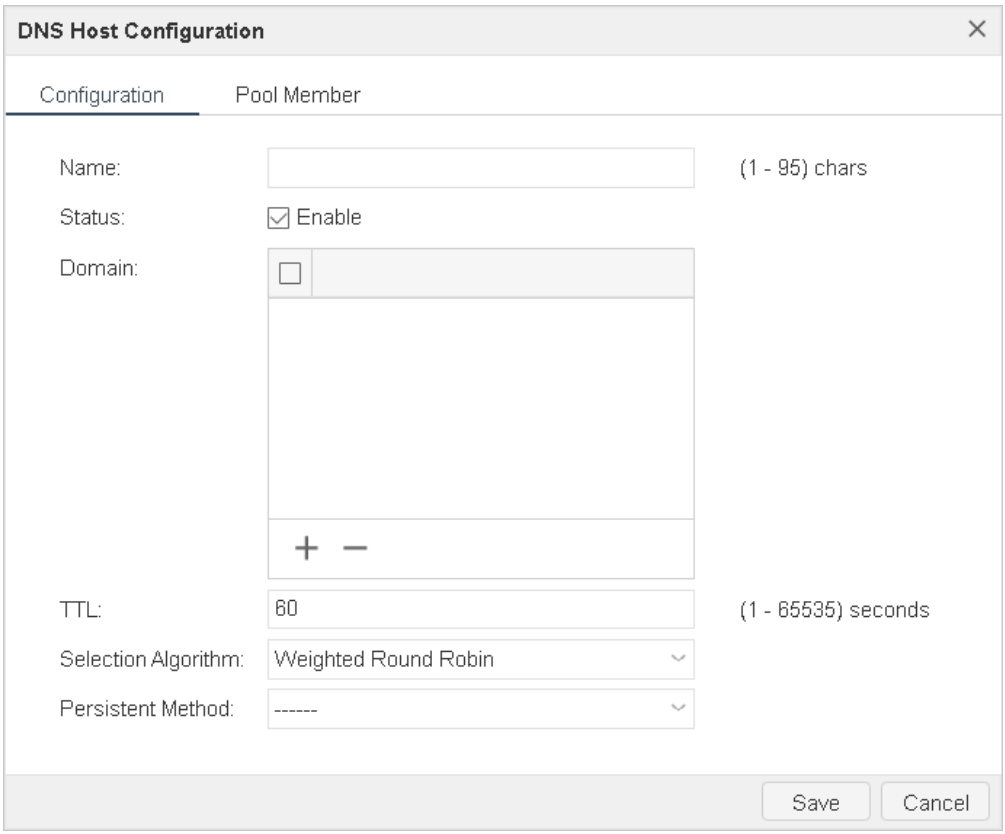
4. Click **Save**.

Configuring DNS Hosts

To create a DNS Host, take the following steps:

1. Select **Load Balance** > **Global Server Load Balance** > **Smart DNS**.
2. Select the **DNS Host** tab.

3. Click **New**, and the DNS Host Configuration dialog box will appear.



Configure the following options.

Option	Description
Name	Specify the name of the DNS host.
Status	Enable or disable the DNS host. The disabled DNS host will be unavailable.
Domain	Specify the domain name that needs to be resolved by Smart DNS. You can add 1 to 128 domain names and domain names with the wildcard * in the host segment. Only if all domain names configured for the DNS host belong to the domain of a certain zone can the DNS host be bound to the zone.
TTL	Specify the amount of time that the A or AAAA records returned by Smart DNS to the client will be cached. Within the TTL, if the client requests the domain name again, the record in the cache will be used. If the TTL is

Option	Description
	expired, the cached record will be deleted, and system will resolve the domain name again.
Selection Algorithm	Specify a load balance algorithm.
Pool Member	Select a pool member you have created. The selected member will provide services to the DNS host.

4. Click **Save**.

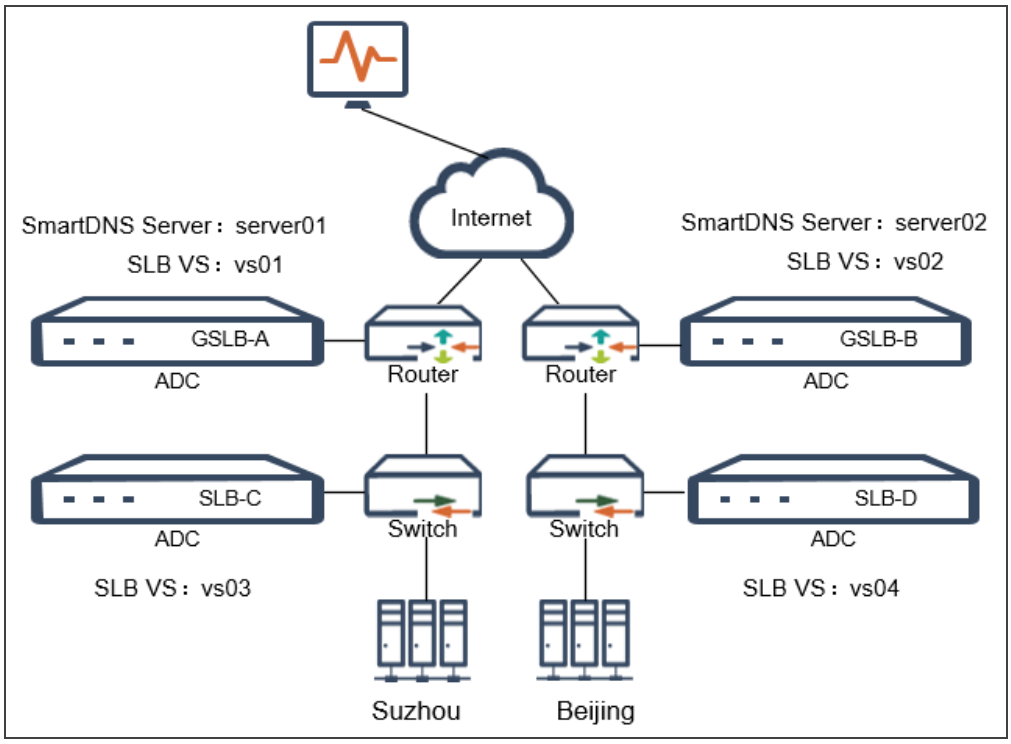
Data Center

The system allows you to configure data centers and create a sync group for multiple GSLB devices in different data centers. This group synchronizes the configuration and status of the GSLB devices to implement load balancing. Assume that a sync group of data centers is created. When the client sends a DNS request, the system resolves the request based on the client location and returns the optimal resolution record to the client. If the data center that is nearest to the client cannot provide services, the system returns a server address in another data center to the client. This way, the client can access data without interruption. In addition, data centers can automatically add SLB virtual servers to smart DNS servers to provide services for the client. Generally, you cannot enable this function and the device cluster function at the same time.

Data centers include local data centers and remote data centers. A local data center configured in a GSLB device is considered as a remote data center in another device. After you configure a local data center and remote data center for each ADC device, a GSLB sync group is created for the devices. All the ADC devices in the sync group synchronize their own GSLB configurations, except the health check configuration and the listening address of DNS servers.

For SLB devices that are not configured with data centers (the ADC devices that enable the SLB function), you can register these devices into the corresponding data centers based on their locations. This way, the GSLB devices corresponding to the data centers can automatically or manually add SLB virtual servers to smart DNS servers, synchronize these devices in the GSLB sync group, and then provide services for the client.

Typical Scenario



For example, the system contains two data center nodes which are in Suzhou and Beijing respectively. Deploy Devices GSLB-A and SLB-C for the node in Suzhou, and deploy Devices GSLB-B and SLB-D for the node in Beijing. Create a GSLB sync group for Devices GSLB-A and GSLB-B, register Device SLB-C into the Suzhou node, and register Device SLB-D into the Beijing node. Then, configure the smart DNS server server01 and SLB virtual server vs01 in Device GSLB-A, configure the SLB virtual server vs03 in Device SLB-C, configure the smart DNS server server02 and SLB virtual server vs02 in Device GSLB-B, and configure the SLB virtual server vs04 in Device SLB-D.

After the preceding configurations are complete, the smart DNS server list of Devices GSLB-A and GSLB-B displays the following servers: server01, server02, vs01, vs02, vs03, and vs04. Therefore, when the client sends a DNS request, the system returns the optimal server IP address based on the client location and the status of each server. This implements the GSLB function in a multi-data center environment.

Configuring Data Centers

To configure data centers to create a GSLB sync group, take the following steps:

1. Configure a local data center for a GSLB device based on its own location. For more information, see the Configuring a Local Data Center section.
2. Add a remote data center to the GSLB device to create a GSLB sync group. For more information, see the Adding a Remote Data Center section.
3. Configure the IP address and port number used for registration in the ADC devices that enable the SLB function. For more information, see the Registering SLB Devices into a Data Center section.
4. Register the local devices into the data center.

Configuring a Local Data Center

If you want to create a GSLB sync group for a device, you should configure a local data center and add a remote data center for the device.

To configure a local data center, take the following steps:

1. Select Load Balancing > Global Server Load Balancing > Data Center.
2. Click New, and the Data Center Configuration dialog box will appear.

In the Data Center Configuration dialog box, configure the following options:

Option	Description
Name	Specify the name of the local data center, which can be 1 to 95 characters in length. The name must be unique in a GSLB sync group.
Node ID	Specify the node ID of the local data center. The node ID must be unique in a GSLB sync group.
Type	Select Local to specify the data center as the local one.
IP Address	Specify the IP address of the interface as that of the local data center. This IP address must be accessible to the IP address of the remote data center.
Contact	Specify the contact of the local data center, which can be 0 to 127 characters in length.
Location	Specify the location of the local data center, which can be 0 to 127 char-

Option	Description
	acters in length.
Virtual Server Discovery	Select Enable to enable the Virtual Server Discovery function. Assume that the function is enabled. When a GSLB sync group is created, the system automatically discovers the newly added SLB virtual servers from the system and local devices. You can view these servers in Load Balancing > Global Server Load Balancing > Smart DNS > Server. Note: For virtual servers that are created in local devices before the GSLB sync group is created, the system cannot automatically discover them. For more information about how to use these virtual servers, see the Virtual Server Discovery section.
Local Device IP/Port	Add the IP address and port number of local devices and configure them into the local data center. The local devices are the ADC devices registered into the data center. These ADC devices need to enable the SLB function. You need to configure the registration in the local devices in advance. For more information, see the Configuring a Local Device section.

3. Click Save to complete the configuration.

Adding a Remote Data Center

To add a remote data center, take the following steps:

1. Select Load Balancing > Global Server Load Balancing > Data Center.
2. Click New, and the Data Center Configuration dialog box will appear.

In the Data Center Configuration dialog box, configure the following options:

Option	Description
Name	Specify the name of the remote data center.
Node ID	Specify the node ID of the remote data center.
Type	Select Remote.

Option	Description
IP Address	Specify the IP address of the remote data center.
Contact	Specify the contact of the remote data center, which can be 0 to 127 characters in length.
Location	Specify the location of the remote data center, which can be 0 to 127 characters in length.

3. Click Save to complete the configuration.

Registering SLB Devices into a Data Center

In a device configured with the local data center, the system considers the other ADC devices registered into the data center as local devices. After local devices are registered into the corresponding local data center, the virtual server information of the local devices can be automatically or manually synchronized to all devices within the GSLB sync group. In other words, all the devices in the sync group can display the virtual servers of the local devices in Load Balancing > Global Server Load Balancing > Smart DNS > Server.

Configuring a Local Device

To configure a local device, take the following steps:

1. Select Load Balancing > Server Load Balancing > Local Device.
2. Select Enable the enable the Local Device function.

On the Local Device page, configure the following options:

Option	Description
Local Device	Select Enable to enable the Local Device function. This way, devices can be registered into the data center.
Local Device IP	Specify the IP address of the local device, which is used to be registered into the data center.
Local Device Port	Specify the port number of the local device, which is used to be registered into the data center. Default value: 1616.

Option	Description
Status	Display the status of the local device. Valid values: • Connected: The local device is registered into the data center. • Disconnected: The local device fails to be registered into the data center.

3. Click OK.

Virtual Server Discovery

After a local device is registered into the corresponding local data center, the data center cannot discover the virtual servers that have already been created by the local device. Therefore, you can manually discover virtual servers in the local device so that the devices in the GSLB sync group can reference them. To manually discover virtual servers in the local device, take the following steps:

1. Load Balancing > Global Server Load Balancing > Data Center.
2. In the top toolbar, click Virtual Server Discovery.
3. After the discovery is complete, the "Operated successfully!" message will appear.

Chapter 6 Health Check

The device can perform health checks on servers to locate and remove abnormal ones. The abnormal servers will be excluded from the available servers to ensure that client requests will be distributed to real servers that work normally.

Health check is used to check the availability of various servers. System supports multiple health check types, including TCP, UDP, HTTP, HTTPS, etc.

Besides, servers with IPv4 and IPv6 addresses are supported.

This section introduces the following topics:

Configuring Health Checks

To create a health check, take the following steps:

1. Select **Load Balance** > **Health Check** > **Health Check**.
2. Click **New**, and select a health check type. System supports to perform health checks on the following protocols: ICMP, TCP, TCP-ECHO, TCP-HALF-OPEN, UDP, HTTP, HTTPS, SMTP, POP3, IMAP, DNS, FTP, THIRD-PARTY, RADIUS-AUTHENTICATION, RADIUS-ACCOUNTING, WEBSOCKET, WEBSOCKET-SSL, SNMP-DCA, SNMP-DCA-BASE, SIP-UDP and SIP-TCP.
   Configuration options will vary depending on different protocol types. For specific configurations, see the actual page.

   In the pop-up health check configuration dialog box, configure the following options:

Option	Description
ICMP Health Check: Used to check whether a real server is up or down. When checking, the	

Option	Description
device sends an ICMP ECHO packet to a real server. Within the timeout period, if a response is received from the real server, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the

Option	Description
	value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
DSR	Select the **Enable** check box to enable the health check in the DSR mode.
Source Interface	Specify the source interface for sending health check requests.
TCP Health Check: Used to check the TCP connection status between the device and a real server. When checking, the device establishes a TCP connection with a real server and sends the specified content. Within the timeout period, if a response returned by the real server contains the expected content you have specified, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and

Option	Description
	Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the TCP connection port for the health check. If not specified, the

Option	Description
	port configured for the real server will be used by default.
DSR	Select the **Enable** check box to enable the health check in the DSR mode.
Source Interface	Specify the source interface for sending health check requests.
Send Buffer	Specify the send buffer for the health check. If the Send Buffer text box is left empty, system will only check whether the TCP connection is established successfully.
Receive	Specify the content that you expect to receive, which will be compared with a response returned by the real server: • If **Match** is selected, it means that if the response returned by the server contains the expected content you have specified, the health check is considered successful. • If **Do Not Match** is selected, it means that if the response returned by the server does not contain the expected content you have specified, the health check is considered successful. If the Receive text box is left empty, while the Send Buffer is not, system will only check whether the connection with the real server is established successfully and whether the real server can respond, rather than checking the response returned by the real server.
TCP-ECHO Health Check: Used to check the TCP connection status between the device and a real server. When checking, the device establishes a TCP connection with a real server via the ECHO port (the default port is 7), and sends a specified string. If the string returned by the real server is the same as the sent string, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.

Option	Description
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.

Option	Description
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the ECHO port for the health check. The default port is 7.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
TCP-HALF-OPEN Health Check: Used to check the TCP connection status between the device and a real server. When checking, the device will try to establish a TCP half-open connection with a real server. After sending a SYN packet to a real server, if the device receives a SYN ACK packet from the real server within the timeout period, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed.

Option	Description
	For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for the SYN ACK packet from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the TCP connection port for the health check.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.

Option	Description
UDP Health Check: Used to check the availability of UDP services on a real server. When checking, the device sends the specified content to a real server over UDP. Within the timeout period, if a response returned by the real server contains the expected content you have specified, the health check is considered successful. If the number of consecutive failures exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the for-

Option	Description
	mula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Port	Specify the UDP port for the health check. If not specified, the port configured for the real server will be used by default.
Source Port	Specify the UDP source port for the health check. If not specified, the default UDP port will be used by default.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
Send Buffer	Specify the send buffer for the health check. If the Send Buffer text box is left empty, system will only check whether an UDP packet can reach the real server.
Receive	Specify the content that you expect to receive, which will be compared with a response returned by the real server: • If **Match** is selected, it means that if the response returned by the server contains the expected content you have specified, the health check is considered successful.

Option	Description
	• If **Do Not Match** is selected, it means that if the response returned by the server does not contain the expected content you have specified, the health check is considered successful. If the Receive text box is left empty, while the Send Buffer is not, system will check whether an UDP packet can reach the real server, and whether the real server can respond, rather than checking the response returned by the real server.
HTTP/HTTPS Health Check: Used to check the availability of HTTP/HTTPS services on a real server. When checking, the device sends the specified content to a real server over HTTP/HTTPS. Within the timeout period, if a response returned by the real server contains the expected content you have specified, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the

Option	Description
	expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the UDP port for the health check. If not specified, the port configured for the real server will be used by default.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
Path	Specify the URL request path for the health check. The default path is "/".
Receive	Specify the content that you expect to receive, which will be compared with a

Option	Description
	response returned by the real server: • If **Match** is selected, it means that if the response returned by the server contains the expected content you have specified, the health check is considered successful. • If **Do Not Match** is selected, it means that if the response returned by the server does not contain the expected content you have specified, the health check is considered successful. If the Receive text box is left empty, while the Path is not, system will only check whether the connection with the real server is established successfully and whether the real server can respond, rather than checking the response returned by the real server.
Status Code	Specify the HTTP/HTTPS status code you expect to receive. If a response returned by the server contains the status code, the health check is considered successful. After both the Receive and Status Code are configured, only if the response returned by the server contains both of them will the health check be considered successful. You can specify multiple status codes, and should separate them by semicolon ";", e.g., "200;302;503". Besides, the wildcard "x" can be included in the status code, such as "30x; 5xx,", but it cannot be placed between two numbers, e.g., "2x3".
Advanced Configuration	
User Agent	Specify the User Agent field for the HTTP/HTTPS health check. The specified User Agent field will be included in the request which is to be sent for the health check. The default field is "HealthCheckClient".
Hostname	Specify the Host field for the HTTP/HTTPS health check. The specified Host field will be included in the request which is to be sent for the health check. The IP address of the real server will be referenced by default.
HTTP Version	Specify the HTTP version for the HTTP health check. The specified HTTP version will be included in the request which is to be sent for the health

Option	Description
	check.
User-defined Request	Specify all the content of the HTTP request message for the HTTP health check. If specified, the content in this user-defined request will **first** be included in the request which is to be sent for the HTTP health check.
SNI	You can enable SNI for the HTTPS health check. If enabled, SNI allows the client to include the requested host name in the first message of its SSL hand-shake, so that the server can determine the correct domain and return cor-responding certificates.
SMTP Health Check: Used to check the availability of SMTP services on a real server. When checking, the device first establishes a TCP connection with a real server, and sends a HELO or QUIT packet to the real server. Within the timeout period, if a SMTP HELO or QUIT response is received from the real server, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is con-sidered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the

Option	Description
	specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the UDP port for the health check. If not specified, the port configured for the real server will be used by default.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
Domain	Specify the host name of the SMTP mail sender.

Option	Description
POP3 Health Check: Used to check the availability of POP3 services on a real server. When checking, within the timeout period, if the device can successfully connect to a real server, and can log out the server after logging in with the specified username and password, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the for-

Option	Description
	mula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the UDP port for the health check. If not specified, the port configured for the real server will be used by default.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
User name	Specify the username for logging into the real sever.
Password	Specify the password corresponding to the username.
IMAP Health Check: Used to check the availability of IMAP services on a real server. When checking, within the timeout period, if the device can successfully connect to a real server, and can log out the server after logging in with the specified username and password, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.

Option	Description
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9

Option	Description
	seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the UDP port for the health check. If not specified, the port configured for the real server will be used by default.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
User name	Specify the username for logging into the real sever.
Password	Specify the password corresponding to the username.
Folder	Specify the folder on the real server for the health check.
DNS Health Check: Used to check the availability of DNS services on a real server. When checking, the device sends the specified domain name to a real server. Within the timeout period, if the data returned by the real server contains the IP address corresponding to the domain name, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers.

Option	Description
	• By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.

Option	Description
Retry Interval	Specify the interval between each retry.
Port	Specify the UDP port for the health check. If not specified, the port configured for the real server will be used by default.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
Domain	Specify the domain name for the health check. If the domain name is empty, it means that once a DNS response is received from the real server, the health check is considered successful.
IP	Specify the IP address corresponding to the specified domain name, which will be compared with the IP address returned by the real server. You can configure an IPv4 or IPv6 address. • If **Match** is selected, it means that if the response returned by the server contains the expected content you have specified, the health check is considered successful. • If **Do Not Match** is selected, it means that if the response returned by the server does not contain the expected content you have specified, the health check is considered successful. If the IP is left empty, it means that once a DNS response is received from the real server, the health check is considered successful.
FTP Health Check: Used to check the availability of FTP services on a real server. When checking, within the timeout period, if the device can successfully connect to a real server, and can log out the server after logging in with the specified username and password, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP

Option	Description
	address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response

Option	Description
	after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the port for the health check. If not specified, the port configured for the real server will be used by default.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server. **Note:** The function will be disabled if you select the Port Mode for the FTP data channel.
Source Interface	Specify the source interface for sending health check requests.
Mode	Specify the mode of the FTP data channel, including Port Mode and Passive Mode. The default option is Passive Mode.
Anonymous Login	Specify whether to log in anonymously. If you select **Yes**, the User Name text box will be filled with "anonymous" and cannot be changed.
User name	Specify the username for logging into the real sever.
Password	Specify the password corresponding to the username.
File Name	Specify the path and name of a to-be-downloaded file. If the file is down-loaded successfully, the health check is successful.
SNMP-DCA Health Check: Used to check the CPU, memory and disk usage of a real server using predefined OIDs.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.

Option	Description
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real

Option	Description
	server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the port for the health check. If not specified, the default SNMP port (161) will be used.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
Community	Specify the community for the SNMP host of the real server. Community is a password sent in clear text between the manager and the agent. You should keep the community here be consistent with the community specified in system management.
Version	Specify the SNMP version for the health check, including 1 and 2C.
Agent Type	Specify the SNMP agent running on the real server, including the UC Davis agent (UCD) and the Windows 2000 Server agent (WIN2000). • If UCD is selected, system will collect load information of the real server using OIDs of CPU, memory and disk provided by UCD. • If WIN2000 is selected, system will use WMI as the agent, and collect load information of the real server using OIDs of CPU, memory and disk provided by WMI.
CPU Threshold	Specify the maximum acceptable CPU usage on the real server for the health check. If this value is exceeded, Alert logs will be generated.
CPU Coefficient	Specify the coefficient that system uses to calculate the weight of the CPU threshold for the health check, providing evidence for selecting a real server.
Memory Threshold	Specify the maximum acceptable memory usage on the real server for the health check. If this value is exceeded, Alert logs will be generated.
Memory Coef-	Specify the coefficient that system uses to calculate the weight of the

Option	Description
ficient	memory threshold for the health check.
Disk Threshold	Specify the maximum acceptable disk usage on the real sever for the health check. If this value is exceeded, Alert logs will be generated.
Disk Coefficient	Specify the coefficient that system uses to calculate the weight of the disk threshold for the health check.
SNMP-DCA-BASE Health Check: Used to check the current user usage of a real server using user-defined OIDs.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the

Option	Description
	health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the port for the health check. If not specified, the default SNMP port (161) will be used.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
Community	Specify the community for the SNMP host of the real server. Community is a password sent in clear text between the manager and the agent. You should keep the community here be consistent with the community specified in system management.
Version	Specify the SNMP version for the health check, including 1 and 2C.
CPU OID	Specify the CPU OID value. The OID value should consist of integers.

Option	Description
CPU Max Value	Specify the maximum value of CPU for calculating the CPU coefficient.
CPU Threshold	Specify the maximum acceptable CPU usage on the real server for the health check. If this value is exceeded, Alert logs will be generated.
CPU Coefficient	Specify the coefficient that system uses to calculate the weight of the CPU threshold for the health check, providing evidence for selecting a real server.
Memory OID	Specify the memory OID value.
Memory Max Value	Specify the maximum value of memory for calculating the memory coefficient.
Memory Threshold	Specify the maximum acceptable memory usage on the real server for the health check. If this value is exceeded, Alert logs will be generated.
Memory Coefficient	Specify the coefficient that system uses to calculate the weight of the memory threshold for the health check.
Disk OID	Specify the disk OID value.
Disk Max Value	Specify the maximum value of disk for calculating the disk coefficient.
Disk Threshold	Specify the maximum acceptable disk usage on the real server for the health check. If this value is exceeded, Alert logs will be generated.
Disk Coefficient	Specify the coefficient that system uses to calculate the weight of the disk threshold for the health check.
THIRD-PARTY Health Check: System supports to upload third-party scripts for health check. Currently, Python scripts (.py files in UNIX format) are supported. In addition, the device comes with an Exchange-based third-party health check script, which can be used in the health checks on the Exchange server. When checking, the device performs the health check according to the script content. Within the timeout period, if the script has been successfully executed, the health check is considered successful.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If not specified, system will directly reference the IP address of the real server.
Interval	Specify the interval between each health check.

Option	Description
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the timeout period for script execution for the health check. If the

Option	Description
	script has been executed successfully within the timeout period, the health check is considered successful.
Retry Times	Specify the number of attempts to retry the health check.
Port	Specify the port for the health check. If not specified, system will reference the port of the real server.
Parameter	Specify the script startup parameter of the script for the health check.
File Name	Select a health check script from the drop-down list. The script needs to be uploaded in advance. For specific information, see Uploading a Third-Party Script.
RADIUS-AUTHENTICATION Health Check: Used to check the availability of RADIUS-AUTHENTICATION services on a real server. When checking, the device sends the configured RADIUS packet to a real server. Within the timeout period, if an Access-Accept packet is received from the real server, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If not specified, system will directly reference the IP address of the real server.
NAS IP	Specify the NAS address. You can configure an IPv4 or IPv6 address.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is con-

Option	Description
	sidered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the port for the health check. If not specified, system will reference the port of the real server.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address

Option	Description
	of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
User name	Specify the username for logging into the real sever.
Password	Specify the password corresponding to the username.
Shared Secret	Specify the shared secret between the device and the real server.
RADIUS-ACCOUNTING Health Check: Used to check the availability of RADIUS-ACCOUNTING services on a real server. When checking, the device sends the configured RADIUS packet to a real server. Within the timeout period, if an Accounting-Response packet is received from the real server, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If not specified, system will directly reference the IP address of the real server.
NAS IP	Specify the NAS address. You can configure an IPv4 or IPv6 address.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned

Option	Description
	the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the port for the health check. If not specified, system will reference the port of the real server.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
User name	Specify the username for logging into the real sever.

Option	Description
Shared Secret	Specify the shared secret between the device and the real server.
WEBSOCKET Health Check: Used to check the availability of WebSocket services on a real server. When checking, the device sends a packet to a real server. Within the timeout period, if a response is received from the real server, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If not specified, system will directly reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you

Option	Description
	have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the port for the health check. If not specified, system will reference the port of the real server.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
Key	Specify the value of the Sec-WebSocket-Key to prevent cross-protocol attacks.
Advanced Configuration	
Hostname	Specify the Host field. The specified Host field will be included in the request which is to be sent for the health check. The IP address of the real server will be referenced by default.
Origin	Specify the Origin header field.

Option	Description
Extensions	Specify the value of the Extensions field. The server will determine whether to establish a connection according to the Extensions field supported by the client.
Sub Protocol	By specifying the Sec-WebSocket-Protocol field in the handshake, the client can request the server to use specified sub protocols. If the field is specified, a sub protocol will be selected and returned by the server in the field included in the response to establish a connection.
WEBSOCKET-SSL Health Check: Used to check the availability of WebSocket services encrypted with SSL certificates on a real server. When checking, the device sends a packet to a real server. Within the timeout period, if a response is received from the real server, the health check is considered successful, otherwise the health check will be retried. If the number of consecutive retries exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If not specified, system will directly reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health

Option	Description
	check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the port for the health check. If not specified, system will reference the port of the real server.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
Key	Specify the value of the Sec-WebSocket-Key to prevent cross-protocol attacks.

Option	Description
Cert-chain	Specify the certificate that provides encryption services.
Advanced Configuration	
Hostname	Specify the Host field. The specified Host field will be included in the request which is to be sent for the health check. The IP address of the real server will be referenced by default.
Origin	Specify the Origin header field.
Extensions	Specify the value of the Extensions field. The server will determine whether to establish a connection according to the Extensions field supported by the client.
Sub Protocol	By specifying the Sec-WebSocket-Protocol field in the handshake, the client can request the server to use specified sub protocols. If the field is specified, a sub protocol will be selected and returned by the server in the field included in the response to establish a connection.
SIP-UDP Health Check: Used to check the availability of SIP services over UDP on a real server. When checking, the device sends the specified content to a real server over UDP. Within the timeout period, if a response returned by the real server contains the expected content you have specified, the health check is considered successful. If the number of consecutive failures exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine

Option	Description
	that the health check fails and retry it. If the number of consecutive retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, if there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the UDP port for the health check. If not specified, the port configured for the real server will be used by default.

Option	Description
Source Port	Specify the UDP source port for the health check. If not specified, an available port of the device will be used by default.
DSR	Only if the **Enable** check box is selected can the device perform the health check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
Status Code	Specify the SIP status code you expect to receive. If a response returned by the server contains the status code, the health check is considered successful. You can specify multiple status codes, and should separate them by semicolon ";", e.g., "200;302;503". Besides, the wildcard "x" can be included in the status code, such as "30x; 5xx,", but it cannot be placed between two numbers, e.g., "2x3".
SIP-TCP Health Check: Used to check the availability of SIP services over TCP on a real server. When checking, the device sends the specified content to a real server over TCP. Within the timeout period, if a response returned by the real server contains the expected content you have specified, the health check is considered successful. If the number of consecutive failures exceeds the specified retry times, the health check is considered failed.	
Name	Specify the name of the health check.
IP Address	Specify the IP Address. If **Auto IP** is selected, system will reference the IP address of the real server.
Interval	Specify the interval between each health check.
Failure Judgment	Specify the criterion for judging whether the health check fails. If the health check fails, the real server will be excluded from the available servers. • By Retry Times: With the option selected, system will judge whether the health check fails according to the Timeout, Retry Interval and Retry Times you have specified. Within the timeout period, if the real server has not returned the expected response, system will determine that the health check fails and retry it. If the number of consecutive

Option	Description
	retries exceeds the value of Retry Times, the health check is considered failed. For example, with the timeout specified as 6 seconds, the number of retries as 3, and the retry interval as 7 seconds, after system sends the specified content to a real server, if the real server has not returned the expected response within 6 seconds, system will retry the health check in the 7th second. After three consecutive retries, if there is still no expected response from the real server, the health check is considered failed. • By Timeout: With the option selected, system will judge whether the health check fails according to the Interval Time and Timeout you have specified. Then, the number of retries is calculated using the formula: Retry Times = Timeout/Interval time (Rounding off). Within the timeout period, if the number of consecutive retries reaches the value of Retry Times, and there is no expected response from the real server, the health check is considered failed. For example, if the interval time is specified as 9 seconds and the timeout period is 20 seconds, the number of retries will be 2. Within 20 seconds, system sends the specified content to a real server every 9 seconds. If the real server has not returned the expected response after two retries (within 18 seconds), the health check is considered failed.
Timeout	Specify the amount of time that the device waits for a response from the real server before assuming the health check fails.
Retry Times	Specify the number of attempts to retry the health check.
Retry Interval	Specify the interval between each retry.
Port	Specify the TCP port for the health check. If not specified, the port configured for the real server will be used by default.
DSR	Only if the **Enable** check box is selected can the device perform the health

Option	Description
	check in the DSR mode. You need to specify the IP Address as the address of the Loopback interface of the real server.
Source Interface	Specify the source interface for sending health check requests.
Status Code	Specify the SIP status code you expect to receive. If a response returned by the server contains the status code, the health check is considered successful. You can specify multiple status codes, and should separate them by semi-colon ";", e.g., "200;302;503". Besides, the wildcard "x" can be included in the status code, such as "30x; 5xx,", but it cannot be placed between two numbers, e.g., "2x3".

3. Click **Save**.

Uploading a Third-Party Script

System supports to upload third-party scripts for health checks. Currently, Python scripts (.py files in UNIX format) are supported.

To upload a third-party script, take the following steps:

1. Select **Load Balance** > **Health Check** > **Health Check**.
2. Click **Manage and Upload File**, and the File Management Configuration dialog box will appear.
3. Click **Browse**, and select a third-party .py script.
4. Click **Upload**, and then the uploaded file will appear in the list.
5. To delete an uploaded file, select the file from the list and click **Delete**.

Cloning a Health Check

System supports the rapid cloning of a health check. You only need to make minor changes to the to-be-cloned health check to generate a new health check.

To clone a health check, take the following steps:

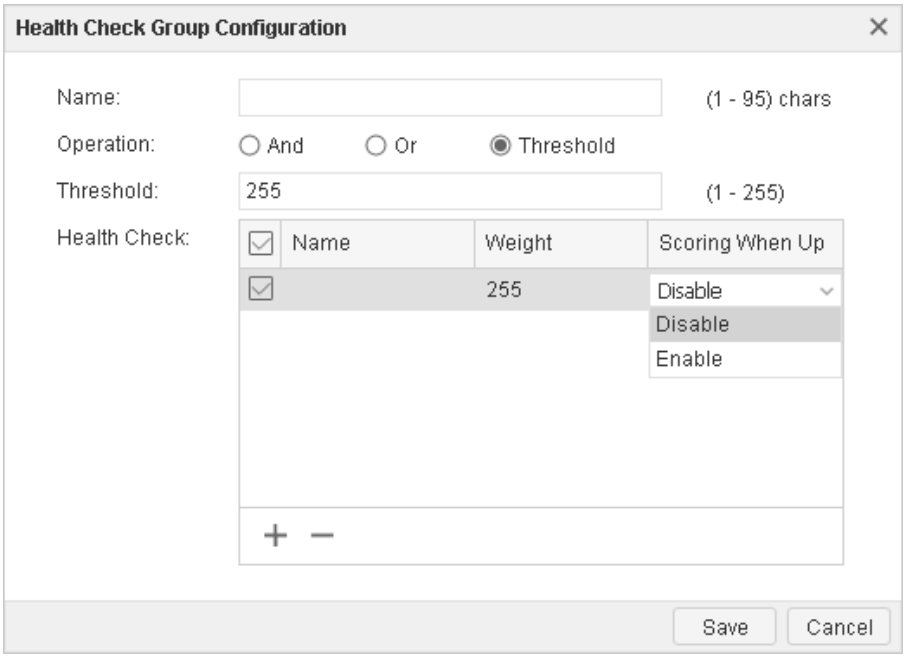
1. Select **Load Balance** > **Health Check** > **Health Check**.
2. Select a health check from the list.
3. Click the **Clone** button above the list, and the **Name** configuration box will appear below the button. Then enter the name of the new health check.
4. The new health check will be generated in the list.

Health Check Group

You can create a health check group by combine multiple health checks into one to perform multiple health checks on a real server at once. When performing the health check based on a health check group, only if all health checks in the group are successful, the check will be considered successful. You can combine up to 16 health checks into a health check group.

To create a health check group, take the following steps:

1. Select **Load Balance** > **Health Check** > **Health Check Group**.
2. Click **New**, and the Health Check Group Configuration dialog box will appear.



3. In the pop-up health check group configuration dialog box, configure the following options:

Option	Description
Name	Specify the name of the health check group. The value range is 1 to 95 characters.
Operation	Specify an operator, i.e., the approach for determining the status of the health check group, including **And**, **Or** and **Threshold**. • And: Indicates that only when the status of all members is "Up", the status of the health check group will be "Up". • Or: Indicates that when the status of at least one member is "Up", the status of the health check group will be "Up". • Threshold: Type a threshold value into the **Threshold** text box. The value range is 1 to 255. System will calculate the sum of weights of members in a health check group according to their status. If the sum is greater than the threshold, the status of the health check group will be "Down".

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Health Check</td><td>Click "+" to add a member to the health check group.
Weight: Type a weight for the member into the text box.
Scoring When Up: Select Enable or Disable from the drop-down list. With the function enabled, the weight of a member whose health check status is "Up" will be counted in the total group weight. By default, the function is disabled, and the weight of a member whose health check status is "Down" will be counted in the total group weight.
To delete a member, select it and click "-". For example, there are four members (HC1, HC2, HC3, and HC4) in a health check group. The configuration and health check status are as follows.<table><tr><th>Name</th><th>Weight</th><th>Scoring When Up</th><th>Health Check Status</th><th>Counted in Group Weight or Not</th></tr><tr><td>HC1</td><td>10</td><td>Enable</td><td>Up</td><td>Yes</td></tr><tr><td>HC2</td><td>20</td><td>Enable</td><td>Down</td><td>No</td></tr><tr><td>HC3</td><td>30</td><td>Disable</td><td>Up</td><td>No</td></tr><tr><td>HC4</td><td>40</td><td>Disable</td><td>Down</td><td>Yes</td></tr></table>As shown in the above table, the weights of HC1 and HC4 will be counted in the total group weight because the health check status of HC1 is "Up" and the Scoring When Up function is enabled, and the health check status of HC4 is "Down" and the Scoring When Up function is disabled. Therefore, the total weight of the health check group is 10 + 40 = 50.</td></tr>
</table>

4. Click **Save**.

Viewing the Health Check Status

In the health check status page, you can view the real servers and virtual servers having been health-checked, their corresponding server pools, health check status, IP: Port, health check objects, etc.

Click **Load Balance** > **Health Check** > **Health Check Status** to enter the Health Check Status page.

Real Server	Server Pool	Update interval	Health Check	IP: Port	Dynamic Weight	Status
2.8080	8080	07/22 08:10	ping	192.168.10.2	0	⊗
3.8080	8080	07/22 08:10	ping	192.168.10.3	0	⊗
1.8080	8080	07/22 08:10	ping	192.168.10.1	0	⊗

Chapter 7 Device Cluster

To meet your high requirements on communication accessibility and network reliability when a communication line or device encounters a failure, the system provides the device cluster function with higher redundant capability. To implement the device cluster function, you need to configure two or more ADC devices that use the same hardware platform, firmware version, software version, and license information. When an ADC device in the cluster fails or cannot process a request from the client, the request will be transferred to an available device for processing. Generally, you cannot enable both the device cluster and high reliability functions. If you enable both, only the high reliability function takes effect.

Basic Concepts

Device Discovery and Authentication

During the device discovery and authentication processes, the system matches the certificate chain of other available ADC devices with that of the local device. Only the devices that pass the authentication can be used with the local device to implement the device cluster function. After a device passes the authentication, the system adds the device to the device cluster list, indicating that mutual trust is formed between the device and the local one.

Device Group

A device group consists of devices with mutual trust that can support one or more services, such as server load balancing (SLB). A device in the device group is identified by its ID. After you create a device group and all of the devices in the group are brought online, the devices enter the cluster running status to implement the device cluster function. Once the cluster relationship is established among the devices, the system starts to synchronize their configurations. This way, when an ADC device in the device group fails and cannot process a request from the client, the request can be transferred to another device in the group that is selected by the system. Therefore, a device group is equivalent to a device for the external network.

Traffic Group

A traffic group is a collection of certain services in the cluster. It is the basic unit for the device to implement high-availability switch. The device binds different services to the traffic group. When the effective device in the group cannot process a request from the client or encounter a failure, the request will be transferred to another device for processing. For example, after you specify the IP address of a virtual server, you can bind it to a traffic group. When the client accesses the virtual

server, the system distributes the request to an available device in the cluster based on the specified switching sequence or algorithm. This available device is the effective device selected after the traffic group is created.

Each interface IP address can be associated with a specific traffic group and traffic is transmitted through the interface. The switchover of the effective device may cause message loss. To reduce the negative impact of message loss on business, you need to configure a virtual MAC address for the traffic group. The traffic is forwarded through the interface that is configured with the virtual MAC address. When the effective device of the traffic group changes, the virtual MAC address is switched to the interface of the corresponding device.

The same traffic group can be bound with multiple IP addresses of different service types. For example, you can bind multiple virtual server IP addresses and the DNS server addresses to the same traffic group. The DNS server addresses are used by multiple GSLB instances to provide public-facing services. However, the service that corresponds to the same IP address can only be bound to a single traffic group.

Cluster Synchronization

Assume that a device in the cluster fails and cannot process a request from the client. To make sure that another device can take over the faulty device, you need to synchronize the information of the faulty device to the new one. The synchronized information between the devices includes the configurations and certain runtime dynamic objects (RDOs). The RDOs to be synchronized between the devices include session information and session persistence tables (IPv6 session persistence tables can be synchronized).

You can synchronize information between the devices by using the following two methods: batch synchronization and real-time synchronization. After a device group is created, the system selects a device from the group as the data center. The data center synchronizes the configurations to other devices or newly added devices in batches. When the configurations are changed, the system synchronizes the changed configurations to other devices in real time. Except for the configurations of the device cluster, the configurations to be imported to local files, and local configurations such as the host name configuration, other configurations are synchronized.

Configuring a Cluster

To configure the device cluster function, take the following steps:

1. Configure the management address of your local device.
2. Configure the local device information.
3. Discover the ADC devices to be added to the cluster and authenticate the devices.

4. Create a device group that contains the local device and devices that pass the authentication.
5. Create a traffic group.
6. Bind the related services to an existing traffic group.

Note: When you configure the device cluster function, the IP address of the device, primary mirror, primary failover, and secondary failover cannot be the same as that of the SLB virtual server.

Configuring the Management Address of the Local Device

When the local device enters the cluster running status, its management address is added to the default traffic group. As a result, you can no longer manage the device based on the address and the device cannot process business that is not related to the cluster. To avoid the above problems, you need to set the management address of the local device to Local IP before you configure the device cluster function. In other words, you need to disable the Configuration Sync function or enable the Set as Local IP function for the required interface.

Device Discovery and Authentication

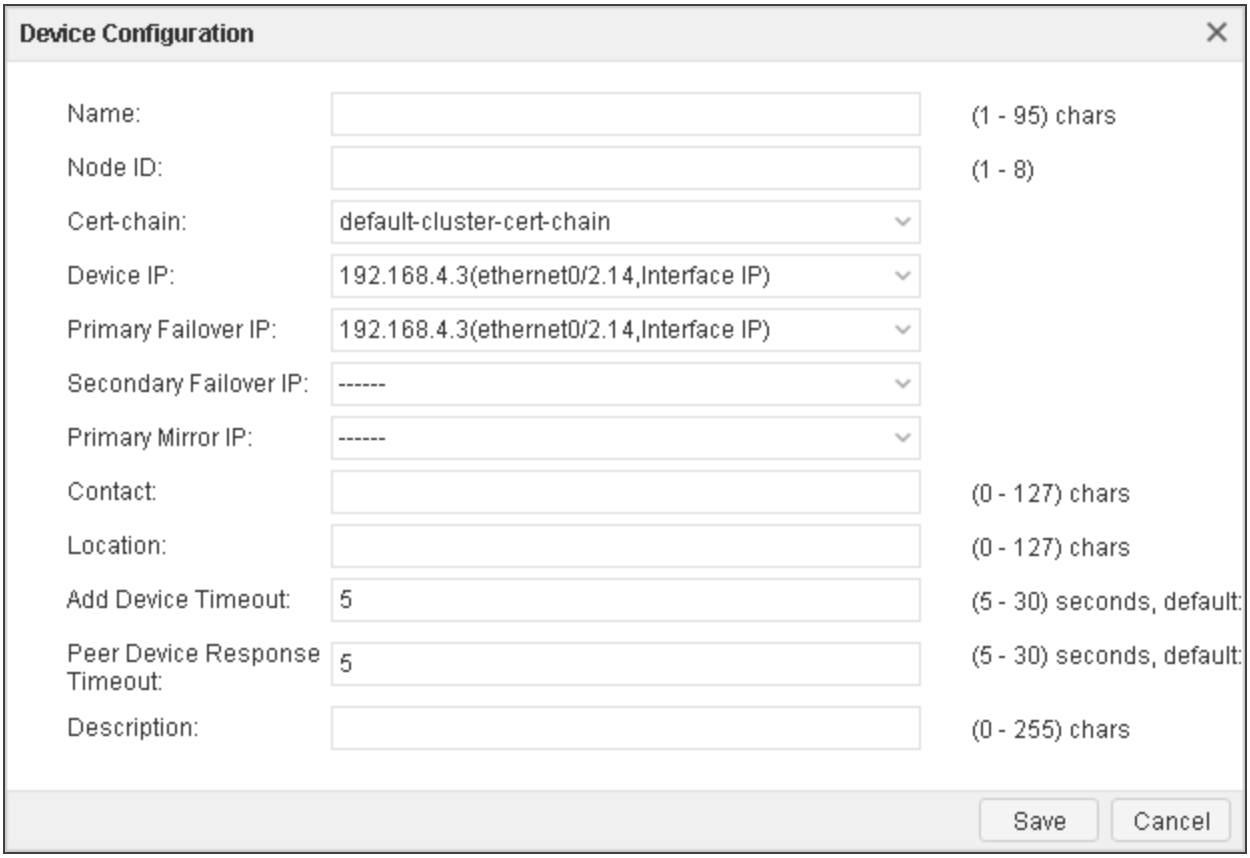
In the device cluster, the device to which you currently log in is the local device. You can view the device in the Name column on the Device List page. To use the device cluster function, configure the local device, and then discover and authenticate other devices.

Configuring the Local Device

To configure the local device, take the following steps:

1. Select System > Device Cluster > Device List.

2. On the page that appears, click New.



In the Device Configuration dialog box, configure the following options:

Option	Description
Name	Specify the device name of 1 to 95 characters in length.
Node ID	Specify the node ID of the cluster to which the device is added. This parameter must be unique.
Cert-chain	Select a certificate chain from the drop-down list, which is used for device authentication.
Device IP	Select the local IP address of the interface from the drop-down list as the device IP address.
Primary Failover IP	Select the local IP address of the interface from the drop-down list as the primary failover IP address of the device. The device sends a heartbeat

Option	Description
	packet to other devices in the device group based on the primary failover IP address to check the working status of the devices. When a fault is detected from a device based on the primary failover IP address, another device will take over this one.
Secondary Fail-over IP	Select the local IP address of the interface from the drop-down list as the secondary failover IP address of the device. If the primary failover IP address is unavailable, use this IP address.
Primary Mirror IP	Select the local IP address of the interface from the drop-down list as the primary mirror IP address of the device. When the effective device of the traffic group generates sessions and session persistence tables after the Mirror RDO function is enabled, the system mirrors these data information to the next effective device by using this IP address.
Contact	Specify the contact information of the device. You can enter an email address or phone number of the administrator.
Location	Specify the location where the device resides.
Add Device Timeout	Specify the timeout period for discovering a device. When you want to discover a device and you fail to receive the response from the peer device within the specified timeout period, the device discovery fails. Valid values: 5 to 30. Default value: 5. Unit: seconds.
Peer Device Response Timeout	Specify the online timeout period of the device. After you discover a device, the system periodically sends a detection request to check whether the peer device is online. If you fail to receive the response from the peer device within the specified timeout period, the peer device is offline. Valid values: 5 to 30. Default value: 5. Unit: seconds.
Description	Enter descriptions for the local device.

3. Click Save.

Discovering a Device

After the local device is configured, the system needs to discover, authenticate, and add other devices. If the certificate chain associated with the device to be discovered is the same as that of the local device, the device passes the authentication and the system adds the device to the cluster device list. To discover and authenticate a device, take the following steps:

1. Select System > Device Cluster > Device List.
2. On the page that appears, click Discover Device. In the Discover Device dialog box, enter the IP address of the device that you want to discover in the text box.

3. Click Discover Device, the system will discover and authenticate the device.
    - If the device passes the authentication, a successful message appears and the device is automatically added to the device list.
    - Otherwise, an error message appears, displaying the failure reason.

You can also perform the following operations on the devices in the device list:

- Click Kick Out Device to remove online devices from the list.
- Click Force Kick Out Device to remove offline devices from the list.
- Click Delete to delete the local device, which indicates that you no longer use the device cluster function. Only after other devices are removed from the list can the local device be deleted.

Configuring a Device Group

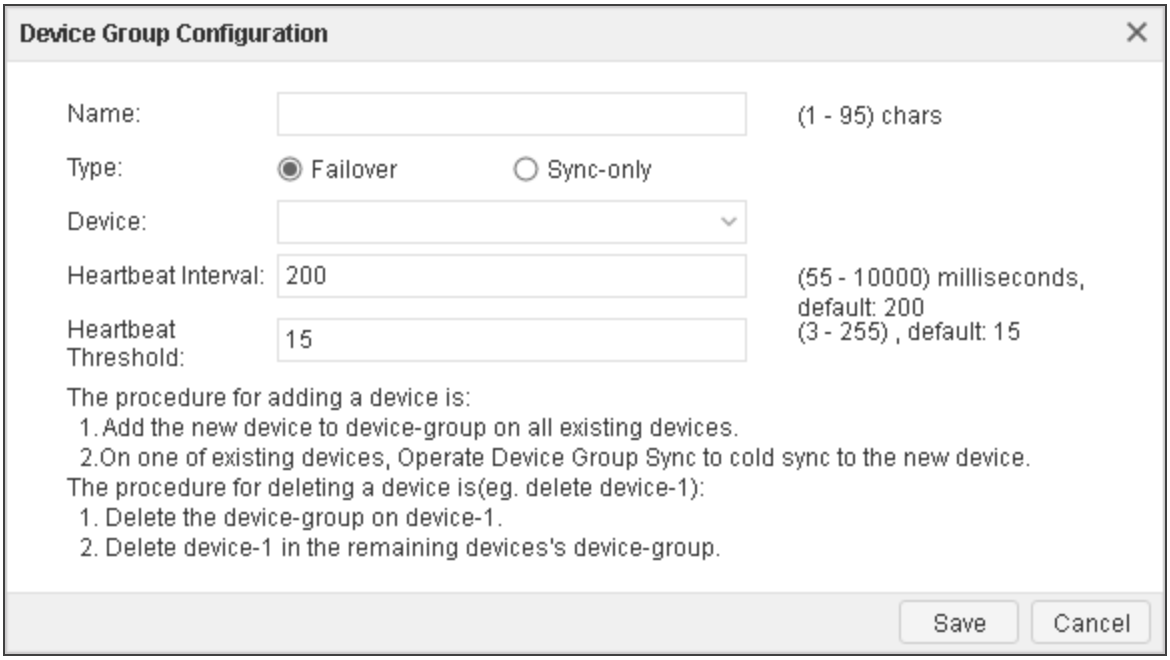
The system allows you to create a device group for ADC devices with mutual trust. This way, a high-availability switchover can be implemented for services in the device group. The maximum number of devices in a device group varies with the model of the devices.

Creating a Device Group

To create a device group, take the following steps:

1. Select System > Device Cluster > Device Group.

2. On the page that appears, click New.



In the Device Group Configuration dialog box, configure the following options:

Option	Description
Name	Specify the device group name of 1 to 95 characters in length.
Type	Specify the type of the device group. Valid values: • Failover: The devices in the device group can be switched over with high availability. That is, if an ADC device in the device group fails, another device in the group will take over this device and continue to process the traffic from the client. • Sync-only: The devices in the device group can only synchronize the related data information.
Sync Scope	This parameter is available when you set the Type parameter to Sync-only.

Option	Description
	It is used to specify the type of the synchronized data information. Valid values: Server Load Balancing, Global Server Load Balancing, and System Configuration.
Device	Specify the device in the device list that you want to add to the device group. Each device can be added to only one device group.
Heartbeat Interval	Specify the interval during which a heartbeat message is sent to other devices in the device group. Valid values: 55 to 10000. Default value: 200. Unit: milliseconds.
Heartbeat Threshold	Specify the threshold of the heartbeat messages that are sent to other devices in the device group. If the number of the heartbeat messages exceeds this threshold and no response from the peer device is returned, the peer device is offline. Valid values: 3 to 255. Default value: 15.

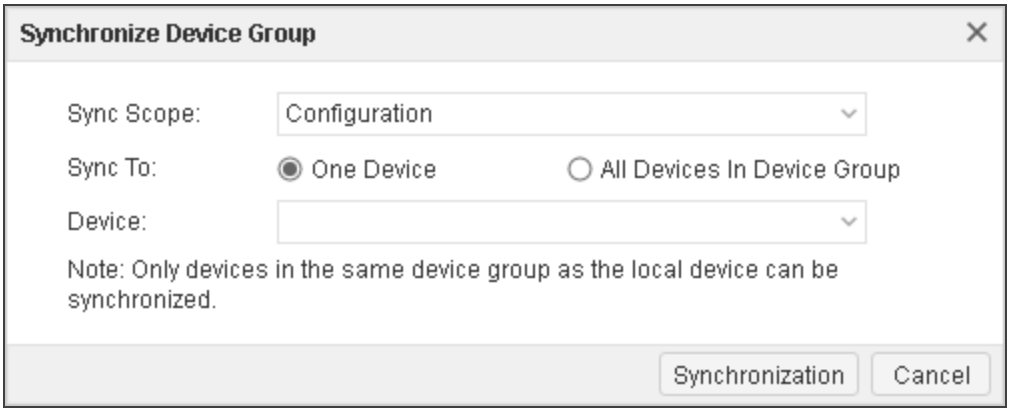
3. Click Save.

Synchronizing the Device Group

To make sure that each device can work properly when a high-availability switchover occurs in the device group of the Failover type, you need to synchronize the device group information and the device configurations. You can log in to all the devices in the device group respectively and repeat the device group configuration steps of the first device, or synchronize the device group configurations of all the devices on a single device. To synchronize the device group configurations of all the devices on a device, take the following steps:

1. Select System > Device Cluster > Device Group.

2. On the page that appears, click Synchronizing Device Group.



In the Device Configuration dialog box, configure the following options:

Option	Description
Sync Scope	Specify the type of data information to be synchronized. Valid values: • Configuration: the configurations of the local device. • Device Group: the device group information in the Device Group list.
Sync To	Specify the device in the cluster to receive the synchronized data information. Valid values: One Device and All Devices in Device Group. If you set this parameter to One Device, you need to select a device from the Device drop-down list.

3. Click Synchronization.

Configuring a Traffic Group

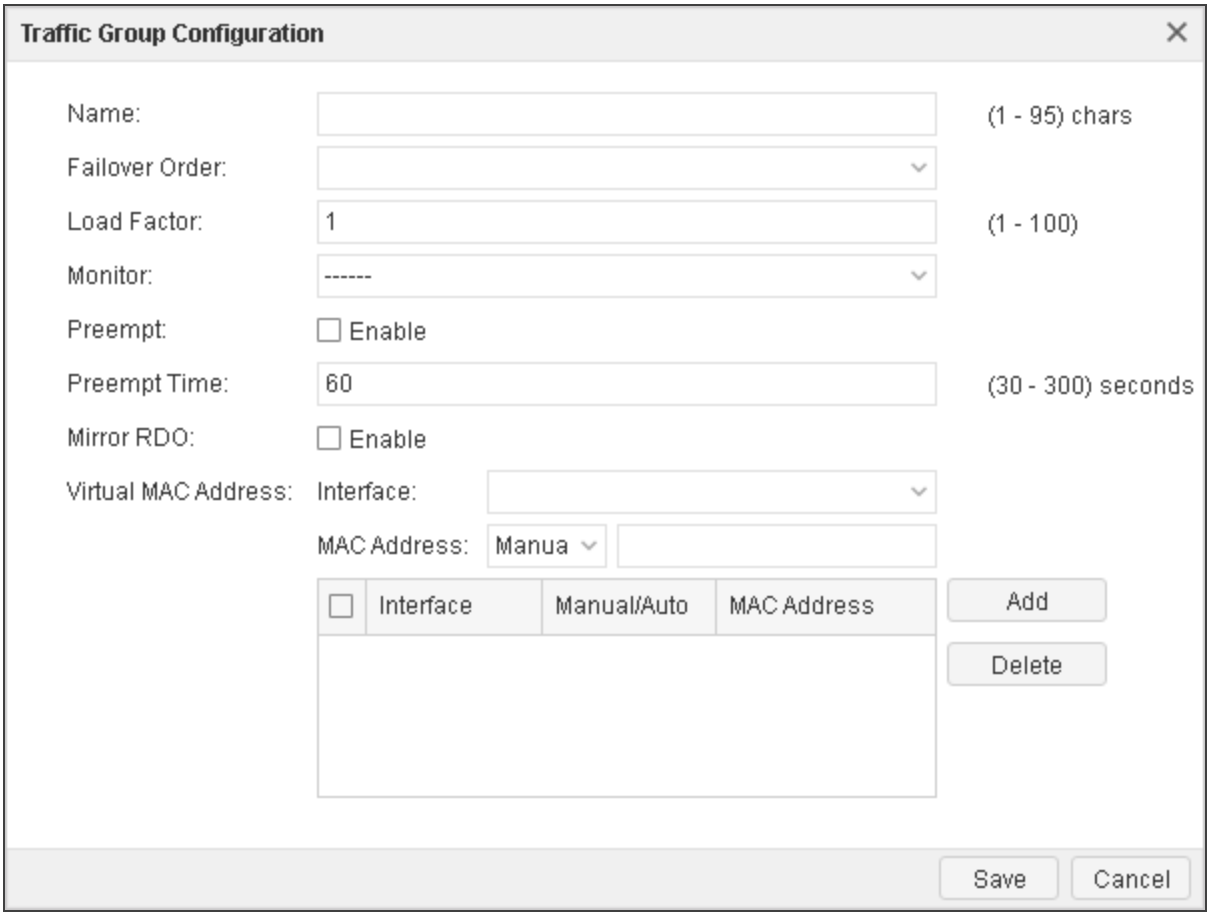
After a traffic group is created, all devices in the device group where the local device resides could be the effective device of the traffic group. When a request from the request that meets the traffic group requirements is sent to the effective device, the device sends the ARP or NA message to divert the request to its system. Then, the system processes the request. The maximum number of traffic groups varies with the model of the devices.

If you do not bind services to an existing traffic group, the services are added to the default traffic group that is predefined by the system. You can modify but not delete the default traffic group.

Creating a Traffic Group

To create a traffic group, take the following steps:

1. Select System > Device Cluster > Traffic Group.
2. On the page that appears, click New.



In the Traffic Group Configuration dialog box, configure the following options:

Option	Description
Name	Specify the traffic group name of 1 to 95 characters in length.
Failover Order	Specify the switchover order when a high-availability switchover occurs in the device group of the Failover type. After receiving a request from the client that meets the traffic group requirements, the system distributes the request to the corresponding device based on the specified failover order.

Option	Description
	Select a device from the drop-down list and you can perform the following operations: • Click  to add the device to or remove the device from the fail-over order list. • Click to adjust the failover order of the device. • Click  to adjust the device to the first or last in the list. **Note:** Assume that you do not specify the failover order of devices for the traffic group. When receiving a request from the client in the traffic group, the system distributes it to the device that has the greatest processing capability in the target device group.
Load Factor	Specify the load factor of the traffic group. When a request from the client that meets the traffic group requirements is sent to a device in the device group, the load weight of the device increases with the load factor. Next time the system will distribute client requests based on the new load status. Valid values: 1 to 100. Default value: 1. For example, the device group DG of the failover type contains the devices AX1, AX2, and AX3. Configure the traffic groups TG1 and TG2. In the TG1, the failover order is AX1>AX3 and the load factor is 10. In the TG2, the failover order is AX2>AX3 and the load factor is 20. TG1 works on AX1 and TG2 works on AX2. Then, create the traffic group TG3 and do not specify the failover order. When receiving a request from the client that meets the requirements of TG3, the system calculates the current load weight of all devices in DG based on the load factors. The load weight of AX1, AX2, and AX3 is 10, 20, and 0 respectively. Therefore, the system will distribute the request to AX3.
Monitor	Specify the name of the configured monitor object. The monitor object is used to identify the status of the traffic group. When the monitor object is invalid, the traffic group is identified as invalid.

Option	Description
Preempt	Select Enable to enable the automatic switchover function. After the function is enabled, the faulty device that is the first one in the failover order will take over its original work when it is recovered.
Preempt Time	Specify the time period after which the automatic switchover occurs. When the faulty device is recovered, it will take over its original work after the specified time period. Valid values: 30 to 300. Default value: 60. Unit: seconds.
Mirror RDO	Select Enable to enable the data object synchronization function. This function can be used to synchronize sessions and session persistence tables. When the effective device of the traffic group generates sessions and session persistence tables after this function is enabled, the system mirrors these data information to the next effective device by using the primary mirror IP address.
Virtual MAC Address	Specify the virtual MAC address for the traffic group interface and click Add. • Interface: Select an interface from the drop-down list. • MAC Address: Specify the virtual MAC address for the selected interface. If you set the type to Manual, you need to enter a virtual MAC Address in the text box. If you set the type to Auto, the system automatically generates a virtual MAC Address for the interface.

3. Click Save.

If you set the type of the virtual MAC Address to Auto, you are allowed to specify the virtual MAC prefix. To specify the virtual MAC prefix, take the following steps:

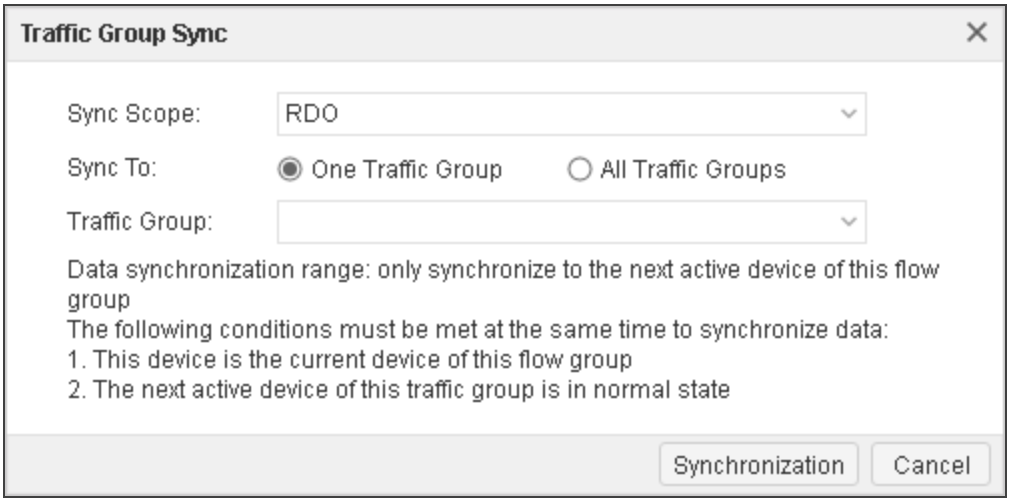
1. Select System > Device Cluster > Traffic Group.
2. On the page that appears, click Virtual MAC Prefix.
3. In the Virtual MAC Prefix dialog box, enter the virtual MAC prefix, which needs to be a six-bit hexadecimal string.
4. Click Save.

Configuring Traffic Group Synchronization

If the local device is the effective one of a traffic group, you can manually synchronize the sessions and session persistence tables of the local device to the next effective device in the traffic group.

To configure traffic group synchronization, take the following steps:

1. Select System > Device Cluster > Traffic Group.
2. On the page that appears, click Traffic Group Sync.



In the Traffic Group Sync dialog box, configure the following options:

Option	Description
Sync Scope	When the local device is the current effective one of one or more traffic groups, the system synchronizes the data objects generated by the local device to the next effective device in the traffic group. The data objects include sessions and session persistence tables.
Sync To	Specify the number of traffic groups to which you want to synchronize the data objects of the local device. Valid values: • One Traffic Group: Select an existing traffic group. The current effective device of the traffic group is the local one. The system synchronizes the data objects of the local device to the next effective device of the traffic group. • All Traffic Group: Specify the current local device as all the traffic groups of the effective one. The system synchronizes the data objects of the local device to the next effective

Option	Description
	device of all these traffic groups respectively.
Traffic Group	This parameter is available if you set the Sync To parameter to One Traffic Group. You need to specify the traffic group to which you want to synchronize the data objects of the local device.

3. Click Synchronization.

Chapter 8 Network

This chapter describes factors and configurations related to network connection, including:

- Security Zone: The security zone divides the network into different sections, such as the trust zone (like intranet) and the untrust zone (like internet). The device can manage and control the traffic flowing into and from security zones once the configured policy rules have been applied.
- Interface: The interface allows inbound and outbound traffic to flow into and from security zones. An interface must be bound to a security zone so that traffic can flow into and from the security zone. Furthermore, for the Layer 3 security zone, an IP address should be configured for the interface, and the corresponding policy rules should also be configured to allow traffic transmission between different security zones.
- MGT Interface: Configure a management interface (MGT Interface) to meet the requirement of separating the management traffic from the data traffic.
- DDNS: Domain Name System.
- DHCP: Dynamic Host Configuration Protocol.
- DDNS: Dynamic Domain Name Server.
- PPPoE: Point-to-Point Protocol over Ethernet.
    - Virtual Router: Virtual Router (VRouter) acts as a router. Different virtual routers have their own independent routing tables.
- Virtual Switch: Running on Layer 2, Virtual Switch (VSwitch) acts as a switch. Once a Layer 2 security zone is bound to a VSwitch, all the interfaces bound to that zone will also be bound to the VSwitch. Traffic can be forwarded between Layer 2 and Layer 3 through the VSwitch interface.
- SSL Inspection Profile: Decrypts the HTTP application traffic encrypted with the SSL protocol, and then forwards the decrypted traffic to other devices in monitoring modes, such as DLP and IDS.
- Global Network Parameters: These parameters mainly include the IP packet's processing options, like IP fragmentation, TCP MSS value, etc.

Security Zone

Security zone is a logical entity. One or more interfaces can be bound to one zone. A zone applied with a policy is known as a security zone, while a zone created for a specific function is known as a functional zone. Zones have the following features:

- An interface should be bound to a zone. A Layer 2 zone will be bound to a VSwitch, while a Layer 3 zone will be bound to a VRouter. Therefore, the VSwitch to which a Layer 2 zone is bound decides which VSwitch the interfaces belong to in that Layer 2 zone, and the VRouter to which a Layer 3 zone is bound decides which VRouter the interfaces belong to in that Layer 3 zone.
- Interfaces in Layer 2 and Layer 3 are working in Layer 2 mode and Layer 3 mode respectively.

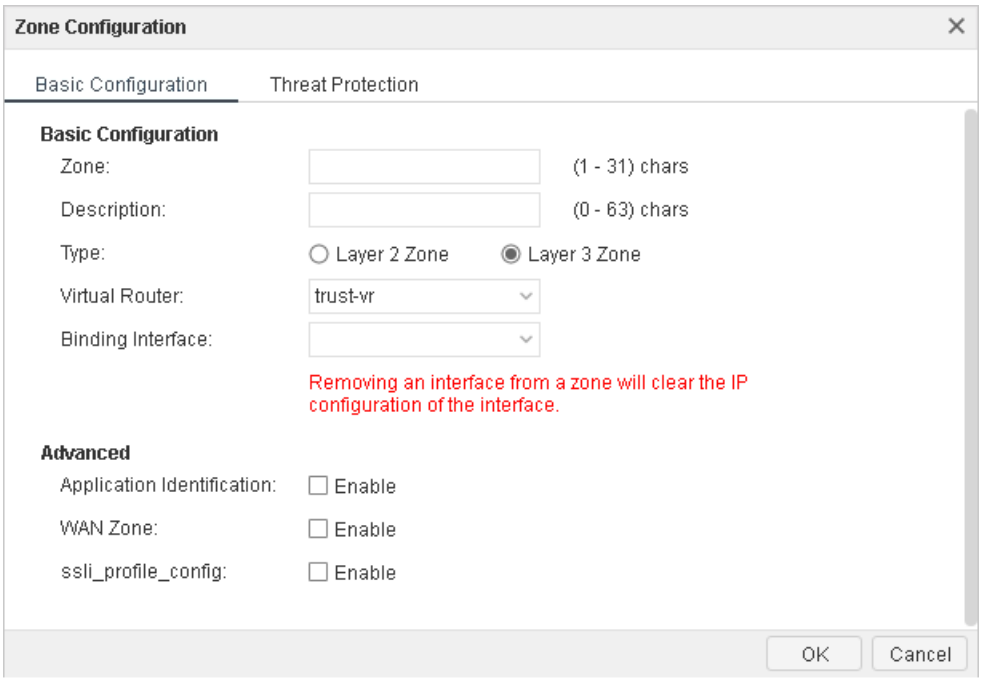
There are 7 pre-defined security zones in ADC, which are trust, untrust, L2-trust, L2-untrust, mgt, ha (HA functional zone) and proxy (Layer 7 SLB functional zone). You can also customize security zones. The proxy security zone is mainly used in the Layer 7 environment. After the ADC device is started, system will create a proxy security zone by default and bind it to the trust-vr. The proxy security zone can only be configured as the destination security zone of a rule, and cannot be edited or deleted.

Configuring a Security Zone

To create a security zone, take the following steps:

1. Select **Network** > **Zone**.

2. Click **New**, and the **Zone Configuration** text box will appear.



3. Type the name of the zone into the **Zone** box.

4. Type the descriptions of the zone into the **Description** text box.

5. Specify a type for the security zone. For a Layer 2 zone, select a VSwitch for the zone from the **VSwitch** drop-down list below; for a Layer-3 zone, select a VRouter from the **Virtual Router** drop-down list.

6. Bind interfaces to the zone. Select an interface from the **Binding Interface** drop-down list.

7. If needed, select the **Enable** check box to enable APP identification for the zone.

8. If needed, select the **Enable** check box to set the zone to a WAN zone, then the interface bound to the zone will be a WAN interface.

9. If needed, enable the SSL Inspection function. After the function is enabled, system can decrypt the HTTP application traffic encrypted with the SSL protocol, and then forward the decrypted traffic to other devices in monitoring modes, such as DLP and IDS. You can select a configured SSL Inspection profile from the **Profile** drop-down list.

10. If needed, select Threat Protection tab and configure the parameters for Threat Protection function. For detailed instructions, see Threat Protection。

11. Click **OK**.

Note:

- Pre-defined zones cannot be deleted.
- When changing the VSwitch to which a zone belongs, make sure there is no binding interface in the zone.

Management Interface

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

To facilitate the management of the device and meet the requirement of separating the management traffic from the data traffic, the system has an independent management interface (MGT Interface). By default, the management interface belongs to the trust zone and the trust-vr virtual router. To separate the traffic of the management interface from the traffic of other interfaces completely, you can add the management interface to the mgt zone.

Configuring a Management Interface

To configure a MGT interface, take the following steps:

1. Select **Network** > **Management Interface**.
2. In the MGT Interface page, the status light behind the interface name shows the status of the management interface.
3. Specify the zone for the management interface in the **Zone** drop-down list. You can only select a Layer 3 zone.
4. Specify the method of obtaining an IP address behind the Type option, including Static IP and Auto-obtain. "Static IP" means specifying a static IP address and the netmask. Click **Advanced** to type the secondary IP address into the text box. You can specify up to 6 secondary IP addresses. "Auto-obtain" means obtaining the IP address through DHCP.
5. Specify the management methods in the Management section by selecting the check boxes of the desired management methods.

6. Specify the mode and rate of the management interface in the Mode section. If you select the Auto duplex transmission mode, you can only select the Auto rate.
7. Select the **Shut Down** check box in the Shut Down section to shut down the management interface.

8. Click **OK**.

Interface

Interfaces allow inbound and outbound traffic to flow into and from security zones. An interface must be bound to a security zone so that traffic can flow into and from the security zone. Furthermore, for the Layer 3 security zone, an IP address should be configured for the interface, and the corresponding policy rules should also be configured to allow traffic transmission between different security zones. Multiple interfaces can be bound to one security zone, but one interface cannot be bound to multiple security zones.

The deivces support various types of interfaces which are basically divided into physical and logical interfaces based on the nature.

- Physical Interface: Each Ethernet interface on devices represents a physical interface. The name of a physical interface, consisting of media type, slot number and location parameter, is pre-defined, like ethernet2/1 or ethernet0/2.
- Logical Interface: Include sub-interface, loopback interface, VSwitch interface, aggregate interface, redundant interface and PPPoE interface.

Interfaces can also be divided into Layer 2 interface and Layer 3 interface based on their security zones.

- Layer 2 Interface: Any interface in Layer 2 zone.
- Layer 3 Interface: Any interface in Layer 3 zone. Only Layer 3 interfaces can operate in NAT/routing mode.

Different types of interfaces provide different functions, as described in the table below.

Type	Description
Sub-interface	The name of a sub-interface is an extension to the name of its original interface, like ethernet0/2.1. System supports the following types of sub-interfaces: Ethernet sub-interface, aggregate sub-interface and redundant sub-interface. An interface and its sub-interfaces can be bound to one single security zone, or to different zones.
Loopback interface	A logical interface. Only if the device with loopback interface configured is in the working state, the interface will be in the working state as well. Therefore, the loopback interface is featured with stability.
Aggregate interface	A collection of physical interfaces that include 1 to 16 physical interfaces. These interfaces averagely share the traffic load to the IP address of the aggregate interface, in an attempt to increase the available bandwidth for a single IP

Type	Description
	address. If one of the physical interfaces within an aggregate interface fails, other physical interfaces can still process the traffic normally. The only effect is the available bandwidth will decrease.
Redundant interface	The redundant interface allows backup between two physical interfaces. One physical interface, acting as the primary interface, processes the inbound traffic, and another interface, acting as the alternative interface, will take over the processing if the primary interface fails.
PPPoE interface	A logical interface based on Ethernet interface that allows connection to PPPoE servers over PPPoE protocol.

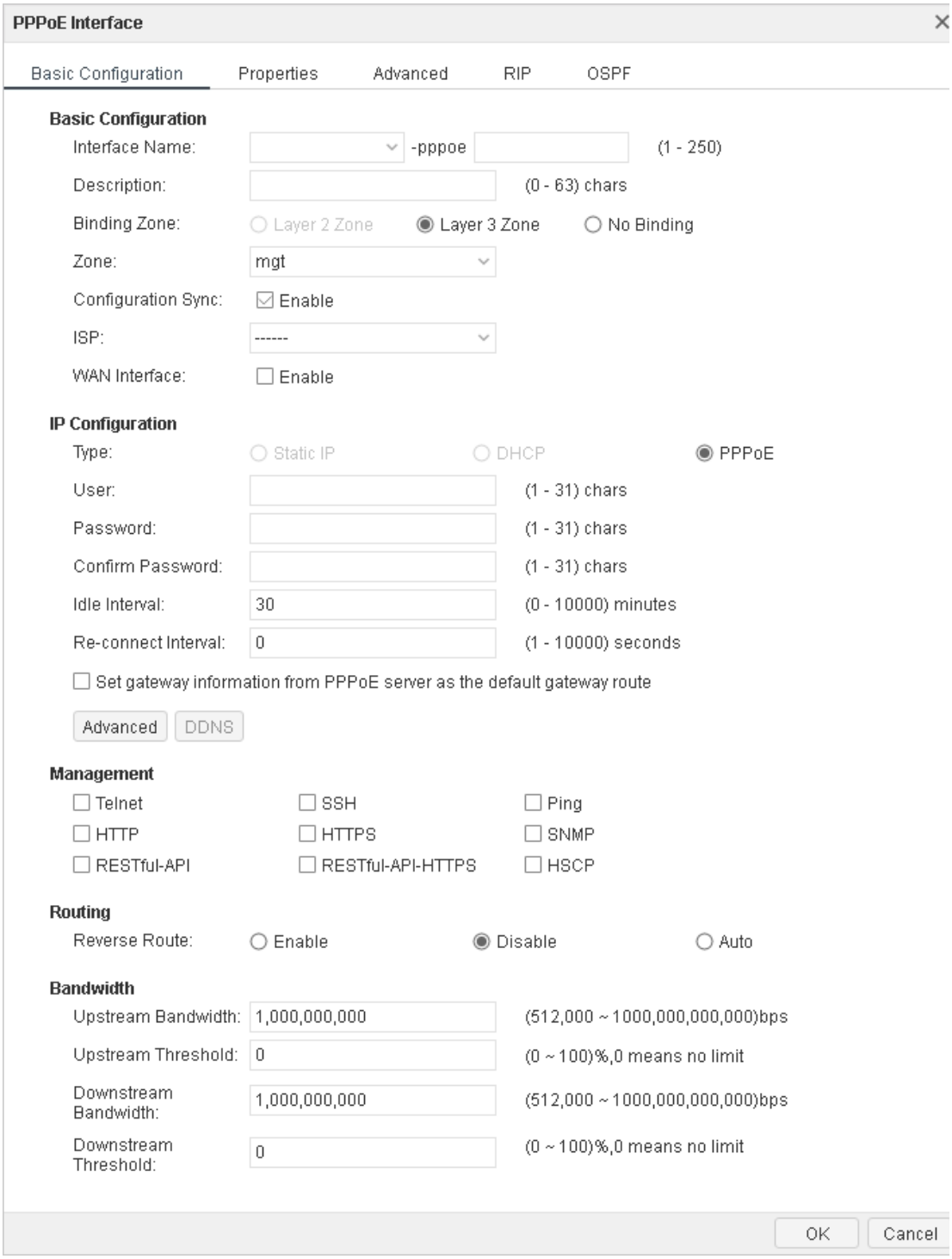
Configuring an Interface

The configuration options for different types of interfaces may vary. For more information, see the following instructions.

Creating a PPPoE Interface

To create a PPPoE interface, take the following steps:

1. Select **Network** > **Interface**.
2. Click **New** > **PPPoE Interface**, and the PPPoE Interface dialog box will appear.



In the Basic tab, configure basic configurations for the interface.

Option	Description
Interface Name	Specify a name for the PPPoE interface.
Description	Enter descriptions for the PPPoE interface as needed. The range is 0 to 63 characters.
Binding Zone	If Layer 3 zone is selected, you should also select a security zone from the **Zone** drop-down list, and the interface will bind to a Layer 3 zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the **Zone** drop-down list.
HA sync	Select this check box to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not selecting this check box disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
ISP	Select an ISP from the ISP drop-down list. After you bind the interface to the specified ISP, the link corresponding to the interface is bound to the ISP.
WAN Interface	Select the **Enable** check box to set the interface to a WAN interface.
User	Specify a username for PPPoE.
Password	Specify PPPoE user's password.
Confirm Password	Enter the password again to confirm.
Idle Interval	If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connections; if the interface requires Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30.
Re-connect Interval	Specify a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000

Option	Description
	seconds. The default value is 0, which means the function is disabled.
Set gateway information from PPPoE server as the default gateway route	With this check box selected, system will set the gateway information provided by PPPoE server as the default gateway route.
Advanced	In the Advanced dialog box, configure advanced options for PPPoE, including: • Access Concentrator: Specify a name for the concentrator. • Authentication: The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). You can select the radio button of the authentication method you need. • Netmask: Specify a netmask for the IP address obtained via PPPoE. • Static IP: You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the box. • Distance: Specify a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specify a route weight. The value range is 1 to 255. The default value is 1. • Service: Specify allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, system will accept any service returned from the server automatically.
DDNS	In the DDNS Configuration dialog box, configure DDNS options for the

Option	Description
	interface. For detailed instructions, see "DDNS" on Page 277.
Management	Select one or more management method check boxes to configure the interface management method.
Reverse Route	Enable or disable reverse route as needed: • Enable: Force to use a reverse route. If the reverse route is not available, packets will be dropped. This option is enabled by default. • Close: Reverse route will not be used. When reaching the interface, the reverse data stream will be returned to its original route without any reverse route check. That is, reverse packets will be sent from the ingress interface that initializes the packets. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
Bandwidth	Specify the actual bandwidth value of the interface as needed. • Upstream Bandwidth : Specify the maximum value of the upstream rate of the interface. The value range is 512,000 to 1,000,000,000,000 bps. The default value is 1,000,000,000 bps. • Upstream Threshold : Specify the upstream bandwidth threshold of the interface. The value ranges from 0% to 100% . The default value is 0%. • Downstream Bandwidth : Specify the maximum value of the downstream rate of the interface. The value range is 512,000 to 1,000,000,000,000 bps. The default value is 1,000,000,000 bps. • Downstream Threshold : Specify the downstream bandwidth threshold of the interface. The value ranges from 0% to 100%. The default value is 0%.

In the Properties tab, configure properties for the interface.

Option	Description
MTU	Specify a MTU for the interface. The value range is 1280 to 1500/1800 bytes. The default value is 1500. The max MTU may vary on different platforms.
ARP Learning	Select the **Enable** check box to enable ARP learning.
ARP Timeout	Specify an ARP timeout for the interface. The value range is 5 to 65535 seconds. The default value is 1200.
Keep-alive IP	Specify an IP address that receives the interface's keep-alive packets.
MAC Clone	Select the **MAC clone** check box to enable the MAC clone function. System clones a MAC address to the Ethernet sub-interface. If you click **Restore Default MAC**, the Ethernet sub-interface will restore the default MAC address.

In the Advanced tab, configure advanced options for the interface.

Option	Description
Shutdown	System supports interface shutdown. You can not only force a specific interface to shut down, but also control the time it shuts down by schedule or according to the link status of tracked objects. Configure the options as below: 1. Select the **Shut down** check box to enable interface shutdown. 2. To control the shutdown by schedule or tracked objects, select the appropriate check box, and then select an appropriate schedule or tracked object from the drop-down list.
Monitor and Backup	Configure the options as below: 1. Select the appropriate check box, and then select an appropriate schedule or tracked object from the drop-down list. 2. Select an action:

Option	Description
	• Shut down the interface: During the time specified in the schedule, or when the tracked object fails, the interface will be shut down and its related route will fail; • Migrate traffic to backup interface: During the time specified in the schedule, or when the tracked object fails, traffic flowing to the interface will be migrated to the backup interface. In such a case you need to select a backup interface from the **Backup Interface** drop-down list and type the time into the **Migrating Time** box. (Migrating time, 0 to 60 minutes, is the period during which traffic is migrated to the backup interface before the primary interface is switched to the backup interface. During the migrating time, traffic is migrated from the primary interface to the backup interface smoothly. By default the migrating time is set to 0, i.e., all the traffic will be migrated to the backup interface immediately.)

In the RIP tab, configure RIP for the interface.

Option	Description
Authentication mode	Specify a packet authentication mode for the system, including plain text (the default) and MD5. The plain text authentication, during which unencrypted string is transmitted together with the RIP packet, cannot assure security, so it cannot be applied to the scenarios that require high security.
Authentication string	Specify a RIP authentication string for the interface.
Transmit version	Specify a RIP information version number transmitted by the interface. By default V1&V2 RIP information will be transmitted.
Receive version	Specify a RIP information version number received by the interface. By default V1&V2 RIP information will be received.
Split horizon	Select the **Enable** check box to enable split horizon. With this function

Option	Description
	enabled, routes learned from an interface will not be sent from the same interface, in order to avoid routing loop and assure correct broadcasting to some extent.

3. In the OSPF tab, configure OSPF for the interface.

Option	Description
Interface Timer	There are four interface timers: the interval for sending Hello packets, the dead interval of adjacent routers, the interval for retransmitting LSA, and the transmit delay for updating packets. • Hello Transmission Interval: Specify the interval for sending Hello packets for an interface. The value range is 1 to 65535 seconds. The default value is 10. • Dead Time: Specify the dead interval of adjacent routes for an interface. The value range is 1 to 65535 seconds. The default value is 40 (4 times of sending the Hello packets). If a router has not received the Hello packet from its peer for a certain period, it will determine the peering router is dead. This period is known as the dead interval between the two adjacent routers. • LSA Transmit Interval: Specify the LSA retransmit interval for an interface. The value range is 3 to 65535 seconds. The default value is 5. • LSU Transmit Delay Time: Specify the transmit delay for updating packet for an interface. The value range is 1 to 65535 seconds. The default value is 1.
Priority	Specify the router priority. The value range is 0 to 255. The default value is 1. The router with priority set to 0 will not be selected as the des-

Option	Description
	ignated router (The designated router will receive the link information of all the other routers in the network, and broadcast the received link information). If two routers within a network can both be selected as the designated router, the router with higher priority will be selected; if the priority level is the same, the one with higher Router ID will be selected.
Network Type	Specify the network type of an interface. The network types of an interface have the following options: broadcast, point-to-point, and point-to-multipoint. By default, the network type of an interface is broadcast.
Link Cost	Select the **Enable** check box to enable the link cost function. The value range is 1 to 65535. By default, the HA synchronization function is enabled, and the link cost will be synchronized to the backup device. Clear the check box to disable the synchronization function, and system will stop synchronizing.

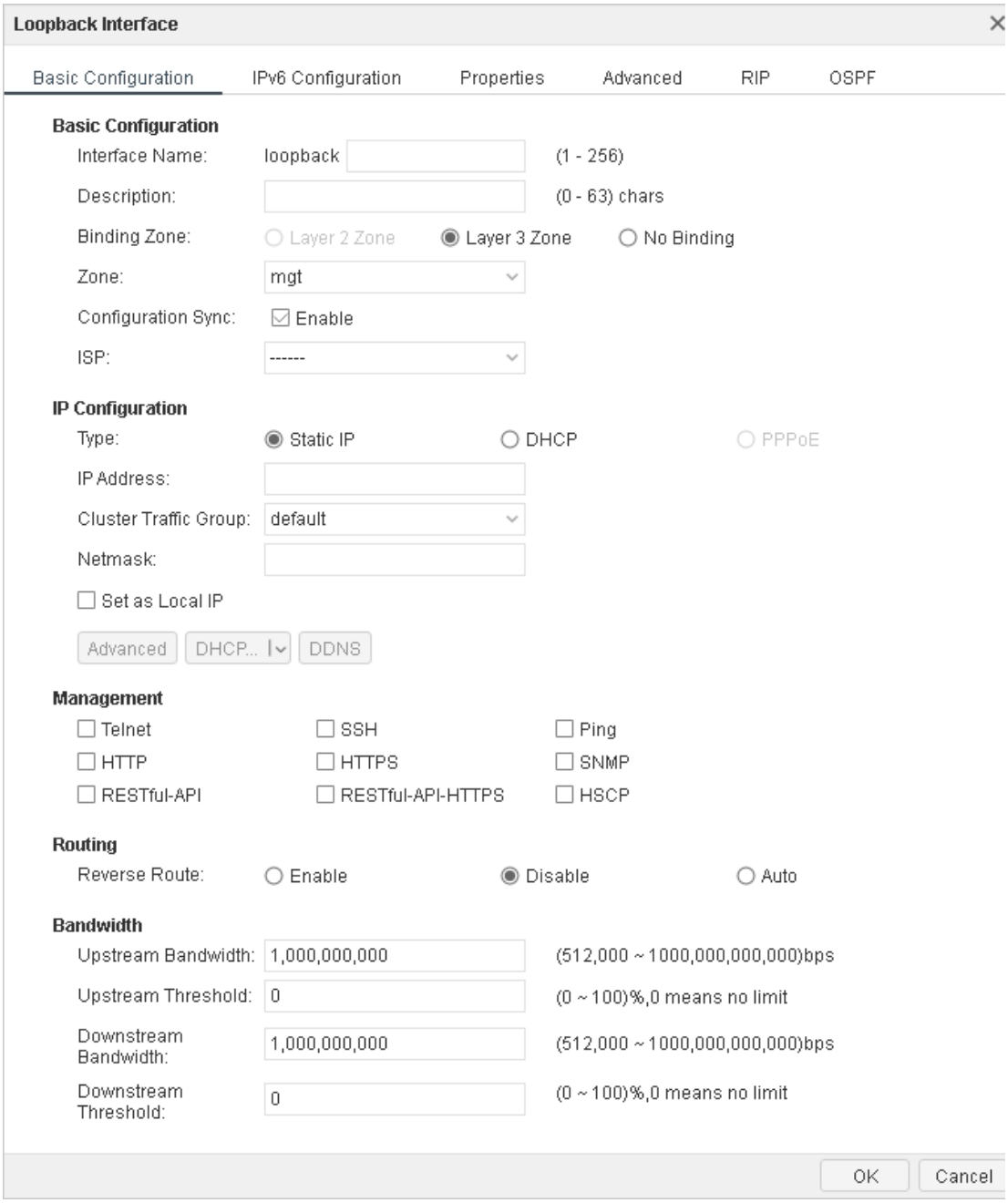
4. Click **OK**.

Creating a Loopback Interface

To create a loopback interface, take the following steps:

1. Select **Network** > **Interface**.

2. Click **New** > **Loopback Interface**, and the Loopback Interface dialog box will appear.



In the Basic tab, configure basic configurations for the interface.

Option	Description
Interface Name	Specify a name for the loopback interface.
Description	Enter descriptions for the loopback interface as needed. The range is 0 to

Option	Description
	63 characters.
Binding Zone	If Layer 3 zone is selected, you should also select a security zone from the **Zone** drop-down list, and the interface will bind to a Layer 3 zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the **Zone** drop-down list.
HA sync	Select this check box to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not selecting this check box disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
ISP	Select an ISP from the ISP drop-down list. After you bind the interface to the specified ISP, the link corresponding to the interface is bound to the ISP
IP Configuration:	Configure Static IP or Auto-obtain according to different IPs
Static IP	IP address: Specify an IP address for the interface.
	Netmask: Specify a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specify a management IP for the interface. Type the IP address into the box. • Secondary IP: Specify secondary IPs for the interface. You can specify up to 6 secondary IP addresses.
	DHCP: In the DHCP Configuration dialog box, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 268.
	DDNS: In the DDNS Configuration dialog box, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 277.

Option	Description
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route.
	Advanced: • Distance: Specify a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specify a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specify a priority for the DNS server. Except for static DNS servers, system can also learn DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server according to its priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority will be. The priority of static DNS servers is 20.
	DDNS: In the DDNS Configuration dialog box, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 277.
Management	Select one or more management method check boxes to configure the interface management method.
Reverse Route	Enable or disable reverse route as needed: • Enable: Force to use a reverse route. If the reverse route is not available, packets will be dropped. This option is enabled by default. • Close: Reverse route will not be used. When reaching the interface, the reverse data stream will be returned to its original route without any reverse route check. That is, reverse packets will be sent from the ingress interface that initializes the packets. • Auto: Reverse route will be prioritized. If available, the reverse route

Option	Description
	will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
Bandwidth	Specify the actual bandwidth value of the interface as needed. • Upstream Bandwidth : Specify the maximum value of the upstream rate of the interface. The value range is 512,000 to 1,000,000,000,000 bps. The default value is 1,000,000,000 bps. • Upstream Threshold : Specify the upstream bandwidth threshold of the interface. The value ranges from 0% to 100% . The default value is 0%. • Downstream Bandwidth : Specify the maximum value of the downstream rate of the interface. The value range is 512,000 to 1,000,000,000,000 bps. The default value is 1,000,000,000 bps. • Downstream Threshold : Specify the downstream bandwidth threshold of the interface. The value ranges from 0% to 100%. The default value is 0%.

3. In the IPv6 Configuration tab, configure IPv6 for the interface.

Option	Description
Enable	Enable IPv6 in the interface.
IPv6 Address	Specify the IPv6 address prefix.
Prefix Length	Specify the prefix length.
Autoconfig	Select the check box to enable Auto-config function. In the address auto-config mode, the interface receives the address prefix in RA packets first, and then combines it with the interface identifier to generate a global address. If the interface is configured with a default router, this option will generate a default route to the default router.
Enable DNS	Select this check box to enable DNS proxy for the interface.

Option	Description
Proxy	
DHCP	You can configure the interface as a DHCPv6 client and obtain IPv6 addresses from the DHCP server. Select DHCP check box to enable DHCP client for the interface. Selecting Rapid-commit option can help fast get IPv6 addresses from the server. You need to enable both of the DHCP client and the server's Rapid-commit function. You can also configure the interface as a DHCPv6 server and DHCPv6 relay proxy. After enabling IPv6, select **DHCPv6 Server** from the **DHCP** drop-down list and configure options as Configuring a DHCPv6 Server. Select **DHCPv6 Relay Proxy** from the **DHCP** drop-down list and configure options as Configuring a DHCPv6 Relay Proxy.
Advanced	
Static	Click **Add** to add several IPv6 address, at most 5 IPv6 addresses. Click **Delete** to delete IPv6 address.
Dynamic	Shows IPv6 address which is dynamic.
Link-local	Specify the link-local address. Link-local address is used for communication between adjacent nodes of a single link. For example, communication between hosts when there are no routers on the link. By default, system will generate a link-local address for the interface automatically if the interface is enabled with IPv6. You can also specify a link-local address for the interface as needed, and the specified link-local address will replace the automatically generated one.
MTU	Specify an IPv6 MTU for an interface. When the device sends RA packets through the interface, you can specify whether to include the MTU value in the RA packets to advertise other routers. The MTU value will be advertised by default.
DAD Attempts	Specify NS packet attempt times. The value range is 0 to 20. Value 0 indicates DAD is not enabled on the interface. DAD (Duplicate Address

Option	Description
	Detection) is designed to verify the uniqueness of IPv6 addresses. This function is implemented by sending NS (Neighbor Solicitation) requests. After receiving a NS packet, if any other host on the link finds that the address of the NS requester is duplicated, it will send a NA (Neighbor Advertisement) packet advertising that the address is already in use, and then the NS requester will mark the address as duplicate, indicating that the address is an invalid IPv6 address.
ND Interval	Specify an interval for sending NS packets. The unit is milliseconds.
ND Reachable Time	Specify the reachable time. After sending an NS packet, if the interface receives acknowledgment from a neighbor within the specified time, it will consider the neighbor as reachable. This time is known as reachable time.
Hop Limit	Specify the hop limit. Hop limit refers to the maximum number of hops for IPv6 or RA packets sent by the interface.
ND RA Suppress	Select the check box to disable RA suppress on LAN interfaces. By default, FDDI interface configured with IPv6 unicast route will send RA packets automatically, and interfaces of other types will not send RA packets.
Manage IP/MASK	Specify the manage IP/MASK.

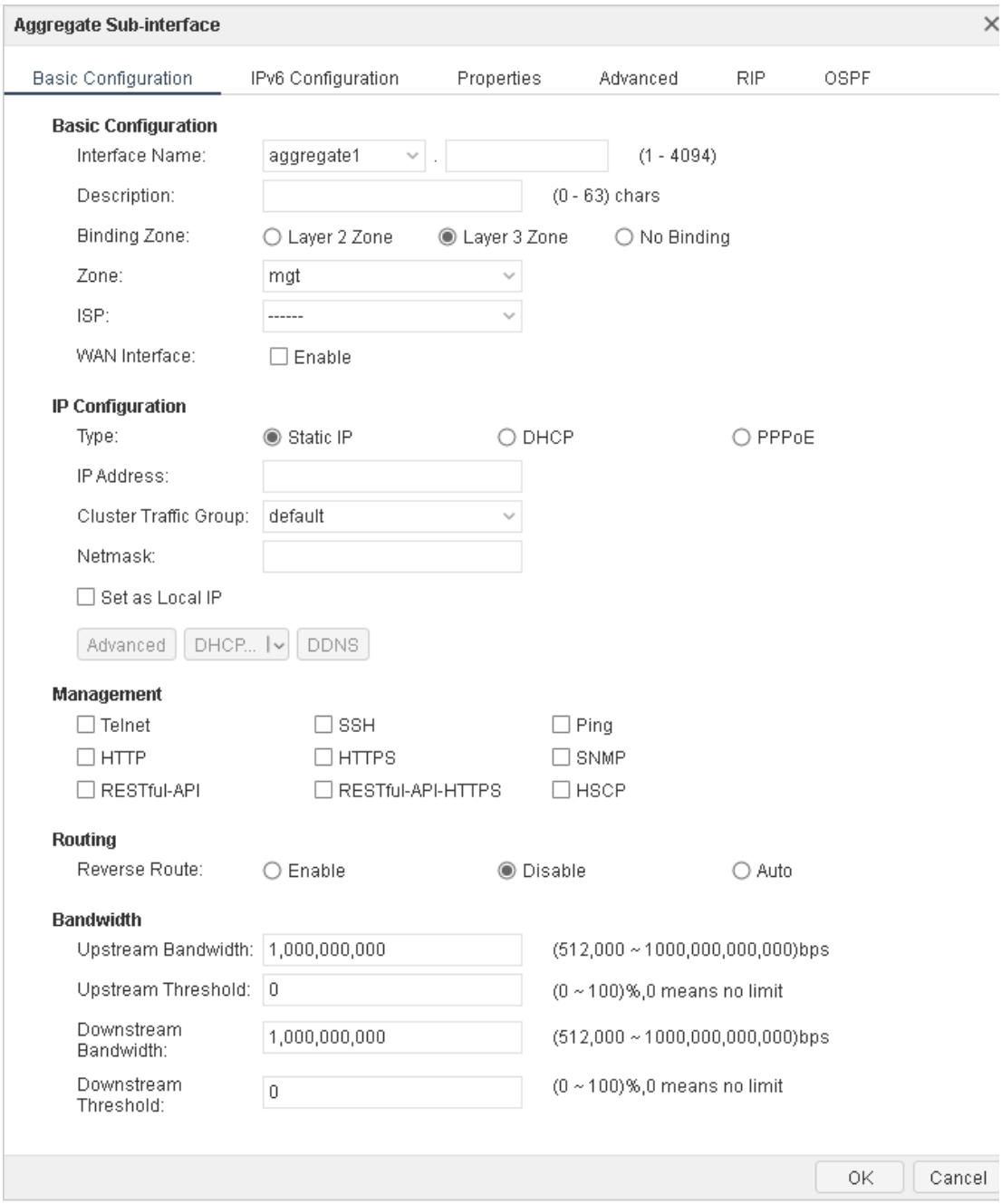
4. "In the Properties tab, configure properties for the interface." on Page 229
5. "In the Advanced tab, configure advanced options for the interface." on Page 229
6. "In the RIP tab, configure RIP for the interface." on Page 230
7. "In the OSPF tab, configure OSPF for the interface." on Page 231
8. Click **OK**.

Creating an Aggregate Interface

To create an aggregate interface, take the following steps:

1. Select **Network** > **Interface**.

2. Click **New** > **Aggregate Interface**, and the Aggregate Interface dialog box will appear.



3. In the Basic tab, configure basic configurations for the interface.

Option	Description
Interface Name	Specify a name for the aggregate interface
Description	Enter descriptions for the aggregate interface as needed. The range is 0 to 63 characters.
Binding Zone	Specify the zone type. If Layer 3 or Layer 2 zone is selected, you should also select a security zone from the **Zone** drop-down list, and the interface will bind to a Layer 3 or Layer 2 zone. If No Binding is selected, you should also select an aggregate interface/redundant interface: Belong to — Description None — This interface does not belong to any object.
Zone	Select a security zone from the **Zone** drop-down list.
Aggregate Mode	Select an aggregate mode for the interface: • Forced: Aggregates multiple physical interfaces to form an aggregate interface. These physical interfaces will share the traffic passing through the aggregate interface equally. • LACP: Enable LACP on the interface to negotiate aggregate interfaces dynamically. LACP options are: • System priority: Specify the LACP system priority. The value range is 1 to 32768. The default value is 32768. This parameter is used to assure the interfaces of two ends are consistent. System will select interfaces based on the end with higher LACP system priority. The smaller the value is, the higher the priority will be. If the LACP system priorities of the two ends are equal, system will compare MACs of the two ends. The smaller the MAC is, the higher the priority will be.

Option	Description
	• Max bundle: Specify the maximum active interfaces. The value range is 1 to 16. The default value is 16. When the active interfaces reach the maximum number, the status of other legal interfaces will change to Standby. • Min bundle: Specify the minimum active interfaces. The value range is 1 to 8. The default value is 1. When the active interfaces reach the minimum number, the status of all the legal interfaces in the aggregate group will change to Standby automatically and will not forward any traffic.
Members	Specify the physical port for the aggregate interface. Select a desired port from the drop-down list. The port should not belong to any other interface or any security zone.
HA sync	Select this check box to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not selecting this check box disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
ISP	Select an ISP from the ISP drop-down list. After you bind the interface to the specified ISP, the link corresponding to the interface is bound to the ISP
WAN Interface	Select the **Enable** check box to set the interface to a WAN interface.
IP Configuration: Configure Static IP, Auto-obtain or PPPoE according to different IPs.	

Option	Description
Static IP	IP address: Specify an IP address for the interface.
	Netmask: Specify a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specify a management IP for the interface. Type the IP address into the box. • Secondary IP: Specify secondary IPs for the interface. You can specify up to 6 secondary IP addresses.
	DHCP: In the DHCP Configuration dialog box, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 268.
	DDNS: In the DDNS Configuration dialog box, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 277.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route.
	Advanced: • Distance: Specify a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specify a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specify a priority for the DNS server. Except for static DNS servers, system can also learn DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server according to its priority during DNS resolution. The priority is rep-

Option	Description
	resented in numbers from 1 to 255. The larger the number is, the higher the priority will be. The priority of static DNS servers is 20.
	DDNS: In the DDNS Configuration dialog box, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 277.
PPPoE	Obtain IP through PPPoE. Configure the following options: • User: Specify a username for PPPoE. • Password: Specify PPPoE user's password. • Confirm Password: Enter the password again to confirm. • Idle interval: If the PPPoE interface has been idle (no traffic) for a certain period, i.e., the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30. • Re-connect Interval: Specify a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled. • Set gateway information from PPPoE server as the default gateway route - With this check box selected, system will set the gateway information provided by PPPoE server as the default gateway route.
Management	Select one or more management method check boxes to configure the interface management method.
Reverse Route	Enable or disable reverse route as needed: • Enable: Force to use a reverse route. If the reverse route is not available, packets will be dropped. This option is enabled by default.

Option	Description
	• Close: Reverse route will not be used. When reaching the interface, the reverse data stream will be returned to its original route without any reverse route check. That is, reverse packets will be sent from the ingress interface that initializes the packets. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
Members	Specify the physical port for the aggregate interface. Select a desired port from the drop-down list. The port should not belong to any other interface or any security zone.
Bandwidth	Specify the actual bandwidth value of the interface as needed. • Upstream Bandwidth : Specify the maximum value of the upstream rate of the interface. The value range is 512,000 to 1,000,000,000,000 bps. The default value is 1,000,000,000 bps. • Upstream Threshold : Specify the upstream bandwidth threshold of the interface. The value ranges from 0% to 100% . The default value is 0%. • Downstream Bandwidth : Specify the maximum value of the downstream rate of the interface. The value range is 512,000 to 1,000,000,000,000 bps. The default value is 1,000,000,000 bps. • Downstream Threshold : Specify the downstream bandwidth threshold of the interface. The value ranges from 0% to 100%. The default value is 0%.

4. "In the IPv6 Configuration tab, configure IPv6 for the interface." on Page 236

5. "In the Properties tab, configure properties for the interface." on Page 229

6. "In the Advanced tab, configure advanced options for the interface." on Page 229

7. "In the RIP tab, configure RIP for the interface." on Page 230

8. "In the OSPF tab, configure OSPF for the interface." on Page 231

9. In the Load Balance tab, configure a load balance mode for the interface. "Flow-based" means enabling automatic load balance based on the flow. This is the default mode. "Tuple" means enabling load based on the source/destination IP, source/destination MAC, source/destination interface or protocol type of packet, or the combination of the selected items.

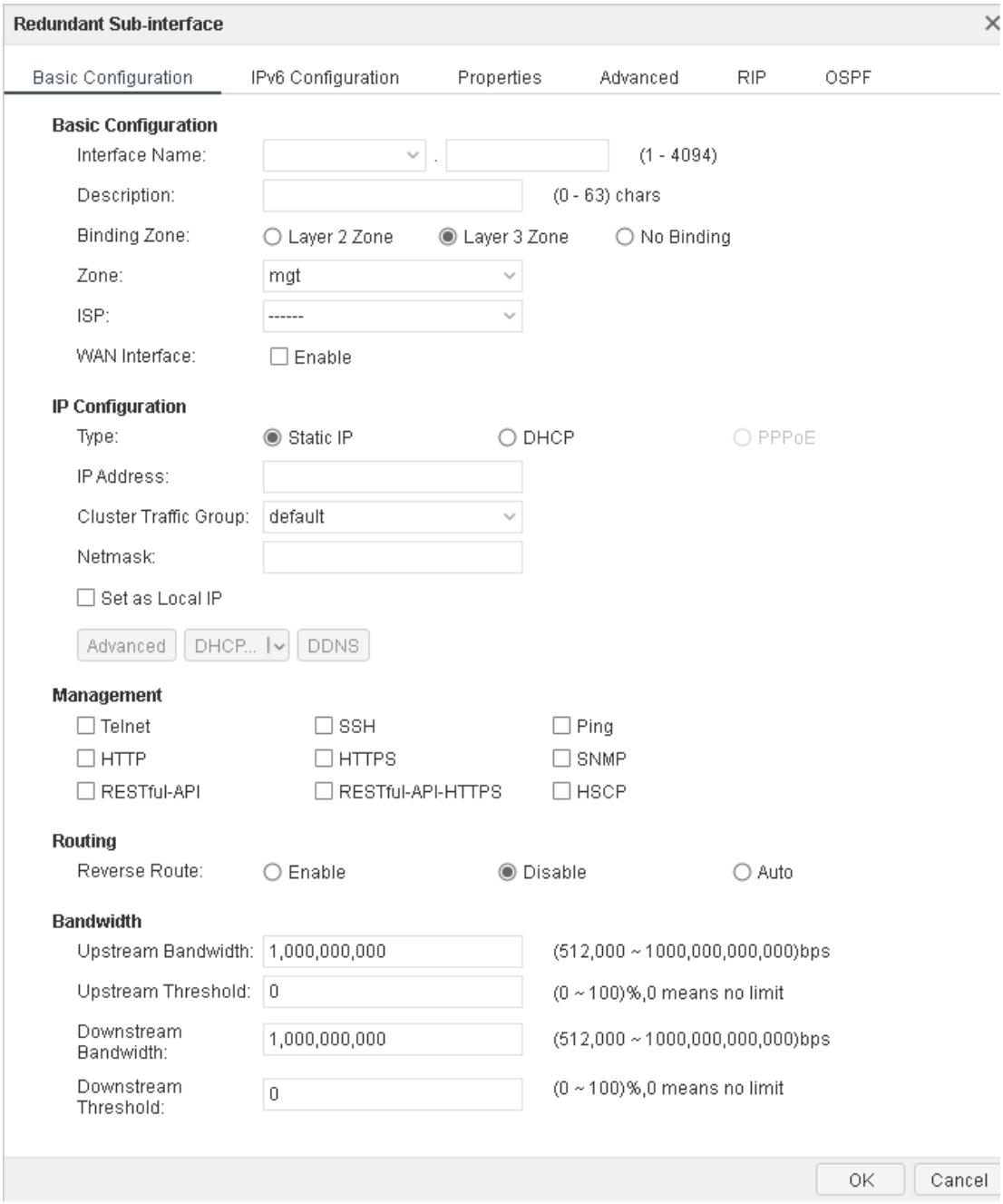
10. Click **OK**.

Creating a Redundant Interface

To create a redundant interface, take the following steps:

1. Select **Network** > **Interface**.

2. Click **New** > **Redundant Interface**, and the Redundant Interface dialog box will appear.



3. "In the Basic tab, configure basic configurations for the interface." on Page 239
4. "In the IPv6 Configuration tab, configure IPv6 for the interface." on Page 236
5. "In the Properties tab, configure properties for the interface." on Page 229
6. "In the Advanced tab, configure advanced options for the interface." on Page 229

7. "In the RIP tab, configure RIP for the interface." on Page 230

8. "In the OSPF tab, configure OSPF for the interface." on Page 231

9. Click **OK**.

Creating an Ethernet Sub-interface/an Aggregate Sub-interface/a Redundant Sub-interface

To create an ethernet sub-interface/an aggregate sub-interface/a redundant sub-interface, take the following steps:

1. Select **Network** > **Interface**.

2. Click **New** > **Ethernet Sub-interface/Aggregate Sub-interface/Redundant Sub-interface**.

3. In the Basic tab, configure basic configurations for the interface.

Option	Description
Interface Name	Specify a name for the virtual forward interface.
Description	Enter descriptions for the virtual forward interface as needed. The range is 0 to 63 characters.
Binding Zone	If Layer 3 zone is selected, you should also select a security zone from the **Zone** drop-down list, and the interface will bind to a Layer 3 zone. If No Binding is selected, the interface will not bind to any zone.
Zone	Select a security zone from the **Zone** drop-down list.
ISP	Select an ISP from the ISP drop-down list. After you bind the interface to the specified ISP, the link corresponding to the interface is bound to the ISP
WAN Interface	Select the **Enable** check box to set the interface to a WAN interface.
IP Configuration: Configure Static IP or Auto-obtain according to different IPs.	

Option	Description
Static IP	IP address: Specify an IP address for the interface.
	Netmask: Specify a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specify a management IP for the interface. Type the IP address into the box. • Secondary IP: Specify secondary IPs for the interface. You can specify up to 6 secondary IP addresses.
	DHCP: In the DHCP Configuration dialog box, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 268.
	DDNS: In the DDNS Configuration dialog box, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 277.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route.
	Advanced: • Distance: Specify a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specify a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specify a priority for the DNS server. Except for static DNS servers, system can also learn DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that the system can choose a DNS server according to its priority during DNS resolution. The priority is

Option	Description
	represented in numbers from 1 to 255. The larger the number is, the higher the priority will be. The priority of static DNS servers is 20.
	DDNS: In the DDNS Configuration dialog box, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 277.
PPPoE	Obtain IP through PPPoE. Configure the following options: (Effective only when creating a aggregate sub-interface) • User: Specify a username for PPPoE. • Password: Specify PPPoE user's password. • Confirm Password: Enter the password again to confirm. • Idle Interval: If the PPPoE interface has been idle (no traffic) for a certain period, i.e., the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30. • Re-connect Interval: Specify a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled. • Set gateway information from PPPoE server as the default gateway route - With this check box selected, system will set the gateway information provided by PPPoE server as the default gateway route.
Management	Select one or more management method check boxes to configure the interface management method.
Reverse Route	Enable or disable reverse route as needed: • Enable: Force to use a reverse route. If the reverse route is not avail-

Option	Description
	able, packets will be dropped. This option is enabled by default. • Close: Reverse route will not be used. When reaching the interface, the reverse data stream will be returned to its original route without any reverse route check. That is, reverse packets will be sent from the ingress interface that initializes the packets. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
Bandwidth	Specify the actual bandwidth value of the interface as needed. • Upstream Bandwidth : Specify the maximum value of the upstream rate of the interface. The value range is 512,000 to 1,000,000,000,000 bps. The default value is 1,000,000,000 bps. • Upstream Threshold : Specify the upstream bandwidth threshold of the interface. The value ranges from 0% to 100% . The default value is 0%. • Downstream Bandwidth : Specify the maximum value of the downstream rate of the interface. The value range is 512,000 to 1,000,000,000,000 bps. The default value is 1,000,000,000 bps. • Downstream Threshold : Specify the downstream bandwidth threshold of the interface. The value ranges from 0% to 100%. The default value is 0%.

4. "In the IPv6 Configuration tab, configure IPv6 for the interface." on Page 236
5. "In the Properties tab, configure properties for the interface." on Page 229
6. "In the Advanced tab, configure advanced options for the interface." on Page 229
7. "In the RIP tab, configure RIP for the interface." on Page 230

8. "In the OSPF tab, configure OSPF for the interface." on Page 231

9. Click **OK**.

Editing an Interface

To edit an interface, take the following steps:

1. Select **Network** > **Interface**.

2. Select the Ethernet Interface/HA Interface you want to edit from the interface list and click **Edit**, and the Ethernet Interface/HA Interface dialog box will appear.

3. **In the Basic tab, configure basic configurations for the interface.**

Option	Description
Interface Name	Specify a name for the interface.
Description	Enter descriptions for the interface. The range is 0 to 63 characters.
Binding Zone	Specify the zone type. If Layer 3 or Layer 2 zone is selected, you should also select a security zone from the **Zone** drop-down list, and the interface will bind to a Layer 3 or Layer 2 zone. If No Binding is selected, you should also select an aggregate interface/redundant interface: Belong to: Aggregate Interface — The interface you specified belongs to an aggregate interface. • Interface Group: Choose an aggregate interface to which the aggregate interface belongs from the **Interface Group** drop-down list. • Port LACP priority: Port LACP priority determines the sequence of becoming the Selected status for the mem-

Option	Description
	bers in the aggregate group. The smaller the number is, the higher the priority will be. Which links in the aggregate group that will be aggregated is determined by the interface LACP priority and the LACP system priority. • Port timeout mode: The LACP timeout refers to the time interval for the members. System supports two timeout modes of **Fast** (1 second) and **Slow** (30 seconds, the default value), i.e., the timeout value for a member to wait for receiving LACPDU packets. If the local member does not receive the LACPDU packet from its peer after three times of the timeout value is exceeded, the peer will be concluded as down, and the status of the local member will change from Active to Selected, and stop traffic forwarding. Redundant Interface: The interface you specified belongs to a redundant interface. Select that redundant interface from the **Interface Group** drop-down list. None: This interface does not belong to any object
Zone	Select a security zone from the **Zone** drop-down list.
HA sync	Select this check box to enable the HA Sync function, which disables Local property and uses the virtual MAC, and the primary device will synchronize its information with the backup device; not selecting this check box disables the HA Sync function, which enables Local property and uses the original MAC, and the primary device will not synchronize its information with the backup device.
ISP	Select an ISP from the ISP drop-down list. After you bind the interface to the specified ISP, the link corresponding to the interface is bound to the ISP
WAN Interface	Select the **Enable** check box to set the interface to a WAN interface.

Option	Description
IP Configuration: Configure Static IP, Auto-obtain or PPPoE according to different IPs.	
Static IP	IP address: Specify an IP address for the interface.
	Netmask: Specify a netmask for the interface.
	Set as Local IP: In an HA environment, if this option is specified, the interface IP will not synchronize to the HA peer.
	Advanced: • Management IP: Specify a management IP for the interface. Type the IP address into the box. • Secondary IP: Specify secondary IPs for the interface. You can specify up to 6 secondary IP addresses.
	DHCP: In the DHCP Configuration dialog box, configure DHCP options for the interface. For detailed instructions, see "DHCP" on Page 268.
	DDNS: In the DDNS Configuration dialog box, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 277.
Auto-obtain	Set gateway information from DHCP server as the default gateway route: With this check box selected, system will set the gateway information provided by the DHCP server as the default gateway route.
	Advanced: • Distance: Specify a route distance. The value range is 1 to 255. The default value is 1. • Weight: Specify a route weight. The value range is 1 to 255. The default value is 1. • Management Priority: Specify a priority for the DNS server. Except for static DNS servers, system can also learn DNS servers dynamically via DHCP or PPPoE. Therefore, you need to configure priorities for the DNS servers, so that system can choose a DNS server

Option	Description
	according to its priority during DNS resolution. The priority is represented in numbers from 1 to 255. The larger the number is, the higher the priority will be. The priority of static DNS servers is 20.
	DDNS: In the DDNS Configuration dialog box, configure DDNS options for the interface. For detailed instructions, see "DDNS" on Page 277.
PPPoE	User: Specify a username for PPPoE. Password: Specify PPPoE user's password. Confirm Password: Enter the password again to confirm. Idle Interval: If the PPPoE interface has been idle (no traffic) for a certain period, i.e. the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30. Re-connect Interval: Specify a re-connect interval (i.e., system will try to re-connect automatically after being disconnected for the interval). The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled. Set gateway information from PPPoE server as the default gateway route: With this check box selected, system will set the gateway information provided by PPPoE server as the default gateway route.

Option	Description	
	Advanced	Access concentrator: Specify a name for the concentrator. Authentication: The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). You can select the radio button of the authentication method you need. Netmask: Specify a netmask for the IP address obtained via PPPoE. Static IP: You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the box. Service: Specify allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, system will accept any service returned from the server automatically. Distance: Specify a route distance. The value range is 1 to 255. The default value is 1. Weight: Specify a route weight. The value range is 1 to 255. The default value is 1.
	Set gateway information from PPPoE server as the default gateway route: With this check box selected, system will set the gateway information provided by PPPoE server as the default gateway route.	
Management	Select one or more management method check boxes to configure the interface management method.	
Reverse Route	Enable or disable reverse route as needed: • Enable: Force to use a reverse route. If the reverse route is not available, packets will be dropped. This option is enabled by default.	

Option	Description
	• Close: Reverse route will not be used. When reaching the interface, the reverse data stream will be returned to its original route without any reverse route check. That is, reverse packets will be sent from the ingress interface that initializes the packets. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send packets; otherwise the ingress interface that initializes the packets will be used as the egress interface that sends reverse packets.
Bandwidth	Specify the actual bandwidth value of the interface as needed. • Upstream Bandwidth : Specify the maximum value of the upstream rate of the interface. The value range is 512,000 to 1,000,000,000,000 bps. The default value is 1,000,000,000 bps. • Upstream Threshold : Specify the upstream bandwidth threshold of the interface. The value ranges from 0% to 100% . The default value is 0%. • Downstream Bandwidth : Specify the maximum value of the downstream rate of the interface. The value range is 512,000 to 1,000,000,000,000 bps. The default value is 1,000,000,000 bps. • Downstream Threshold : Specify the downstream bandwidth threshold of the interface. The value ranges from 0% to 100%. The default value is 0%.

4. "In the IPv6 Configuration tab, configure IPv6 for the interface." on Page 236

5. In the Properties tab, configure properties for the interface.

Property	Description
Duplex	Specify a duplex working mode for the interface. Options include auto, full duplex and half duplex. Auto is the default working mode, in which system will select the most appropriate duplex working mode automatically. 1000M

Property	Description
	half duplex is not supported.
Rate	Specify a working rate for the interface. Options include Auto, 10M, 100M and 1000M. Auto is the default working mode, in which system will detect and select the most appropriate working mode automatically. 1000M half duplex is not supported.
Combo Type	This option is applicable to the Combo port of copper port + fiber port. If both the copper port and the fiber port are plugged with cable, the fiber port will be prioritized by default; if the copper port is used at first, and the cable is plugged into the fiber port, and the fiber port will be used for data transmission after reboot. You can specify how to use a copper port or fiber port. For detailed options, see the following instructions: • Auto: The above default scenario. • Copper forced: The copper port is enforced. • Copper preferred: The copper port is prioritized. • Fiber forced: The fiber port is enforced. • Fiber preferred: The fiber port is prioritized. With this option configured, the device will migrate the traffic on the copper port to the fiber port automatically without reboot.
MTU	Specify a MTU for the interface. The value range is 1280 to 1500/1800 bytes. The default value is 1500. The max MTU may vary on different Hillstone platforms.
ARP Learning	Select the **Enable** check box to enable ARP learning.
ARP Timeout	Specify an ARP timeout for the interface. The value range is 5 to 65535 seconds. The default value is 1200.
Keep-alive IP	Specify an IP address that receives the interface's keep-alive packets.
MAC Clone	Select the **MAC clone** check box to enable the MAC clone function. System

Property	Description
	clones a MAC address to the Ethernet sub-interface. If you click **Restore Default MAC**, the Ethernet sub-interface will restore the default MAC address.

6. "In the Advanced tab, configure advanced options for the interface." on Page 229
7. "In the RIP tab, configure RIP for the interface." on Page 230
8. "In the OSPF tab, configure OSPF for the interface." on Page 231
9. Click **OK**.

Note:

- Before deleting an aggregate/redundant interface, you should remove other interfaces' bindings to it, aggregate/redundant sub-interfaces' configuration, its IP address configuration and its binding to the security zone.
- An Ethernet interface can only be edited but cannot be deleted.

DNS

DNS, the abbreviation for Domain Name System, is a computer and network service naming system in form of domain hierarchy. DNS is designed for TCP/IP network to query for Internet domain names (e.g., www.xxxx.com) and translate them into IP addresses (e.g., 10.1.1.1) to locate related computers and services.

The device's DNS provides the following functions:

- Server: Configure DNS servers for the device.
- Proxy: As a DNS proxy, the device can filter the DNS request according to the DNS proxy rules set by the user, and system will forward the qualified DNS request to the designated DNS server.
- Analysis: Set retry times and timeout for the device's DNS services, and TTL of responses for the device's DNS proxy services.
- Cache: Stores DNS mappings to the cache to speed up the query. You can create, edit and delete DNS mappings.

Configuring a DNS Server

You can configure a DNS server for system to implement DNS resolution. To create a DNS server, take the following steps:

1. Select **Network** > **DNS** > **DNS Server**.
2. Click **New**, and the DNS Server Configuration dialog box will appear.
3. Type the IP address for the DNS server into the **Server IP** box.
4. Select a VRouter from the **Virtual Router** drop-down list. The default VRouter is trust-vr.
5. Select an interface from the **Egress Interface** drop-down list. This parameter is mainly used for multi-exit DNS proxy. If the DNS server will only be used for DNS resolution, you can select the default "------".
6. Click **OK**.

Configuring a DNS Proxy

DNS Proxy function takes effect through the DNS proxy rules. Generally, a proxy rule consists of two parts: filtering condition and action. You can set the filtering condition by specifying traffic's ingress interface, source address, destination

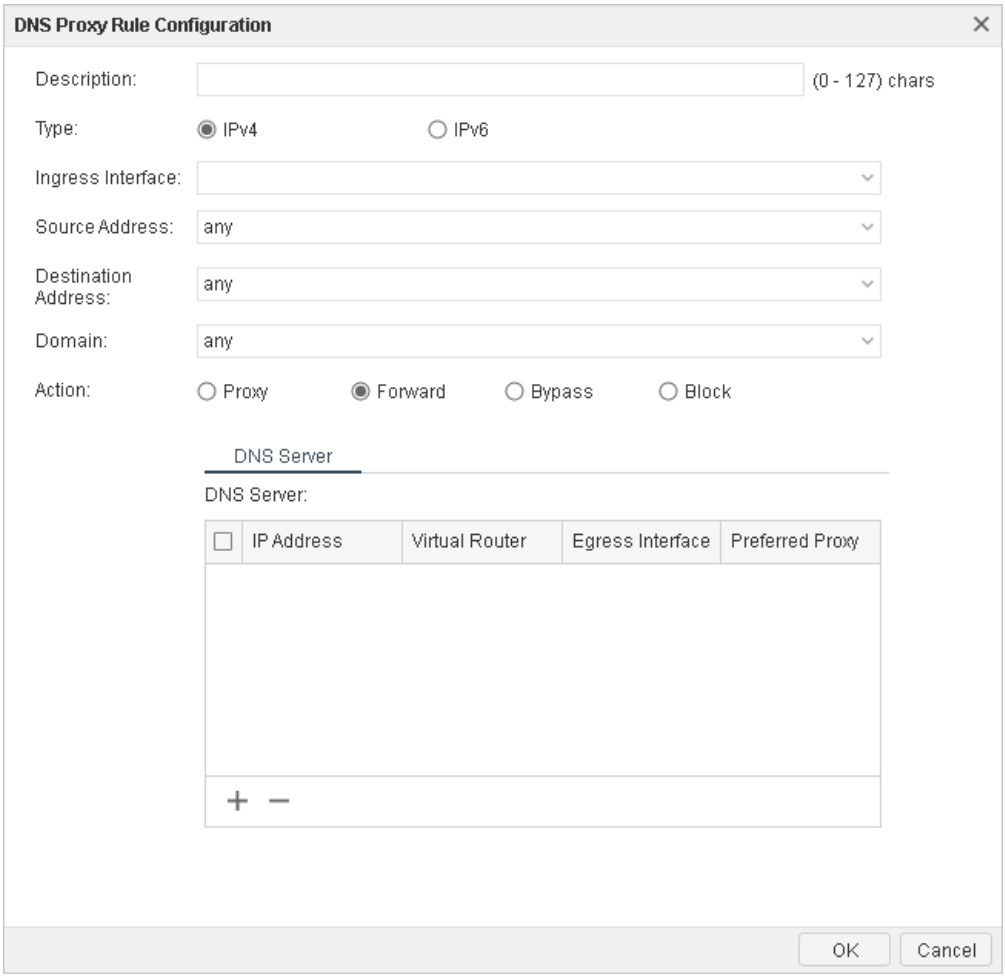
address, and domain name.

The action of the DNS proxy rules includes proxy, forward, bypass and block. If the action of a DNS proxy rule is specified as "Proxy", you need to configure a DNS proxy server, and then the DNS request meeting the filtering condition will be resolved by the DNS proxy server; if specified as "Forward", you need to configure a DNS server, and then the DNS request meeting the filtering condition will be resolved by the DNS server.

Configuring a DNS Proxy Rule

To create a DNS proxy rule, take the following steps:

1. Select **Network** > **DNS** > **DNS Proxy**.
2. Click **New**.



In the DNS Proxy Rule Configuration dialog box, configure the following settings.

Option	Description
Description	Add the description. The value range is 0 to 127 characters.
Ingress Interface	Specify the ingress interface of the DNS request needs to be macthed with the rule to filter the DNS request message. You can specify multiple interfaces. If specified, system will handle the traffic of the ingress interface according to the action set in the rule.
Source Address	Specify the source address of the DNS request needs to be macthed with the rule to filter the DNS request message. You can specify multiple source address filtering conditions. Select an address type from the **Address** drop-down list; select or type the source addresses based on the selected type; click "->" to add the addresses to the right pane; and after adding the desired addresses, click the blank area in this dialog box to complete the source address configuration. The default address configuration is any.
Destination Address	Specify the destination address of the DNS request needs to be macthed with the rule to filter the DNS request message. You can specify multiple destination address filtering conditions. Select an address type from the **Address** drop-down list; select or type the destination addresses based on the selected type; click "->" to add the addresses to the right pane; and after adding the desired addresses, click the blank area in this dialog box to complete the destination address configuration. The default address configuration is any.
Domain	Specify the domain name of the DNS request needs to be macthed with the rule to filter the DNS request message. You can specify multiple domain name filtering conditions. Click the **Domain** drop down list, and select the **Host Book** or **Domain** from the **Type** drop-down list; select or type the host books or domain names; click "->" to add the host books or domain names to the right

Option	Description
	pane; and after adding the desired the host books or domain names, click the blank area in this dialog box to complete the domain configuration. The domain name supports regular expressions, and only supports expressions containing "*". The default domain configuration is any.
Action	Specify the action for a DNS proxy rule. For the DNS request that meets the filtering conditions, system can proxy, bypass or block the traffic. • Proxy: If specified, the DNS request will be resolved by the proxy server. • Forward: If specified, the DNS request will be resolved by the configured DNS sever. The action takes effect only when the device works in the routing mode. • Release: If specified, the DNS request will be released and forwarded to the DNS server from which the original message is sent. • Block: If specified, the DNS request will be blocked and droped.
DNS Server	Specify the DNS server for a DNS proxy rule. If the action of the proxy rule is specified as "Proxy" or "Forward", you need to specify a DNS server. To add a DNS server, click "+" at the bottom of the DNS server list, and then specify the IP address and virtual router. Besides, you can add up to six DNS servers for one DNS rule, and you can specify the egress interface or enable the preferred proxy function for a DNS server as needed. If multiple DNS servers are configured, system will select the DNS server for resolution in the following order: • The DNS server with the preferred proxy enabled will be prioritized. • If there is no preferred server, system will query if there are DNS servers bound with egress interfaces; if so, system will select a DNS sever from the servers with egress interfaces in a round robin man-

Option	Description
	ner. • If there are no DNS servers bound with egress interfaces, system will select a DNS server from the rest DNS servers in a round robin manner. **Note:** • If the action of a DNS proxy rule is specified as "Proxy", the actual forwarding egress interface of a DNS proxy server will be determined based on the configured virtual router and egress interface. • If the action of a DNS proxy rule is specified as "Forward", the virtual server, egress interface and preferred proxy function configured for a DNS server will only be used as the basis for selecting a DNS server for resolution. After a DNS server is selected, the actual forwarding egress interface will be determined based on the routing configuration.

3. Click **OK**.

Enabling/Disabling a DNS Proxy Rule

By default, the configured DNS proxy rule will take effect immediately. You can terminate its control over the traffic by disabling the rule.

To disable or enable the function, take the following steps:

1. Select **Network** > **DNS** > **DNS Proxy**.
2. Select the rule that you want to enable/disable.
3. Click **Enable** or **Disable** to enable or disable the rule. You can view the status of a rule in the Status column.

Adjusting DNS Proxy Rule Position

Each DNS proxy rule is labeled with a unique ID. After a DNS request reaches the device, the device will query for DNS proxy rules by turn, and process the DNS request according to the first matched rule. However, the position of a DNS proxy rule is not determined by its ID number. By default, a newly created DNS proxy rule will be put at the bottom of all rules, that is, the lowest priority. You can move the position of DNS proxy rules to adjust their priority. The DNS proxy rule position can be an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after an ID or a name.

To adjust the rule position, take the following steps:

1. Select **Network** > **DNS** > **DNS Proxy**.
2. Select the check box of the security policy whose position will be adjusted, and click **Priority**.
3. In the pop-up menu, click **Top**, **Bottom**, **Before Name** or **After Name**. If you select **Before ID** or **After ID**, you need to type an ID number into the text box. Then the selected rule will be moved before or after the specified rule.

DNS Proxy Global Configuration

To set the DNS proxy global configuration, take the following steps:

1. Select **Network** > **DNS** > **DNS Proxy**.
2. Click **DNS Proxy Global Configuration**.

In the DNS Proxy Global Configuration dialog box, configure the following settings.

Option	Description
TTL	Enable and specify the TTL for DNS-proxy's response packets. If the DNS-proxy requests are not responded after the TTL, the DNS client will clear all DNS records. The value range is 30 to 600 seconds. The default value is 60.
Server Track	Enable the DNS proxy server track and configure the time interval of tracking for DNS proxy server. The value range is 3 to 60 seconds, and the default value is 10 seconds. System will periodically detect the DNS proxy server at a specific time interval. When the server cannot be tracked, the IP address of server will be removed from the DNS resolution list untill the link is restored. By default, the tracking for DNS proxy server is enabled.
UDP Checksum	Click the check box to enable/disable calculating the checksum of UDP packet for DNS proxy. This function is enabled by default. System will calculate the checksum of UDP packet for DNS proxy when the DNS proxy on interfaces is enabled. If you need to improve the performance of the device, you can disable this function.

3. Click **OK**.

Configuring an Analysis

To configure the retry times and timeout for DNS requests, take the following steps:

1. Select **Network** > **DNS** > **Analysis**.
2. Select a retry times radio button. If there is no response from the DNS server after the timeout, system will send the request again; if there is still no response from the DNS server after the specified retry times (i.e. the number of times to repeat the DNS request), system will send the request to the next DNS server.
3. Select a timeout value radio button. System will wait for the DNS server's response after sending the DNS request and will send the request again if no response returns after a specified time. The period of waiting for a response is known as timeout.

4. When the device acts as a proxy, specify the TTL value for DNS responses in the **TTL** text box. The value range is 30 to 600 seconds.

5. Click **Apply**.

Configuring a DNS Cache

When using DNS, system might store the DNS mappings to its cache to speed up the query. There are three ways to obtain DNS mappings:

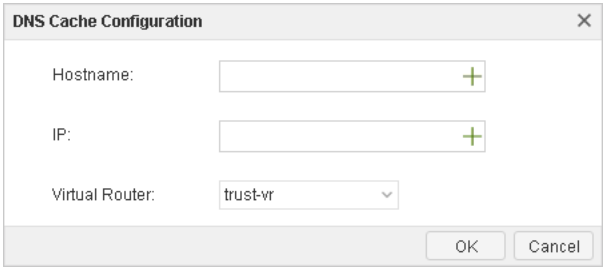
- Dynamic: Obtains from DNS response.
- Static: Adds DNS mappings to cache manually.
- Register: DNS hosts specified by some modules of security devices, such as NTP, AAA, etc.

For convenient management, DNS static cache supports group function, which means users combine the multiple domain hosts with the same IP address and virtual router into a single DNS static cache group.

To add a static DNS mapping to cache, take the following steps:

1. Select **Network** > **DNS** > **Cache**.

2. Click **New**, and the DNS Cache Configuration dialog box will appear.



Option	Description
Hostname	Specify the hostname of a DNS cache group. You can click + to add or click − button to delete the specified hostname. The maximum number of domain hosts is 128, and the maximum length of each hostname is 255 characters.
IP	Specify the host IPv4 address of a DNS cache group. You can click + to add or click − button to delete the specified IP. The maximum number of

Option	Description
	host IP address is 8, and the earlier configured IP will be matched first.
Virtual Router	Select a VRouter to which a DNS cache group belongs.

3. Click **OK**.

Note:

- Only DNS static cache group can support new, edit and delete operations, while dynamic and register cache cannot.
  - User can clear the register cache only by deleting the defined hosts in function module.
  - DNS static cache is superior to dynamic and register cache, which means the static cache will cover the same existed dynamic or register cache.

DHCP

DHCP, the abbreviation for Dynamic Host Configuration Protocol, is designed to allocate appropriate IP addresses and related network parameters for subnetworks automatically, thus reducing requirement on network administration. Besides, DHCP can avoid address conflict to assure the re-allocation of idle resources.

DHCP supports to allocate IPv4 and IPv6 addresses. After the IPv6 function is enabled, you can configure an interface of the device as a DHCP client to obtain an IPv6 address from a DHCP server. For the DHCP client configuration of the interface, you need to configure it in the Interface section. For the IPv6 configuration of the DHCP server and relay agent, see Configuring a DHCPv6 Server and Configuring a DHCPv6 Relay Agent.

System supports DHCP client, DHCP server and DHCP relay proxy.

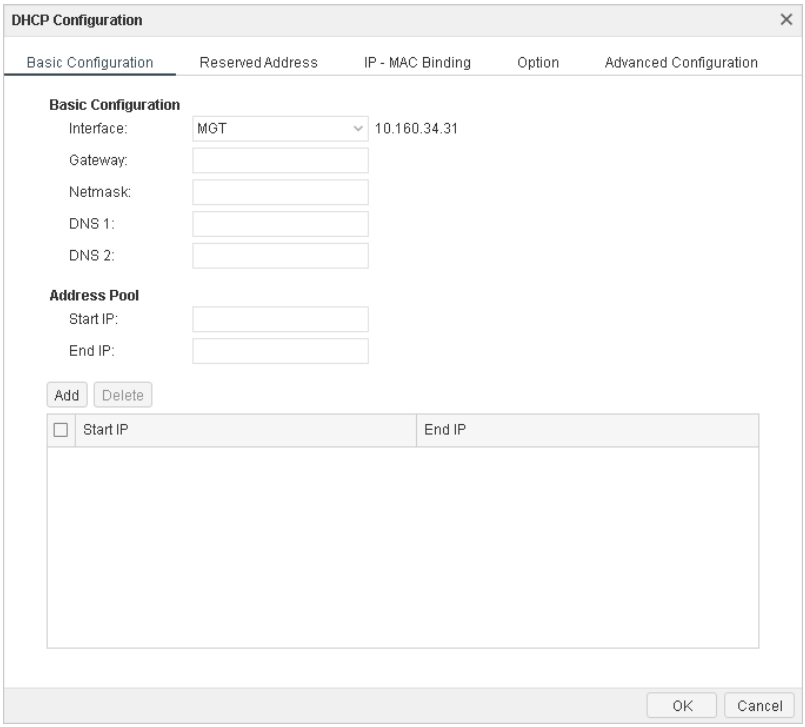
- DHCP client: The interface can be configured as a DHCP client and obtain IP addresses and network parameters from the DHCP server. For more information on configuring a DHCP client, see "Configuring an Interface" on Page 224.
- DHCP server: The interface can be configured as a DHCP server and allocate IP addresses and network parameters chosen from the configured address pool for the connected hosts.
- DHCP relay proxy: The interface can be configured as a DHCP relay proxy to obtain DHCP information from the DHCP server and forward the information to connected hosts.

The device is designed with all the above three DHCP functions, but an individual interface can be only configured with one of the above functions.

Configuring a DHCP Server

To create a DHCP server, take the following steps:

1. Select **Network** > **DHCP**.
2. Select **New** > **DHCP Server**, and the DHCP Configuration dialog box will appear.



3. In the Basic Configuration tab, configure as following:

Option	Description
Interface	Configure an interface which enables the DHCP server.
Gateway	Configure a gateway IP for the client.
Netmask	Configure a netmask for the client.
DNS1	Configure a primary DNS server for the client. Type the server's IP address into the box.
DNS2	Configure an alternative DNS server for the client. Type the server's IP address into the box.
Address Pool	Configure an IP range in the address pool. The IPs within this range will be allocated. Take the following steps: 1. Type the start IP and end IP into the **Start IP** and **End IP** boxes respectively. 2. Click **Add** to add an IP range which will be displayed in the list below.

Option	Description
	3. Repeat the above steps to add more IP ranges. To delete an IP range, select the IP range you want to delete from the list and click **Delete**.

4. Configure Reserved Address (IP addresses in the Reserved Address, within the IP range of the address pool, are reserved for the DHCP server and will not be allocated).

   To configure a reserved address, click the **Reserved Address** tab, type the start and end IP for an IP range into the **Start IP** and **End IP** boxes respectively, and then click **Add**. To delete an IP range, select the IP range you want to delete from the list and then click **Delete**.

5. Configure IP-MAC Binding. If the IP is bound to a MAC address manually, the IP will only be allocated to the specified MAC address.

   To configure an IP-MAC Binding, click the **IP-MAC Binding** tab and type the IP and MAC address into the **IP address** and **MAC** box respectively, type the description in the **Description** text boxes if necessary, and then click **Add**. Repeat the above steps to add multiple entries. To delete an IP-MAC Binding, select an entry from the list and click **Delete**.

6. In the Option tab, configure the options supported by DHCP server.

Option	Description
49	After you configure the option 49 settings, the DHCP client can obtain the list of the IP addresses of systems that are running the X window System Display Manager. To configure the option 49 settings: 1. Select **49** from the **Option** drop-down list. 2. Type the IP address of the system that is running the X window System Display Manager into the **IP address** box. 3. Click **Add**. 4. Repeat the above steps to add multiple entries. To delete an entry, select it from the list and click **Delete**.
60	Option 60 is written by the device when generating DHCP packets to identify the type or configuration of the device. After configuring the

Option	Description
	VCI carried by option 60 for DHCP server, the DHCP packets sent by the DHCP server will carry this option and the corresponding VCI. 1. Select **60** from the **Option** drop-down list. 2. Select **ASCII** or **HEX** from the **Format** drop-down list. When selecting ASCII, the VCI matching string must be enclosed in quotes if it contains spaces. 3. Enter the VCI in the **Sign** text box. 4. Click **Add**.
138	The DHCP server uses option 138 to carry a list of 32-bit (binary) IPv4 addresses indicating one or more CAPWAP ACs available to the WTP. Then the WTP discovers and connects to the AC according to the provided AC list. 1. Select **138** from the **Option** drop-down list. 2. Enter the AC IP address in the **IP address** text box. 3. Click **Add**. You can add up to four AC IP addresses. If you do not set the option 138 for the DHCP server or the DHCP client does not request option 138, DHCP server will not offer the option 138 settings.

7. In the Advanced tab, configure the DHCP server's advanced options.

Option	Description
Domain	Configure the domain name of the DHCP client.
Lease	Specify a lease time. The value range is 300 to 1048575 seconds. The default value is 3600. Lease is the period during which a client is allowed to use an IP address, starting from the time the IP address is assigned. After the lease expires, the client will have to request an IP address again from the

Option	Description
	DHCP server. The client will send a lease renewal request to the original DHCP server after 50% of the lease time has expired; and the client will broadcast a lease renewal request to renew the IP address after 87.5% of the lease time has expired.
Auto Configure	Enable automatic configuration. Select an interface with DHCP client enabled on the same gateway from the drop-down list. "----" indicates auto configure is not enabled. Auto configure will activate function in the following condition: Another interface with DHCP configured on the device enables DHCP client. When auto configure is enabled, if the DHCP server (Hillstone device) does not have DNS, WINS or domain name configured, the DHCP client (DHCP) will dispatch the DNS, WINS and domain name information obtained from a connected DHCP server to the host that obtains such information from the DHCP server(Hillstone device). However, the DNS, WINS and domain name that are configured manually still have the priority.
WINS1	Configure a primary WINS server for the client. Type the server's IP address into the box.
WINS2	Configure an alternative WINS server for the client. Type the server's IP address into the box.
SMTP Server	Configure a SMTP server for the client. Type the server's IP address into the box.
POP3 Server	Configure a POP3 server for the client. Type the server's IP address into the box.
News Server	Configure a news server for the client. Type the server's IP address into the box.
Relay Agent	When the device1 with DHCP server enabled is connected to another device2 with DHCP relay enabled, and the PC obtains device1's DHCP information from device2, then only when the relay agent's IP address

Option	Description
	and netmask are configured on device1 can the DHCP information be transmitted to the PC successfully. Relay agent: Type relay agent's IP address and netmask, i.e., the IP address and netmask for the interface with relay agent enabled on device2.
VCI-match-string	The DHCP server can verify the VCI carried by option 60 in the client's DHCP packets. When the VCI in the client's DHCP packet matches the VCI matching string you configured in the DHCP server, the DHCP server will offer the IP address and other corresponding information. If not, the DHCP server will drop the client's DHCP packets and will not reply to the client. If you do not configure a VCI matching string for the DHCP server, it will ignore the VCI carried by option 60. 1. Select the type of the VCI matching string, ASCII or HEX. When selecting ASCII, the VCI matching string must be enclosed in quotes if it contains spaces. 2. Enter the VCI matching string in the text box.

8. Click **OK**.

Configuring a DHCP Relay Proxy

The device can act as a DHCP relay proxy to receive requests from a DHCP client and send requests to the DHCP server, and then obtain DHCP information from the server and return it to the client.

To create a DHCP relay proxy, take the following steps:

1. Select **Network** > **DHCP**.
2. Click **New** > **DHCP Relay Proxy**.
3. In the DHCP Relay Proxy dialog box, select an interface to which the DHCP Relay Proxy will be applied from the **Interface** drop-down list.

4. Type the IP addresses of DHCP servers into the **Server 1**/**Server 2**/**Server 3** boxes.

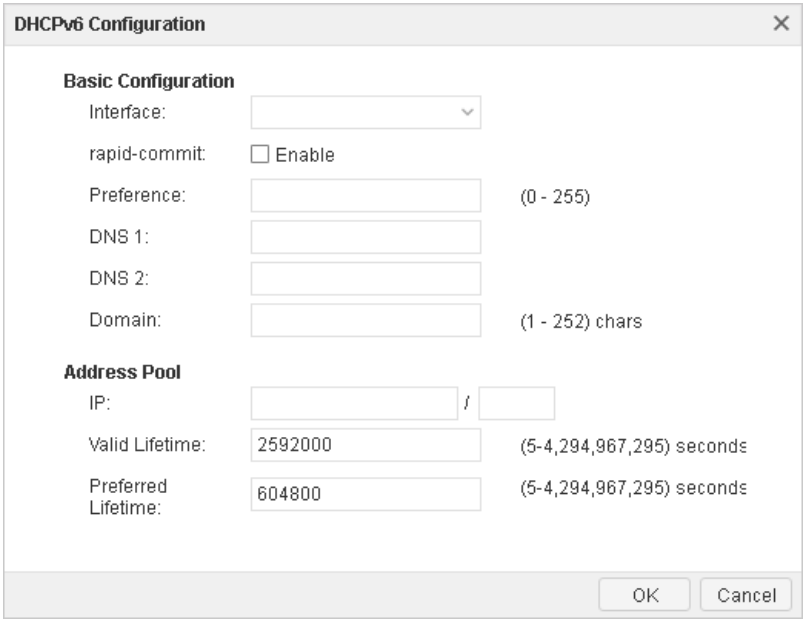
5. Click **OK**.

Configuring a DHCPv6 Server

To create a DHCPv6 server to allocate IPv6 addresses, take the following steps:

1. Select **Network** > **DHCP**.

2. Select **New** > **DHCPv6 Server**.



In the DHCPv6 Configuration dialog box, configure as following:

Option	Description
Interface	Configure an interface which enables the DHCPv6 server to allocate IPv6 addresses to DHCP clients in the subnets.
rapid-commit	Selecting this check box can help fast get IPv6 address from the server. You need to enable both of the DHCP client and server's Rapid-commit function.
Preference	Specify the priority of the DHCPv6 server. The range should be from 0 to 255. The bigger the value is, the higher the priority is.
DNS1	Configure a primary DNS server for the client. Type the server's IP address into the box.
DNS2	Configure an alternative DNS server for the client. Type the server's IP address into the box.
Domain	Configure the domain name for the DHCP client.
Address Pool: Configure the address pool for the DHCP server. System can act as a DHCPv6 server to allocate IPv6 addresses for the DHCP clients in the subnets. You need to specify the address range of the address pool for allocation.	
IP	Specify the IPv6 address prefix and prefix length.
Valid Lifetime	Specify the valid lifetime for the IPv6 address.
Preferred Life-time	Specify the preferred lifetime for the IPv6 address. The preferred lifetime should not be larger than the valid lifetime.

3. Click **OK**.

Configuring a DHCPv6 Relay Proxy

The device can act as a DHCPv6 relay proxy to receive requests from a DHCPv6 client and send requests to the DHCPv6 server, and then obtain DHCP information from the server and return it to the client .

To create a DHCPv6 relay proxy, take the following steps:

1. Select **Network** > **DHCP**.

2. Click **New** > **DHCPv6 Relay Proxy**.

3. In the DHCP Relay Proxy dialog box, select an interface to which the DHCPv6 Relay Proxy will be applied from the **Interface** drop-down list.

4. Type the IPv6 addresses of DHCPv6 servers into the **Server 1**/**Server 2**/**Server 3** boxes.

5. If the DHCPv6 server is specified as link-local address, you need to select the egress interface name from **Egress Interface 1**/**Egress Interface 2**/**Egress Interface 3** drop-down list.

6. Click **OK**.

DDNS

DDNS (Dynamic Domain Name Server) is designed to resolve fixed domain names to dynamic IP addresses. Generally you will be allocated with a dynamic IP address from ISP each time you connect to the Internet, i.e., the allocated IP addresses for different Internet connections will vary. DDNS can bind the domain name to your dynamic IP address, and the binding between them will be updated automatically each time you connect to the Internet.

In order to enable DDNS, you will have to register in a DDNS provider to obtain a dynamic domain name. Hillstone devices support the following 5 DDNS providers, and you can visit one of the following websites to complete the registration:

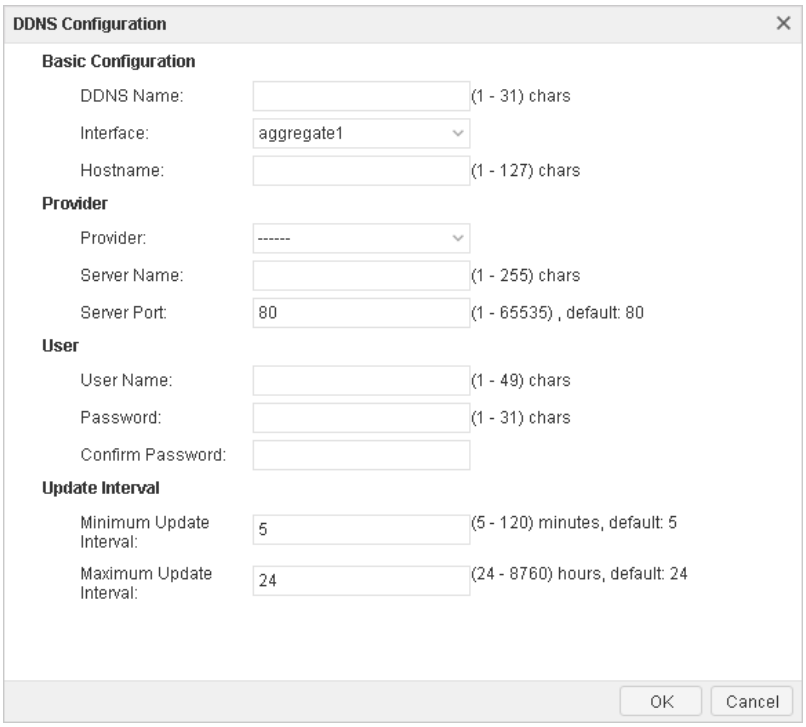
- dyndns.org: http://dyndns.com/dns
- 3322.org: http://www.pubyun.com
- no-ip.com: http://www.noip.com
- Huagai.net: http://www.ddns.com.cn
- ZoneEdit.com: http://www.zoneedit.com

Configuring a DDNS

To create a DDNS, take the following steps:

1. Select **Network** > **DDNS**.

2. Click **New**.



3. In the DDNS Configuration dialog box, configure as follows:

Option	Description
DDNS Name	Specify the name of DDNS.
Interface	Specify the interface to which DDNS is applied.
Hostname	Specify the domain name obtained from the DDNS provider.
Provider	Specify a DDNS provider. Choose one from the drop-down list.
Server Name	Specify a server name for the configured DDNS.
Server Port	Specify a server port number for the configured DDNS. The value range is 1 to 65535. The default value is 80.
User Name	Specify the user name registered in the DDNS provider.
Password	Specify the corresponding password.
Confirm Pass-	Enter the password again to confirm.

Option	Description
word	
Minimum Update Interval	When the IP address of the interface with DDNS enabled changes, system will send an update request to the DDNS server. If the server does not respond to the request, system will send the request again according to the configured min update interval. For example, if the minimum update interval is set to 5 minutes, then system will send the second request 5 minutes after the first request failure; if it fails again, system will send the third request 10 (5x2) minutes later; if it fails again, and system will send the fourth request 20 (10*2) minutes later, and so forth. The value will not increase anymore when reaching 120 minutes. That is, system will send the request at a fixed interval of 120 minutes. The value range is 1 to 120 minutes. The default value is 5.
Maximum Update Interval	In case the IP address has not changed, system will send an update request to the DDNS server at the maximum update interval. Type the maximum update interval into the box. The value range is 24 to 8760 hours. The default value is 24.

4. Click **OK**.

Note: The Server name and Server port in the configuration options must be the corresponding name and port of the DDNS server. Do not configure these options if the exact information is unknown. The server will return the name and port information automatically after connection to the DDNS server has been established successfully.

PPPoE

PPPoE, Point-to-Point Protocol over Ethernet, combines PPP protocol and Ethernet to implement access control, authentication, and accounting on clients during an IP address allocation.

The implementation of PPPoE protocol consists of two stages: discovery stage and PPP session stage.

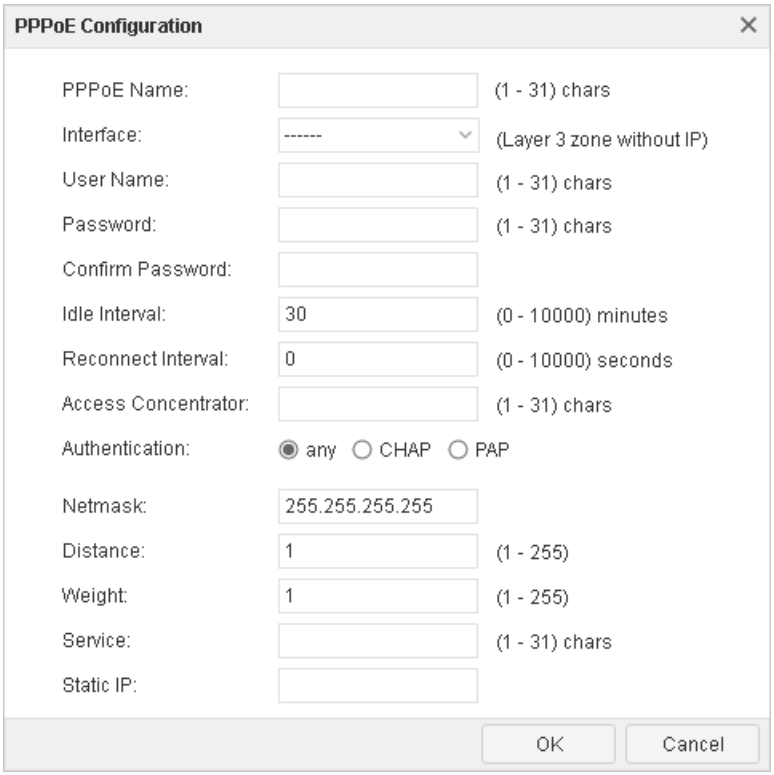
- Discovery stage: The client discovers the access concentrator by identifying the Ethernet MAC address of the access concentrator and establishing a PPPoE session ID.
- PPP session stage: The client and the access concentrator negotiate over PPP. The negotiation procedure is the same with that of a standard PPP negotiation.

Interfaces can be configured as PPPoE clients to accept PPPoE connections.

Configuring PPPoE

To create a PPPoE instance, take the following steps:

1. Select **Network** > **PPPoE**.
2. Click **New**.



3. In the PPPoE Configuration dialog box, configure as follows.

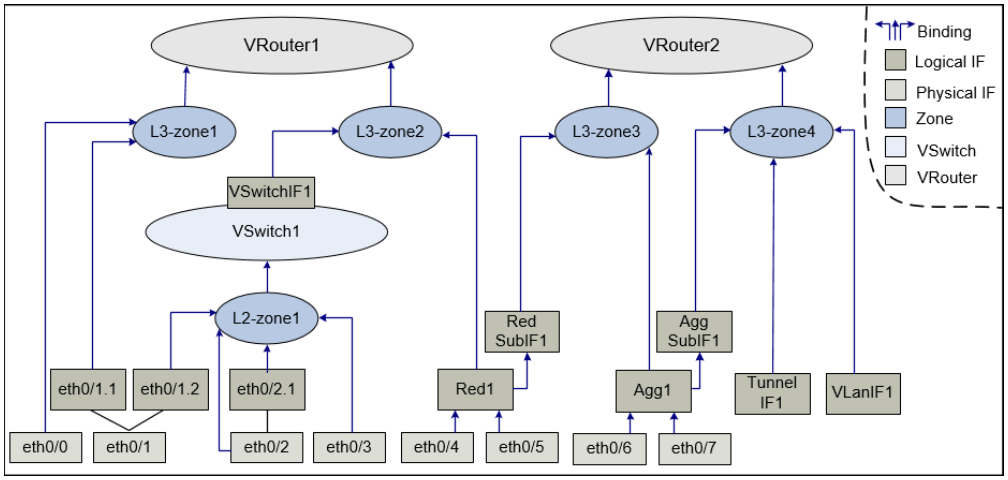
Option	Description
PPPoE Name	Specify a name for the PPPoE instance.
Interface	Select an interface from the drop-down list.
User Name	Specify a username.
Password	Specify the corresponding password.
Conform Password	Enter the password again to confirm.
Idle Interval	Automatic connection. If the PPPoE interface has been idle (no traffic) for a certain period, i.e., the specified idle interval, system will disconnect the Internet connection; if the interface requires Internet access, system will connect to the Internet automatically. The value range is 0 to 10000 minutes. The default value is 30.
Reconnect Inter-	If the PPPoE connection disconnects for any reason for a certain period,

Option	Description
val	i.e. the specified re-connect interval, system will try to re-connect automatically. The value range is 0 to 10000 seconds. The default value is 0, which means the function is disabled.
Access Concentrator	Specify a name for the concentrator.
Authentication	The devices will have to pass PPPoE authentication when trying to connect to a PPPoE server. The supported authentication methods include CHAP, PAP and Any (the default, anyone between CHAP and PAP). To configure a PPPoE authentication method, click the authentication you want to select. The configured authentication must be the same with that configured in the PPPoE server.
Netmask	Specify a netmask for the IP address obtained via PPPoE.
Distance	Specify a route distance. The value range is 1 to 255. The default value is 1.
Weight	Specify a route weight. The value range is 1 to 255. The default value is 1.
Service	Specify allowed service. The specified service must be the same with that provided by the PPPoE server. If no service is specified, system will accept any service returned from the server automatically.
Static IP	You can specify a static IP address and negotiate to use this address to avoid IP change. To specify a static IP address, type it into the box.

4. Click **OK**.

Virtual Router

Virtual Router (VRouter) is known as VR in system. VR acts as a router, and different VRs have their own independent routing tables. A VR named "trust-vr" is implemented with the system, and by default, all of the Layer 3 security zones are bounded to the trust-vr automatically. Hillstone devices support multiple VRs, and the max amount of supported VRs may vary with different hardware platforms. Multiple VRs divide a device into multiple virtual routers, and each router utilizes and maintains their independent routing table. In such a case one device is acting as multiple routers. Multiple VRs allow a device to achieve the effects of the address isolation between different route zones and address overlapping between different VRs, as well as to avoid route leaking to some extent, enhancing route security of network. For more information about the relationship between interface, security zone, VSwitch and VRouter, see the following diagram:



As shown above, the binding relationship between them are:

- Interfaces are bound to security zones. Those that are bound to Layer 2 security zones and Layer 3 security zones are known as Layer 2 interfaces and Layer 3 interfaces respectively. One interface can be only bound to one security zone; the primary interface and sub interface can belong to different security zones.
- Security zones are bound to a VSwitch or VRouter. Layer 2 security zones are bound to a VSwitch (by default the pre-defined Layer 2 security zone is bound to the default VSwitch1), and Layer 3 security zones are bound to a VRouter (by default the pre-defined Layer 3 security zone is bound to the default trust-vr), thus realizing the binding between the interfaces and VSwitch or VR. One security zone can be only bound to one VSwitch or VR.

Creating a Virtual Router

To create a Virtual Router, take the following steps:

1. Select **Network** > **Virtual Router** > **Virtual Router**.
2. Click **New**, and the Virtual Router Configuration dialog box will appear.
3. Type the name into the **Virtual Router** text box.
4. Click **OK**.

Virtual Switch

System might allow packets between some interfaces to be forwarded in Layer 2 (known as transparent mode), and packets between some interfaces to be forwarded in Layer 3 (known as routing mode), specifically depending on the actual requirement. To facilitate a flexible configuration of hybrid mode of Layer 2 and Layer3, system introduces the concept of Virtual Switch (VSwitch). By default system uses a VSwitch known as Vswitch1. Each time you create a VSwitch, system will create a corresponding VSwitch interface (VSwitchIF) for the VSwitch automatically. You can bind an interface to a VSwitch by binding that interface to a security zone, and then binding the security zone to the VSwitch.

A VSwitch acts as a Layer 2 forwarding zone, and each VSwitch has its own independent MAC address table, so the packets of different interfaces in one VSwitch will be forwarded according to Layer 2 forwarding rules. You can configure policy rules conveniently in a VSwitch. A VSwitchIF virtually acts as a switch uplink interface, allowing packets forwarding between Layer 2 and Layer 3.

Creating a VSwitch

To create a VSwitch, take the following steps:

1. Select **Network** > **VSwitch**.
2. Click **New**, and the VSwitch Configuration dialog box will appear.

Options are described as follows.

Option	Description
VSwitch Name	Specify a name for the VSwitch.
Forward Tagged Packets	Enable VLAN transparent so that the device can transmit VLAN tagged packets transparently, i.e., packets tagged with VLAN ID will still keep the original ID after passing through the device.

Option	Description
Forward Double Tagged Packets	Enable VLAN transparent so that the device can transmit VLAN double tagged packets transparently, i.e., packets tagged with VLAN ID will still keep the original ID after passing through the device.
Drop Unknown Multicast Packets	Drops the packets sent to unknown multicast to save bandwidth.

3. Click **OK**.

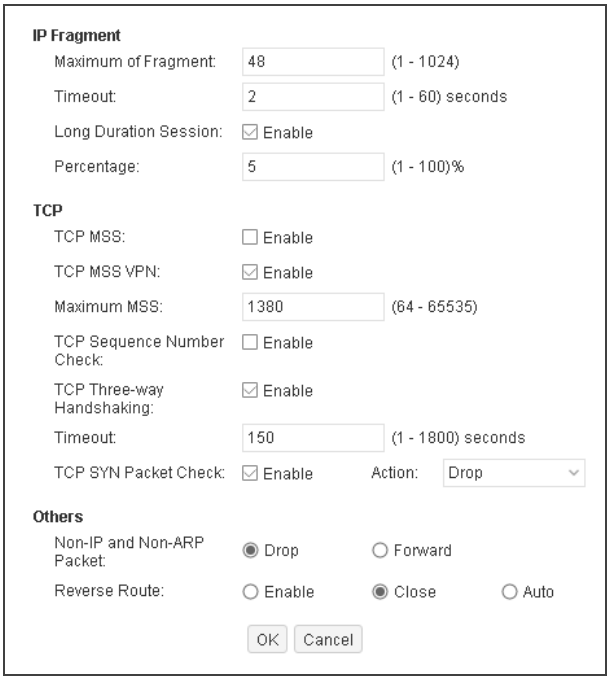
Global Network Parameters

Global network parameters are the settings for the data stream related to the whole system, and all data packets (TCP and IP packets) flowing through system are subject to those parameters.

Configuring Global Network Parameters

To configure global network parameters, take the following steps:

1. Select **Network** > **Global Network Parameters** > **Global Network Parameters**.



2. Configure the following parameters.

IP Fragment	
Maximum Fragment Number	Specify a maximum fragment number for every IP packet. The value range is 1 to 1024. The default value is 48. Any IP packet that contains more fragments than this number will be dropped.
Timeout	Specify a timeout period of fragment reassembling. The value range is 1 to 30. The default value is 2. If the Hillstone device has not received all the fragments after the timeout, the packet will be dropped.
Long Duration Session	Enable or disable long duration session. If this function is enabled, specify long duration session's percentage in the **Percentage** text box below. The default value is 10, i.e., 10% of long duration session in the total sessions.
TCP	
TCP MSS	Specify a MSS value for all the TCP SYN/ACK packets. Select the **Enable** check box, and type the value into the **Maximum MSS** text box below.
Maximum MSS	Type the max MSS value into the **Maximum MSS** text box below. The value range is 64 to 65535. The default value is 1448.
TCP MSS VPN	Specify a MSS value for IPSec VPN's TCP SYN packets. Select the **Enable** check box, and type the value into the **Maximum MSS** text box below.
Maximum MSS	Type the max MSS value for IPSEC VPN into the **Maximum MSS** text box below. The value range is 64 to 65535. The default value is 1380.
TCP Sequence Number Check	Configure if the TCP sequence number will be checked. When this function is enabled, if the TCP sequence number exceeds TCP window, that TCP packet will be dropped.
TCP Three-way Handshaking	Configure if the timeout of TCP three-way handshaking will be checked. Select the **Enable** check box to enable this function, and specify a timeout value in the **Timeout** text box below. The value range is 1 to 1800 seconds. The default value is 20. If the three-way handshaking has not been completed after timeout, the connection will be dropped.

IP Fragment	
TCP SYN Packet Check	Select the **Enable** check box to enable this functionand specify the action for TCP non-SYN packet. When the received packet is a TCP SYN packet, the TCP connection will be established. When the received packet is a TCP non-SYN packet, the packet will be processed according to the specified action. • Drop: When the received packet is a TCP non-SYN packet, the system will drop the packet. • RST: When the received packet is a TCP non-SYN packet, the system will drop the packet and send RST packet to the peer device.
Others	
Non-IP and Non-ARP Packet	Specify how to process packets that are neither IP nor ARP.
Reverse Route	Enable or disable reverse route as needed: • Enable: Force to use a reverse route. If the reverse route is not available, packets will be dropped. • Close: Reverse route will not be used. When reaching the device, the reverse data stream will be returned to its original route without any reverse route check. • Auto: Reverse route will be prioritized. If available, the reverse route will be used to send reverse packets; otherwise the packets will be returned to its original route.

3. Click **OK**.

Chapter 9 Advanced Routing

Routing is the process of forwarding packets from one network to the destination address in another network. Router, a packet forwarding device between two networks, is designed to transmit packets based on the various routes stored in routing tables. Each route is known as a routing entry.

Hillstone devices are designed with Layer 3 routing. This function allows you to configure routing options and forward various packets via VRouter. System implements with a default VRouter trust-vr.

Hillstone devices support destination routing, ISP routing, Source-Based Routing (SBR), Source-Interface-Based Routing (SIBR), Destination-Interface-Based Routing (DIBR), Policy-Based Routing (PBR), dynamic routing (including RIP, OSPF and BGP) and Equal Cost MultiPath Routing (ECMP).。

- "Destination Route" on Page 289: A manually-configured route which determines the next routing hop according to the destination IP address.

- "Destination-Interface Route" on Page 290: A route which selects routers and forwards data according to the destination IP address and ingress interface.
  - "Source Route" on Page 292: Source IP based route which selects routers and forwards data according to the source IP address.
  - "Source-Interface Route" on Page 294: Source IP and ingress interface based route which selects routers and forwards data according to the source IP address and ingress interface.
- "ISP Profile" on Page 296: Add a subnet to an ISP.
  - "ISP Route" on Page 299: A route which determines the next hop based on different ISPs.
  - "Policy-based Route" on Page 302: A route which selects routers and forwards data according to the source IP, destination IP address and service type.
  - Dynamic Routing: Select routers and forwards data according to the dynamic routing table generated by dynamic routing protocols ("RIP" on Page 310, OSPF or BGP).
  - ECMP: Load balancing traffic destined to the same IP address or segment in multiple routes with equal management distance.

When forwarding the inbound packets, the device will select a route in the following sequence: PBR > SIBR > SBR > DIBR > Destination routing/ISP routing/Proximity routing/Dynamic routing.

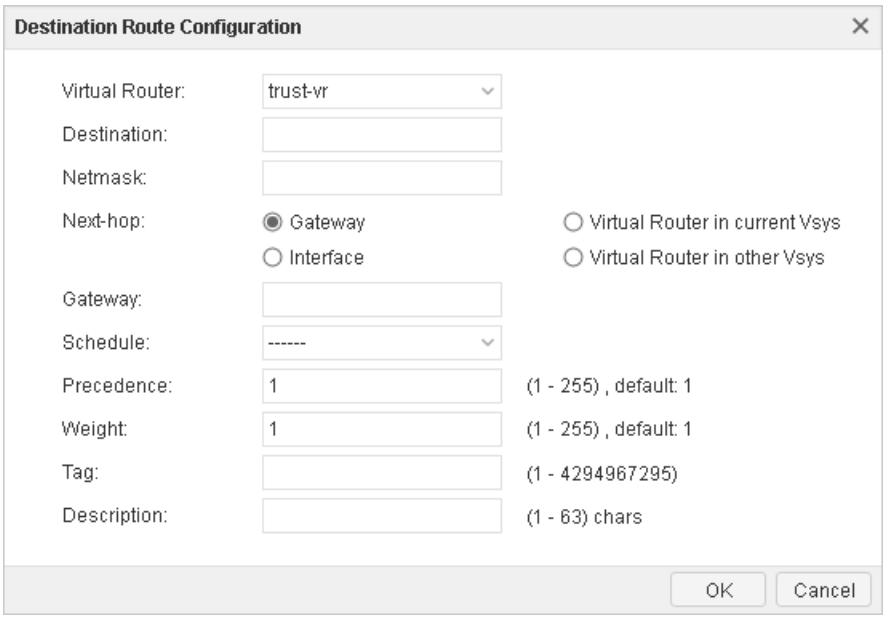
Destination Route

The destination route is a manually-configured route entry that determines the next routing hop based on the destination IP address. Usually a network with comparatively a small number of outbound connections or stable Intranet connections will use a destination route. You can add a default route entry at your own choice as needed.

Creating a Destination Route

To create a destination route, take the following steps:

1. Select **Network** > **Routing** > **Destination Route**.
2. Click **New**.



In the Destination Route Configuration dialog box, enter values.

Option	Description
Virtual Router	From the **Virtual Router** drop-down list, select a virtual router for the new route. The default value is "trust-vr".
Destination	Type the IP address for the route into the text box.

Option	Description
Netmask	Type the corresponding subnet mask into the text box.
Next-hop	To specify the type of next hop, click **Gateway**, **Virtual Router in current Vsys**, **Interface**, or **Virtual Router in other Vsys**. • Gateway: Type the IP address into the **Gateway** text box. • Virtual Router in current Vsys: Select a virtual router from the **Virtual Router** drop-down list. • Interface: Select an interface from the **Interface** drop-down list. Type the IP address into the **Gateway** text box. • Virtual Router in other Vsys: Select a Vsys from the **VSYS** drop-down list. Select a virtual router from the **Virtual Router** drop-down list.
Schedule	Specify a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. The route will take effect within the time range specified by the schedule.
Precedence	Type the route precedence into the text box. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the route into the text box. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the **Description** text box if necessary.

3. Click **OK**. The new route entry will be displayed in the destination route list.

Destination-Interface Route

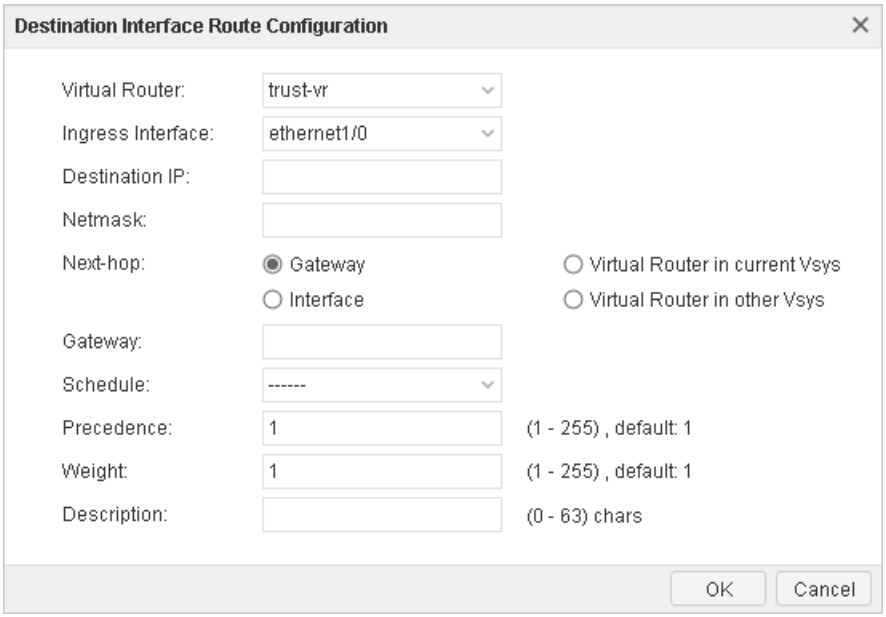
Destination interface route is designed to select a route and forward data based on the Destination IP address and ingress interface of a packet.

Creating a Destination-Interface Route

To create a Destination-Interface route, take the following steps:

1. Select **Network** > **Routing** > **Destination Interface Route**.

2. Click **New**.



In the Destination Interface Route Configuration dialog box, enter values.

Option	Description
Virtual Router	From the **Virtual Router** drop-down list, select a virtual router for the new route. The default value is "trust-vr".
Ingress Interface	Select an interface for the route from the drop-down list.
Destination IP	Type the destination IP for the route into the text box.
Netmask	Type the corresponding subnet mask into the text box.
Next-hop	To specify the type of next hop, click **Gateway**, **Virtual Router in current Vsys**, **Interface**, or **Virtual Router in other Vsys**. • Gateway: Type the IP address into the **Gateway** text box. • Virtual Router in current Vsys: Select a virtual router from the **Virtual**

Option	Description
	Router drop-down list. • Interface: Select an interface from the **Interface** drop-down list. Type the IP address into the **Gateway** text box. • Virtual Router in other Vsys: Select a Vsys from the **VSYS** drop-down list. Select a virtual router from the **Virtual Router** drop-down list.
Schedule	Specify a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. The route will take effect within the time range specified by the schedule.
Precedence	Type the route precedence into the text box. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the DIBR into the text box. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the **Description** text box if necessary.

3. Click **OK**. The new route entry will be displayed in the destination-interface route list.

Source Route

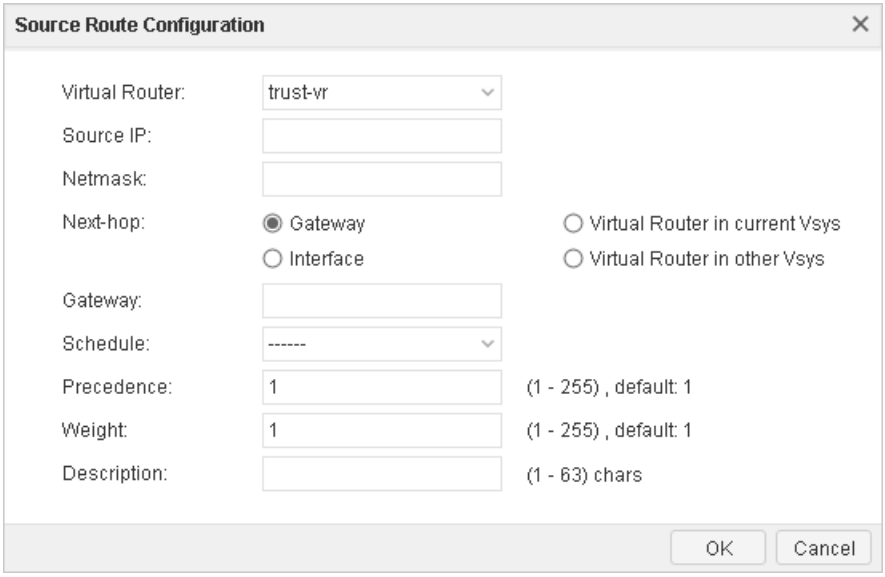
Source route is designed to select a router and forward data based on the source IP address of a packet.

Creating a Source Route

To create a source route, take the following steps:

1. Select **Network** > **Routing** > **Source Route**.

2. Click **New**.



In the Source Route Configuration dialog box, enter values.

Option	Description
Virtual Router	From the **Virtual Router** drop-down list, select a virtual router for the new route. The default value is "trust-vr".
Source IP	Type the source IP for the route into the text box.
Netmask	Type the corresponding subnet mask into the text box.
Next-hop	To specify the type of next hop, click **Gateway**, **Virtual Router in current Vsys**, **Interface**, or **Virtual Router in other Vsys**. • Gateway: Type the IP address into the **Gateway** text box. • Virtual Router in current Vsys: Select a virtual router from the **Virtual Router** drop-down list. • Interface: Select an interface from the **Interface** drop-down list. Type the IP address into the **Gateway** text box. • Virtual Router in other Vsys: Select a Vsys from the **VSYS** drop-down

Option	Description
	list. Select a virtual router from the **Virtual Router** drop-down list.
Schedule	Specify a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. The route will take effect within the time range specified by the schedule.
Precedence	Type the route precedence into the text box. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the route into the text box. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the **Description** text box if necessary.

3. Click **OK**. The new route entry will be displayed in the source route list.

Source-Interface Route

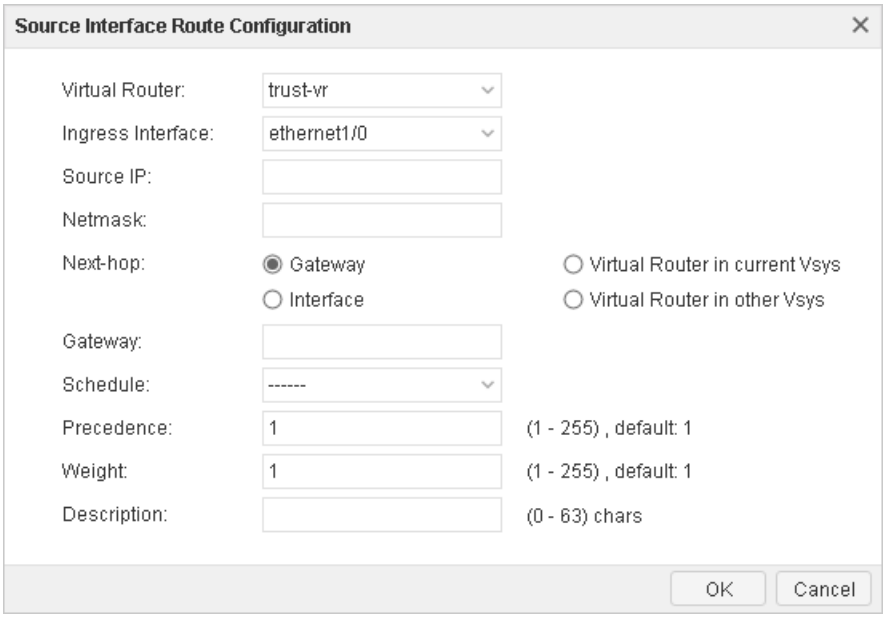
Source interface route is designed to select a router and forward data based on the source IP address and ingress interface of a packet.

Creating a Source-Interface Route

To create a Source-Interface route, take the following steps:

1. Select **Network** > **Routing** > **Source Interface Route**.

2. Click **New**.



In the Source Interface Route Configuration dialog box, enter values.

Option	Description
Virtual Router	From the **Virtual Router** drop-down list, select a virtual router for the new route. The default value is "trust-vr".
Ingress Interface	Select an interface for the route from the drop-down list.
Source IP	Type the source IP for the route into the text box.
Netmask	Type the corresponding subnet mask into the text box.
Next-hop	To specify the type of next hop, click **Gateway**, **Virtual Router in current Vsys**, **Interface**, or **Virtual Router in other Vsys**. • Gateway: Type the IP address into the **Gateway** text box. • Virtual Router in current Vsys: Select a virtual router from the **Virtual Router** drop-down list. • Interface: Select an interface from the **Interface** drop-down list. Type

Option	Description
	the IP address into the **Gateway** text box. • Virtual Router in other Vsys: Select a Vsys from the **VSYS** drop-down list. Select a virtual router from the **Virtual Router** drop-down list.
Schedule	Specify a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. The route will take effect within the time range specified by the schedule.
Precedence	Type the route precedence into the text box. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 1. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the route into the text box. This parameter is used to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the **Description** text box if necessary.

3. Click **OK**. The new route entry will be displayed in the source-interface route list.

ISP Profile

To configure an ISP route, you need to first add a subnet to an ISP, and then configure the ISP route. The destination of the route is determined by the name of the ISP. You can customize ISP information, or upload profiles that contain different ISP information. Besides, system provides a predefined IPv4 ISP profile, including three ISPs: China-telecom, China-unicom and China-mobile, as well as a predefined IPv6 ISP profile, including three ISPs: China-telecom-v6, China-unicom-v6 and China-mobile-v6.

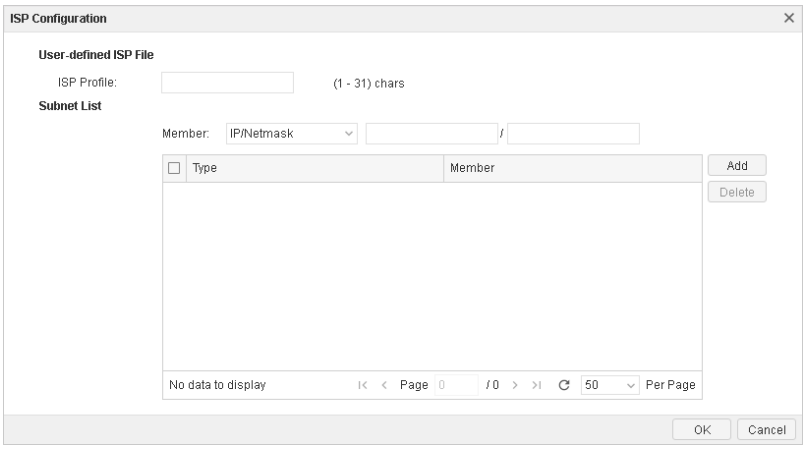
Creating an ISP Profile

To create an ISP Profile, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.

2. Select the **IPv4** or **IPv6** tab, this option can only be configured in the IPv6 version.

3. Click New. In the ISP Configuration dialog box, enter values.



Option	Description
ISP Profile	Type the name for the new ISP profile into the text box.
Subnet List	
Member	Specifies the member type of the ISP profile, including subnet member entry and ISP profile member entry. • Add subnet member: Select **IP/Netmask** from the drop-down list, and then type the IPv4 address and nermask for the subnet into the textbox. • Add an IPv4 ISP menber: Add an IPv4 ISP profile entry, that is to add other configured IPv4 ISP profile (predefined IPv4 ISP profile or user-defined IPv4 ISP profile), select **ISP Profile** from the drop-down list, and then select the ISP profile name. When creating an IPv6 ISP profile: • Add subnet member: Select **IPv6/Prefix** from the drop-down list, and then type the IPv6 address and prefix for the subnet into the text-box. • Add an IPv6 ISP menber: Add an IPv6 ISP profile entry, that is to add other configured IPv6 ISP profile (predefined IPv6 ISP profile

Option	Description
	or user-defined IPv6 ISP profile), select **ISP Profile** from the drop-down list, and then select the ISP profile name.
Add	Add the member to the ISP profile. The member will be displayed in the list below. If needed, repeat the steps to add multiple members for the ISP profile.
Delete	To delete a member, select the member you want to delete from the list.

4. Click **OK**. The new ISP will be displayed in the ISP list.

Uploading an ISP Profile

To upload an ISP Profile, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.
2. Select the **IPv4** or **IPv6** tab, this option can only be configured in the IPv6 version.
3. Click Upload, and the User-defined ISP File dialog box will appear. Then, click Browse to select an ISP profile in your PC.

4. Click **Upload** to upload the selected ISP profile to the device.

Upgrading ISP Information

To upgrade ISP information, take the following steps:

1. Select **System** > **Upgrade Management** > **Information Database Update**.
2. Configure the upgrade information of predefined ISP profile in the **ISP Database** module, for specific configurations, refer to the **Upgrading System** > Update Information Database.

Saving a User-defined ISP Profile

To save a user-defined ISP profile to the local, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.
2. Select the **IPv4** or **IPv6** tab, this option can only be configured in the IPv6 version.
3. Click **Save**, and the Save ISP File dialog box will appear.
4. Select a user-defined ISP profile from the **ISP profile** drop-down list.
5. Click **Save** to save the profile to a specified location in your PC.

Deleting User-defined ISP Profile

To delete a user-defined ISP profile, take the following steps:

1. Select **Network** > **Routing** > **ISP Profile**.
2. Select the **IPv4** or **IPv6** tab, this option can only be configured in the IPv6 version.
3. Selete the user-defined ISP profile, and click **Delete**.

ISP Route

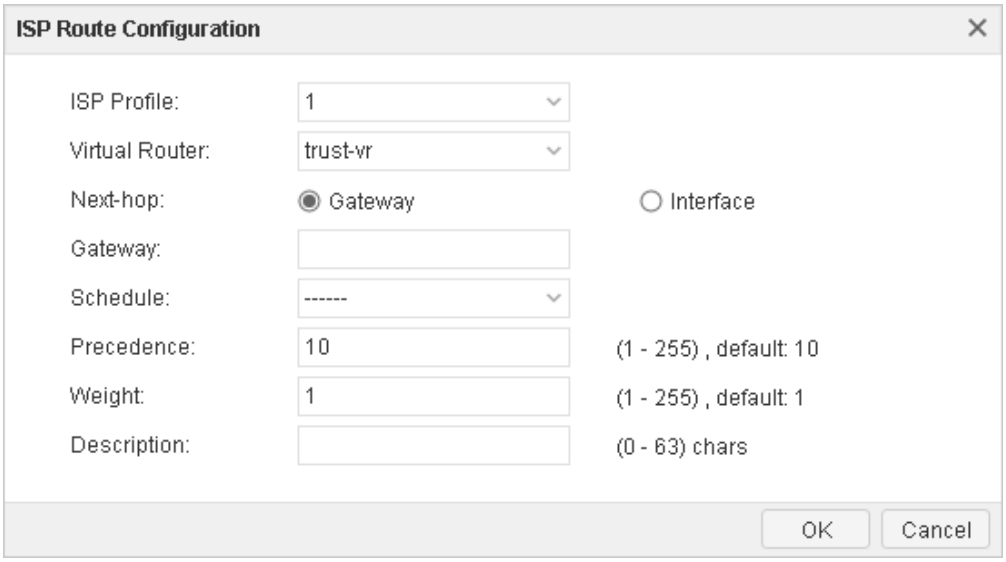
Generally many users might apply for multiple lines for load balancing purpose. However, a typical balance will not have the function based on the traffic's direction. For such a scenario, the device provides the ISP route, which allows traffic from different ISPs to take their proprietary routes, thus accelerating network access.

To configure an ISP route, first you need to add a subnet to an ISP, and then configure the ISP route. The destination of the route is determined by the name of the ISP. You can customize ISP information, or upload profiles that contain different ISP information. Besides, system provides a predefined IPv4 ISP profile, including three ISPs: China-telecom, China-unicom and China-mobile, as well as a predefined IPv6 ISP profile, including three ISPs: China-telecom-v6, China-unicom-v6 and China-mobile-v6.

Creating an ISP Route

To create an ISP route(IPv4 or IPv6), take the following steps:

1. Select **Network** > **Routing** > **ISP Route**.
2. Select the **IPv4** or **IPv6** tab, this option can only be configured in the IPv6 version.
3. **Click New. In the ISP Route Configuration dialog box, enter values.**



Option	Description
ISP Profile	Select an ISP profile name from the drop-down list.
Virtual Router	From the **Virtual Router** drop-down list, select a virtual router for the new route. The default value is "trust-vr".
Next-hop	To specify the type of next hop, click **Gateway** or **Interface**. • Gateway: Type the IP address into the **Gateway** text box. • Interface: Select an interface from the **Interface** drop-down list. Type the IP address into the **Gateway** text box.
Schedule	Specify a schedule when the rule will take effect. Select a desired schedule from the **Schedule** drop-down list. The route will take effect within the time range specified by the schedule. To create a new schedule, click **New Schedule**.
Precedence	Type the route precedence into the text box. The smaller the parameter is, the higher the precedence is. If multiple routes are available, the route with higher precedence will be prioritized. The value range is 1 to 255. The default value is 10. When the value is set to 255, the route will be invalid.
Weight	Type the weight for the ISP route into the text box. This parameter is used

Option	Description
	to determine the weight of traffic forwarding in load balance. The value range is 1 to 255. The default value is 1.
Description	Type the description information into the **Description** text box if necessary.

4. Click **OK**. The new route entry will be displayed in the ISP route list.

Policy-based Route

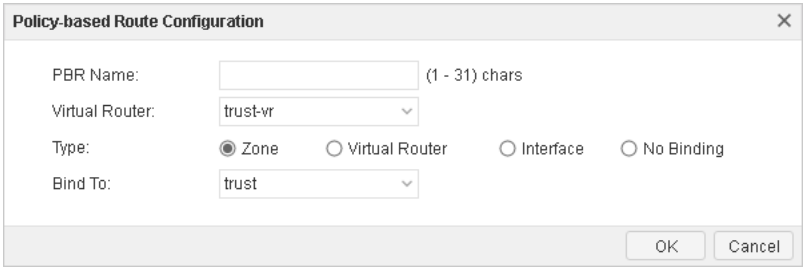
Policy-based Route (PBR) is designed to select a router and forward data based on the source IP address, destination IP address and service type of a packet.

Creating a Policy-based Route

To create a Policy-based route, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.

2. Click **New**, and select **PBR** from the drop-down list.



In the Policy-based Route Configuration dialog box, configure the following.

Option	Description
PBR Name	Specify a name for the policy-based route.
Virtual Router	From the **Virtual Router** drop-down list, select a virtual router for the new route. The default value is "trust-vr".
Type	Specify the object type that the policy-based route binds to. You can select **Zone**, **Virtual Router**, **Interface** or **No Binding**. • Zone: Click this option button and select a zone from the **Bind To**

Option	Description
	drop-down list. • Virtual Router: Click this option button, and the virtual router that the policy-based route binds to will be displayed below. • Interface: Click this option button and select an interface from the **Bind To** drop-down list. • No Binding: This policy-based route is no binding.

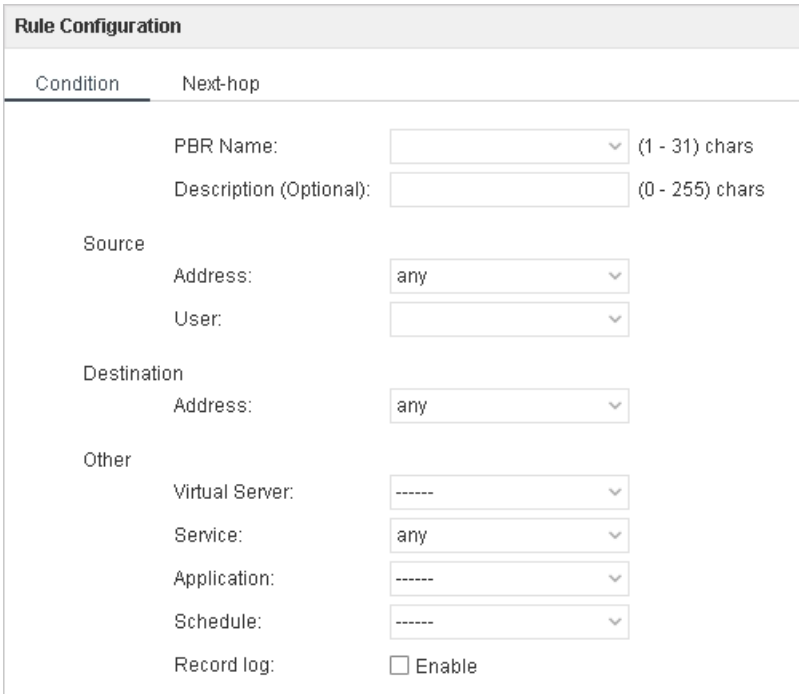
3. Click **OK**. The new route entry will be displayed in the policy-based route list.

Creating a Policy-based Route Rule

To create a Policy-based Route rule, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.

2. Click **New**, and select **Rule** from the drop-down list. The Rule Configuration dialog box will appear.



In the Condition tab, configure the following.

Option	Description
PBR Name	Specify a name for the policy-based route.
Description (Optional)	Specify the description for the PBR rule.
Source	
Address	Specify the source addresses of the PBR rule. 1. Select an address type from the **Address** drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click → to add the addresses to the right pane. 4. After adding the desired addresses, click the blank area in this dialog box to complete the source address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click **Add** to create a new address entry. • The default address configuration is any. To restore the configuration to this default one, select the **any** check box.
User	Specify a role, user or user group for the PBR rule. 1. From the **User** drop-down list, select the AAA server to which the users and user groups belong. To specify a role, select **Role** from the **AAA Server** drop-down list. 2. Based on different types of AAA server, you can execute one or more actions: search a user/user group/role, or expand the user/user group list, and enter the name of the user/user group. 3. After selecting users/user groups/roles, click → to add them to the right pane. 4. After adding the desired objects, click the blank area in this dialog box

Option	Description
	to complete the user configuration.
Destination	
Address	Specify the destination addresses of the PBR rule. 1. Select an address type from the **Address** drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click to add the addresses to the right pane. 4. After adding the desired addresses, click the blank area in this dialog box to complete the destination address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click **Add** to create a new address entry. • The default address configuration is any. To restore the configuration to this default one, select the **any** check box.
Other	
Virtual Server	Specify a virtual server.
Host Book	Specify the name of the host book.
Service	Specify a service or service group. 1. From the **Service** drop-down list, select a type: Service or Service Group. 2. You can search the desired service/service group, or expand the service/service group list. 3. After selecting the desired services/service groups, click to add them to the right pane. 4. After adding the desired objects, click the blank area in this dialog box

Option	Description
	to complete the service configuration. You can also perform other operations: • To add a new service or service group, click **Add**. • The default service configuration is any. To restore the configuration to this default one, select the **any** check box.
Application	Specify an application/application group/application filter. 1. From the **Application** drop-down list, you can search the desired application/application group/application filter, or expand the list of applications/application groups/application filters. 2. After selecting the desired applications/application groups/application filters, click → to add them to the right pane. 3. After adding the desired objects, click the blank area in this dialog box to complete the application configuration. To create a new application group or application filter, click **New AppGroup** or **New AppFilter**.
Schedule	Specify a schedule when the PBR rule will take effect. Select a desired schedule from the **Schedule** drop-down list. To create a new schedule, click **New Schedule**.
Record log	Select the **Enable** check box to enable the logging function for PBR rules.

In the Next-hop tab, configure the following.

Option	Description
Set Next-hop	To specify the type of next hop, click **IP Address**, **Virtual Router in current Vsys**, **Interface**, or **Virtual Router in other Vsys**. • IP Address: Select the radio button to specify an IP address as the next hop. Type the IP address into the **IP Address** text box.

Option	Description
	• Virtual Router in current Vsys: Select the radio button to specify a virtual router in the current VSYS as the next hop. Select a virtual router from the **Next-Hop Virtual Router** drop-down list. • Interface: Select the radio button to specify an interface as the next hop. Select an interface from the **Interface** drop-down list.
Track Object	Select the track object from the drop-down list. See "Track Object" on Page 350.
Weight	Specify the weight for the next hop. If a PBR rule is configured with multiple next hops, system will distribute the traffic in proportion to the corresponding weight.
Add	Click to add the specified next hop. The added next hop entry will be displayed in the table below.
Delete	Select next-hop entries you want to delete from the next hop table, and click **Delete**.

Adjusting Priority of a PBR Rule

To adjust priority of a Policy-based Route rule, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.

2. **Select the rule you want to adjust priority from the list, click Priority. In the Adjust Priority dialog box, configure the following.**

Option	Description
Top	Click this option button to move the PBR rule to the top.
Bottom	Click this option button to move the PBR rule to the bottom.
Before ID	Click this option button and type the ID into the box to move the PBR rule to the position before the ID.
After ID	Click this option button and type the ID into the box to move the PBR rule to the position after the ID.

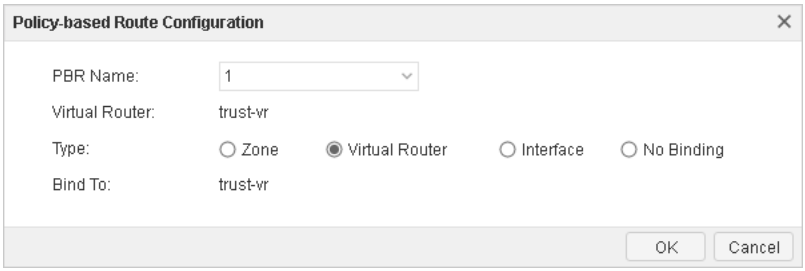
Note: Each PBR rule is labeled with a unique ID. When traffic flows into a Hillstone device, the device will query for PBR rules by turn, and process the traffic according to the first matched rule. However, the PBR rule ID is not related to the matching sequence during the query. You can move a PBR rule's location up or down at your own choice to adjust the matching sequence accordingly, i.e., the rule can be put at the top or bottom of the list, or before or after an ID or a name.

Applying a Policy-based Route

You can apply a policy-based route by binding it to an interface, virtual router or zone.

To apply a policy-based route, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.
2. From the **Virtual Router** drop-down list, select a virtual router for the new route.
3. **Click Bind to. In the Policy-based Route Configuration dialog box, enter values.**



Option	Description
PBR Name	Select a route from the **PBR Name** drop-down list.
Virtual Router	From the **Virtual Router** drop-down list, select a virtual router for the new route. The default value is "trust-vr".
Type	Specify the object type that the policy-based route binds to. You can select **Zone**, **Virtual Router**, **Interface** or **No Binding**. • Zone: Click this option button and select a zone from the **Bind To** drop-down list. • Virtual Router: Click this radio button, and the virtual router that the policy-based route binds to will be displayed below. • Interface: Click this option button and select an interface from the **Bind To** drop-down list. • No Binding: This policy-based route is no binding.

4. Click **OK**. The new route entry will be displayed in the policy-based route list.

DNS Redirect

System supports the DNS redirect function, which redirects the DNS requests to a specified DNS server. For more information about specifying IP addresses of the DNS server, see Configuring a DNS Server. Currently, the DNS redirect function is mainly used to redirect the video traffic for load balancing. With the policy-based route working together, system can redirect the Web video traffic to different links, improving the user experience.

To enable the DNS redirect function, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.

2. Click **Enable DNS Redirect**.

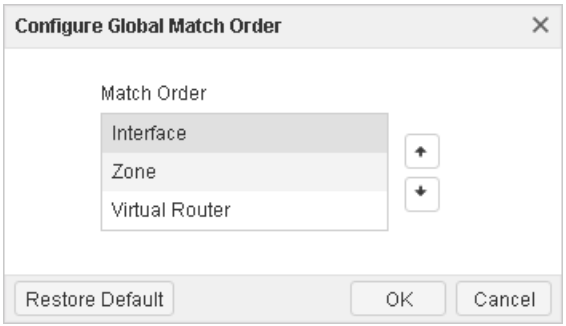
Configuring the Global Match Order

By default, if the PRB rule is bound to both an interface, VRouter and the security zone the interface belongs to, the traffic matching sequence will be: Interface > Zone > VRouter. You can configure the global match order of PBR.

To configure the global match order, take the following steps:

1. Select **Network** > **Routing** > **Policy-based Routing**.

2. Click **Configure Global Match Order**, and the Configure Global Match Order dialog box will appear.



3. Select the items that need to be adjusted, and click  or  .

4. To restore the default matching sequence, click **Restore Default**.

5. Click **OK**. The new route entry will be displayed in the policy-based route list.

RIP

RIP, Routing Information Protocol, is an internal gateway routing protocol that is designed to exchange routing information between routers. Currently, devices support both RIP versions, i.e., RIP-1 and RIP-2. RIP configuration includes basic options, redistribute, Passive IF, neighbor, network and distance. You will also need to configure RIP parameters for different interfaces, including RIP version, split horizon, and authentication mode.

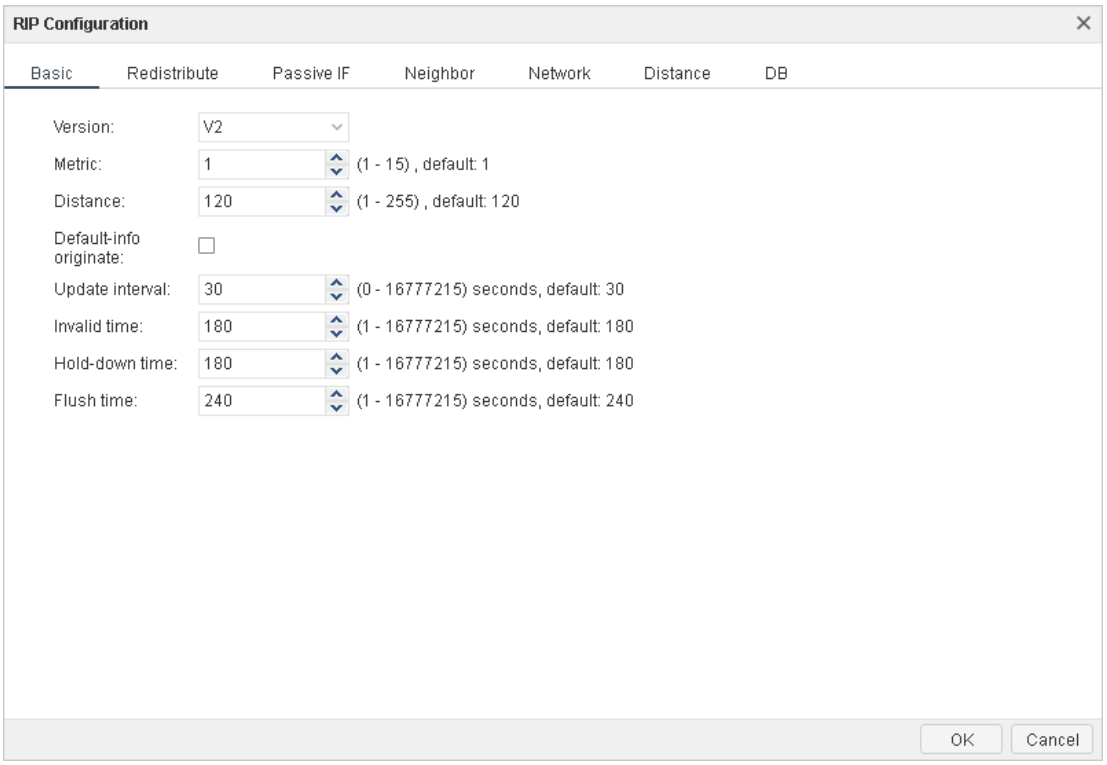
Creating RIP

To create RIP, take the following steps:

1. Select **Network** > **Routing** > **RIP**.

2. From the **Virtual Router** drop-down list, select a virtual router for the new route.

3. Click **New**, and the RIP Configuration dialog box will appear.



In the Basic tab, configure the following.

Option	Description
Version	Specify a RIP version. Hillstone devices support RIP-1 and RIP-2. RIP-1 transmits packets by broadcasting, while RIP-2 transmits packet by multicasting. Select a version from the drop-down list. The default version is RIP-2.
Metric	Specify a default metric. The value range is 1 to 15. If no value is specified, the value of 1 will be used. RIP measures the distance to the destination network by hops. This distance is known as metric. The metric from a router to a directly connected network is 1, increment is 1 for every additional router between them. The max metric is 15, and the network with metric larger than 15 is not reachable. The default metric will take effect when the route

Option	Description
	is redistributed.
Distance	Specify a default distance. The value range is 1 to 255. If no value is specified, the value of 120 will be used.
Default-info originate	Specify if the default route will be redistributed to other routers with RIP enabled. By default RIP will not redistribute the default route. Select the check box to redistribute the default route.
Update interval	Specify an interval in which all RIP routes will be sent to all the neighbors. The value range is 0 to 16777215 seconds. The default value is 30.
Invalid time	If a route has not been updated for the invalid time, its metric will be set to 16, indicating an unreachable route. The value range is 1 to 16777215 seconds. The default value is 180.
Holddown time	If the metric becomes larger (e.g., from 2 to 4) after a route has been updated, the route will be assigned with a holddown time. During the holddown time, the route will not accept any update. The value range is 1 to 16777215 seconds. The default value is 180.
Flush time	System will keep on sending the unreachable routes (metric set to 16) to other routers during the flush time. If the route still has not been updated after the end of flush time, it will be deleted from the RIP information database. The value range is 1 to 16777215 seconds. The default value is 240.

In the Redistribute tab, configure the following.

Option	Description
Protocol	Select a protocol type for the route from the **Protocol** drop-down list. The type can be Connected, Static, OSPF or BGP.
Metric	Type the metric for the route into the **Metric** box. If no value is specified, system will use the default metric value.
Add	Click **Add** to add the Redistribute route entry. All the entries that have been added will be displayed in the Redistribute Route list below.
Delete	Repeat the above steps to add more Redistribute route entries. To delete a

Option	Description
	Redistribute route entry, select the entry you want to delete from the list, and click **Delete**.

In the Passive IF tab, configure the following.

Option	Description
Interface	Select a passive interface from the **Interface** drop-down list.
Add	Click **Add** to add the passive interface. All the interfaces that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more Passive IFs. To delete a Passive IF, select the entry you want to delete from the list, and click **Delete**.

In the Neighbor tab, configure the following.

Option	Description
Neighbor IP	Type the neighbor IP into the **Neighbor IP** box.
Add	Click **Add** to add the neighbor IP. All the neighbor IPs that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more neighbor IPs. To delete a neighbor IP, select the entry you want to delete from the list, and click **Delete**.

In the Network tab, configure the following.

Option	Description
Network (IP/net-mask)	Type the IP address and netmask into the **Network (IP/netmask)** box.
Add	Click **Add** to add the network. All the networks that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more networks. To delete a network, select the entry you want to delete from the list, and click **Delete**.

In the Distance tab, configure the following.

Option	Description
Distance	Type the distance into the **Distance** box. The priority of the specified distance is higher than the default distance.
Network (IP/netmask)	Type the IP prefix and netmask into the **Network (IP/netmask)** box.
Add	Click **Add** to add the distance. All the distances that have been added will be displayed in the list below.
Delete	Repeat the above steps to add more distances. To delete a distance, select the entry you want to delete from the list, and click **Delete**.

In the DB tab, view the database of the RIP route.

All the route entries that can reach target network are stored in the database.

4. Click **OK**. The new route entry will be displayed in the RIP route list.

Note: Configuration for RIP on Hillstone device's interfaces includes: RIP version, split horizon and authentication mode. For more information on how to configure RIP on an interface, see "Configuring an Interface" on Page 224.

OSPF

OSPF, the abbreviation for Open Shortest Path First, is an internal gateway protocol based on link state developed by IETF. The current version of OSPF is version 2 (RFC2328). OSPF is applicable to networks of any size. Its quick convergence feature can send update message immediately after the network topology has changed, and its algorithm assures it will not generate routing loops. OSFP also have the following characteristics:

• Area division: divides the network of autonomous system into areas to facilitate management, thereby reducing the protocol's CPU and memory utilization, and improving performance.

• Classless routing: allows the use of variable length subnet mask.

• ECMP: improves the utilization of multiple routes.

• Multicasting: reduces the impact on non-OSPF devices.

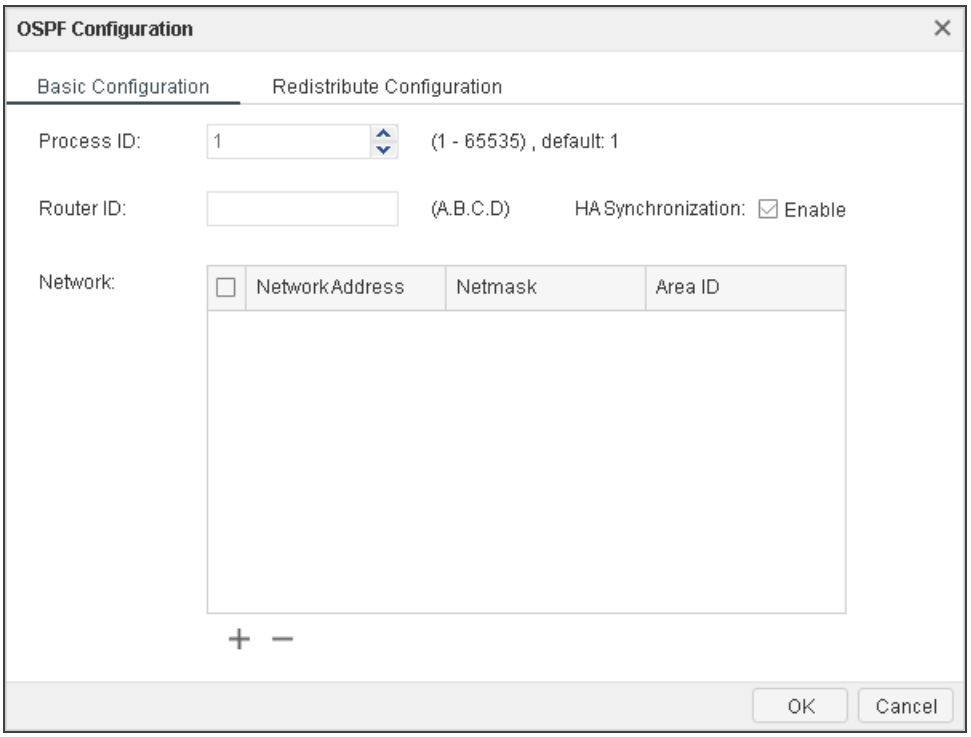
• Verification: interface-based packet verification ensures the security of the routing calculation.

Note: Autonomous system is a router and network group under the control of a management institution. All routers within an autonomous system must run the same routing protocol.

Creating OSPF

To create OSPF, take the following steps:

1. Select **Network** > **Routing** > **OSPF**.
2. From the **Virtual Router** drop-down list, select a virtual router for the new route.
3. Click **New**, and the OSPF Configuration dialog box will appear.



In the Basic tab, configure the following.

Option	Description
Process ID	Enter the OSPF process ID. The default value is 1. The value ranges from 1 to 65535. Each OSPF process is individual, and has its own link state database and the related OSPF routing table. Each VRouter supports up to 4 OSPF processes and multiple OSPF processes maintain a routing table together. When specifying the OSPF process ID, note the following matters: • When running multiple OSPF processes in a VRouter, the network advertised in interfaces in each OSPF process cannot be same. • When route entries with the same prefix exist in multiple OSPF processes, system will compare the administrative distance of each route entry and the route entry with the lower administrative distance will be added to the VRouter's routing table. If their AD is the same, the route entry that was first discovered will be added to the routing table. • If the OSPF route entries are redistributed to other routing protocols, the routing information of process 1 will be redistributed by default. If this process does not exist, the routing information of OSPF will not be redistributed.
Router ID	Enter the Router ID used by OSPF protocol. Each router running OSPF protocol should be labeled with a Router ID. The Router ID is the unique identifier of an individual router in the whole OSPF domain, represented in the form of an IP address.
Network	Configure the network interface that enables OSPF and add the network to the specified area. Click "+", and enter the network address, network mask and area ID. • Network Address: Enter the IP address of network interface that enables OSPF protocol. • Netmask: Enter the mask of IP address.

Option	Description
	• Area ID: Enter the area ID the network will be added to, in form of a 32-bit digital number, or an IP address.

In the Redistribute tab, configure the following.

Option	Description
Static	Select the **Enable** check box to introduce the static route protocol into the OSPF route and redistribute.
Connected	Select the **Enable** check box to introduce the connected route protocol into the OSPF route and redistribute.
RIP	Select the **Enable** check box to introduce the RIP route protocol into the OSPF route and redistribute.
OSPF	Select the **Enable** check box and specify the process ID to introduce other OSPF route protocols into the OSPF route and redistribute.
ISIS	Select the **Enable** check box to introduce the ISIS route protocol into the OSPF route and redistribute.
BGP	Select the **Enable** check box to introduce the BGP route protocol into the OSPF route and redistribute.

4. Click **OK**. The new OSPF process will be displayed in the OSPF route list.

Note: Configuration for OSPF on Hillstone device's interfaces includes: interface timer, priority, network type and link cost. For more information on how to configure OSPF on an interface, see "Configuring an Interface" on Page 224.

Viewing the Neighbor Information

To view the neighbor information, take the following steps:

1. Select **Network** > **Routing** > **OSPF**.

2. Select "+" in front of a process ID, and the neighbor information will be displayed in the list below.

    - Neighbor Router ID: Shows the router ID of OSPF neighbors.
    - Priority: Shows the router priority. The router priority is used to determine which router will act as the designated router. The designated router will receive the link information of all the other routers in the network, and broadcast the received link information.
    - Neighbor State: Shows the OSPF neighbor state. The OSPF neighbor state includes 8 types: Down, Attempt, Init, 2-Way, Exstart, Exchange, Loading and Full. The Full state includes Full/DR and Full/BDR.
    - Timeout: Shows the neighbor timeout, which is the difference between dead time and hello transmission interval. The unit is second. If the OSPF doesn't receive the Hello packets from neighbor, the neighborship cannot be established continually.
    - Neighbor IP: Shows the IP address of neighbor router.
    - Local Interface: Shows the interface sends the Hello packets to the neighbor router.

Chapter 10 Object

This chapter describes the concept and configuration of objects that will be referenced by other modules in system, including:

- "Address" on Page 319: Contains address information, and can be used by multiple modules, such as NAT rules.
- "Service Book" on Page 323: Contains service information, and can be used by multiple modules, such as NAT rules.
- "Host Book" on Page 328: A collection of one domain name or several domain names, and can be used by policy-based route rules.
- "Schedule" on Page 329: Specifies a time range or period. The functions (such as connections between the PPPoE interface and Internet) that use the schedule will take effect in the time range or period specified by the schedule.
- "AAA Server" on Page 332: Describes how to configure an AAA server.
- "User" on Page 338: Contains information about the functions and services provided by a Hillstone device, and users authenticated and managed by the device.
- "Role" on Page 346: Contains role information that associates users to privileges. In function configurations, different roles are assigned with different services. Therefore, the mapped users can gain the corresponding services as well.
- "Track Object" on Page 350: Tracks if the specified object (IP address or host) is reachable or if the specified interface is connected. This function is designed to track HA and interfaces.

Address

IP address is an important element for the configurations of multiple modules, such as policy rules, NAT rules and session limit rules. Therefore, system uses an address book to facilitate IP address reference and flexible configuration. You can specify a name for an IP range, and only the name is referenced during configuration. The address book is the database in system that is used to store the mappings between IP ranges and the corresponding names. The mapping entry between an IP address and its name in the address book is known as an address entry.

System provides a global address book. You need to specify an address entry for the global address book. When specifying the address entry, you can replace the IP range with a DNS name. Interfaces of the configured IPs will be used as address

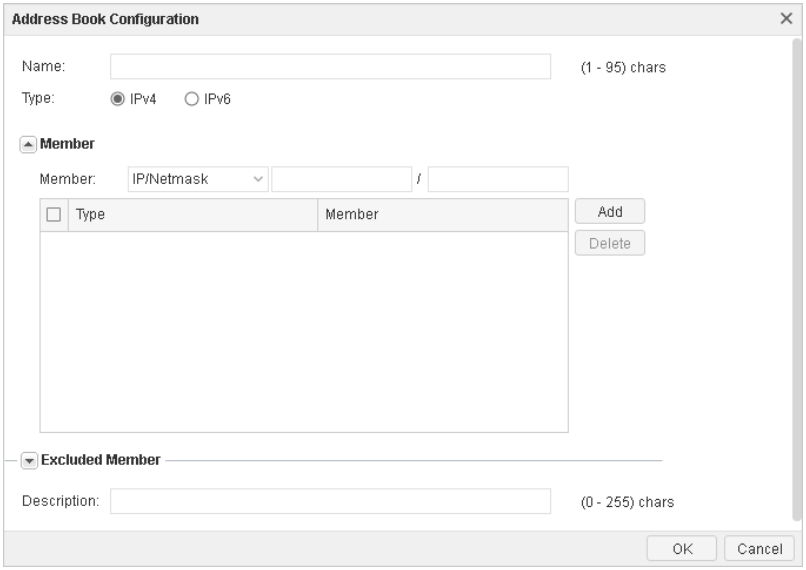
entries and added to the address book automatically. You can use them for NAT conveniently. Furthermore, an address entry also has the following features:

- All address books contain two default address entries named **Any** and **private_network**. The IP address of **Any** is 0.0.0.0/0, which is any IP address. **Any** can neither be edited nor deleted. The IP addresses of **private_network** are 10.0.0.0/8, 172.16.0.0/12, and 192.168.0.0/16, covering all private network addresses. The **private_network** can be edited and deleted.
- One address entry can contain another address entry in the address book.
- If the IP range of an address entry changes, ADC will update other modules that reference the address entry automatically.

Creating an Address Book

To create an address book, take the following steps:

1. Click **Object** > **Address Book**.
2. Click **New**.



In Address Book Configuration dialog box, enter the address entry configuration.

Basic	
Name	Type the address entry name into the **Name** box.

Basic	
Member	
Member	Specify the address book member. Select the IP/Netmask, IP Range, Hostname, Address Book, IP/Wildcard or Country/Region as needed, and enter or select the corresponding configuration in the text box. • The Country/Region member is only supported in the address entry of the IPv4 type. • Only the security policy and the policy-based route support the address entry with the Country/Region member added. • The address entry with the Country/Region member added does not support the **Excluded Member** settings.
Add	Click **Add** to add the configured member to the list below. If needed, repeat the above steps to add more members.
Delete	Delete the selected address entry from the list.
Excluded Member	
Member	Specify the excluded member. Select the **IP/Netmask** or **IP Range** from the drop-down list as needed, and type the corresponding configuration into the text box. **Note:** Excluded members' address range need to be in the address range of the members, otherwise the configuration cannot be completed.
Add	Click **Add** to add the configured excluded member to the list below. If needed, repeat the above steps to add more excluded members.
Delete	Delete the selected excluded member entry from the list

3. Click **OK**. The new address book will be displayed in the address book list.

Viewing Details

To view the details of an address entry, including the name, member, description and reference, take the following steps:

1. Click **Object** > **Address Book**.

2. **Click an address book entry in the member list, and view the details below the list.**

Details	
Name	View the name of the address book.
Type	View the type of the IP address.
Member	View address entry members in the address book.
Excluded Member	View excluded address entry members in the address book.
Description	View the description of the address book.
Referenced by	
Address	Information on other address books that reference the address book.
SNAT	Information on the source NAT rules that reference the address book.
PBR	Information on the PBR rules that reference the address book.

Service Book

Service is an information stream designed with protocol standards. Service has some specific distinguishing features, like corresponding protocol, port number, etc. For example, the FTP service uses TCP protocol, and its port number is 21. Service is an essential element for the configuration of multiple ADC modules including NAT rules etc.

System ships with multiple predefined services/service groups. Besides, you can also customize user-defined services/service groups as needed. All these service/service groups are stored in and managed by ADC service book.

Predefined Service/Service Group

System ships with multiple predefined services, and identifies the corresponding application types based on the service ports. The supported predefined services may vary from different Hillstone device models. Predefined service groups contain related predefined services to facilitate user configuration.

User-defined Service

Except for the above predefined services, you can also create your own user-defined services easily. The parameters that will be specified for the user-defined service entries include:

- Name
- Protocol type
  - The source and destination port for TCP or UDP service, and the type and code value for ICMP service.

User-defined Service Group

You can organize some services together to form a service group, and apply the service group to ADC policies directly to facilitate management. The service group has the following features:

- Each service of the service book can be used by one or more service groups.
- A service group can contain both predefined services and user-defined services.
- A service group can contain another service group. The service group of ADC supports up to 8 layers of nests.

The service group also has the following limitations:

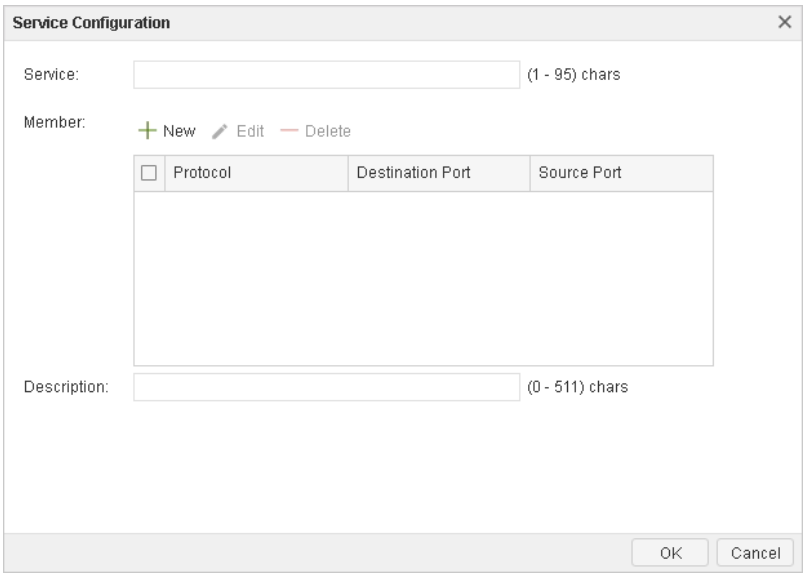
- The name of a service and service group should not be identical.
  - A service group being used by any policy cannot be deleted. To delete such a service group, you must first end its relationship with the other modules.
  - If a user-defined service is deleted from a service group, the service will also be deleted from all of the service groups using it.

Configuring a Service Book

This section describes how to configure a user-defined service and service group.

Configuring a User-defined Service

1. Select **Object** > **Service Book** > **Service**.
2. Click **New**.



In the Service Configuration dialog box, configure the following options.

Option	Description
Service	Type the name for the user-defined service into the text box.

<table>
<tr><th>Option</th><th>Description</th></tr>
<tr><td>Member</td><td>Specify a protocol type for the user-defined service. Click New, and the Service Member Configuration dialog box will appear. The available options include TCP, UDP, ICMP and Others. If needed, you can add multiple service items.

The parameters for the protocol types are described as follows:

<table>
<tr><td>TCP</td><td>Destination Port: Min - Specify the minimum port number of the specified service entry; Max - Specify the maximum port number of the specified service entry. The value range is 0 to 65535, but the destination port number cannot be a single "0".

Source Port: Min - Specify the minimum port number of the specified service entry; Max - Specify the maximum port number of the specified service entry. The value range is 0 to 65535.

Note: The minimum port number cannot exceed the maximum port number.</td></tr>
<tr><td>UDP</td><td>Destination Port: Min - Specify the minimum port number of the specified service entry; Max - Specify the maximum port number of the specified service entry. The value range is 0 to 65535, but the destination port number cannot be a single "0".

Source Port: Min - Specify the minimum port number of the specified service entry; Max - Specify the maximum port number of the specified service entry. The value range is 0 to 65535.

Note: The minimum port number cannot exceed the maximum port number.</td></tr>
<tr><td>ICMP</td><td>Type: Specify an ICMP type for the service entry.</td></tr>
</table>
</td></tr>
</table>

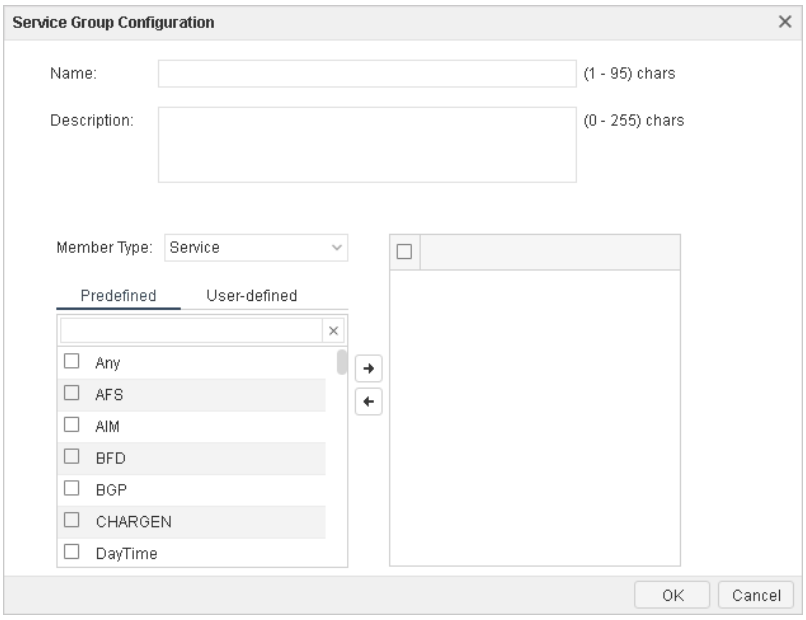
Option	Description	
		You can select 3 (Destination-Unreachable), 4 (Source Quench), 5 (Redirect), 8 (Echo), 11 (Time Exceeded), 12 (Parameter Problem), 13 (Timestamp) or 15 (Information) from the drop-down list. Min Code: Specify the minimum value for the ICMP code of the user-defined service. The value range is 0 to 5. Max Code: Specify the maximum value for the ICMP code of the user-defined service. The value range is 0 to 5. Note: The minimum port number cannot exceed the maximum port number.
	Others	Specify the protocol number for the service entry. The value range is 1 to 255.
Description	If needed, type the description for the user-defined service into the text box.	

3. Click **OK**. The new user-defined service will be displayed in the user-defined service list

Configuring a User-defined Service Group

1. Select **Object** > **Service Book** > **Service Group**.

2. Click **New**.



In the Service Group Configuration dialog box, configure the following options.

Option	Description
Name	Type the name for the user-defined service group into the text box.
Description	If needed, type the description for the user-defined service group into the text box.
Member Type	Specify the members of the service group, including user-defined services, user-defined service groups, predefined services or predefined service groups. Select a service or service group you need from the left pane, and click **Add** to add it to the right pane. You can add multiple members.

3. Click **OK**. The new service group will be displayed in the user-defined service group list.

Viewing Details

To view the details of a service entry, including the name, protocol, destination port and reference, take the following steps:

1. Click **Object** > **Service Book** > **Service**.

2. **Click a service entry in the member list, and view the details below the list.**

Details	
Description	View details of the service.
Referenced by	
Group	Information on the groups that reference the service.
SNAT	Information on the source NAT rules that reference the service.
PBR	Information on the PBR rules that reference the service.

Host Book

You can specify a name to be a collection of one domain name or several domain names, and reference this host book when configuring. Host book is the database to store the relationships of domain integrations and the specified names in system. The entry of the relationship of domain integrations and the specified name is called host entry.

Notes:

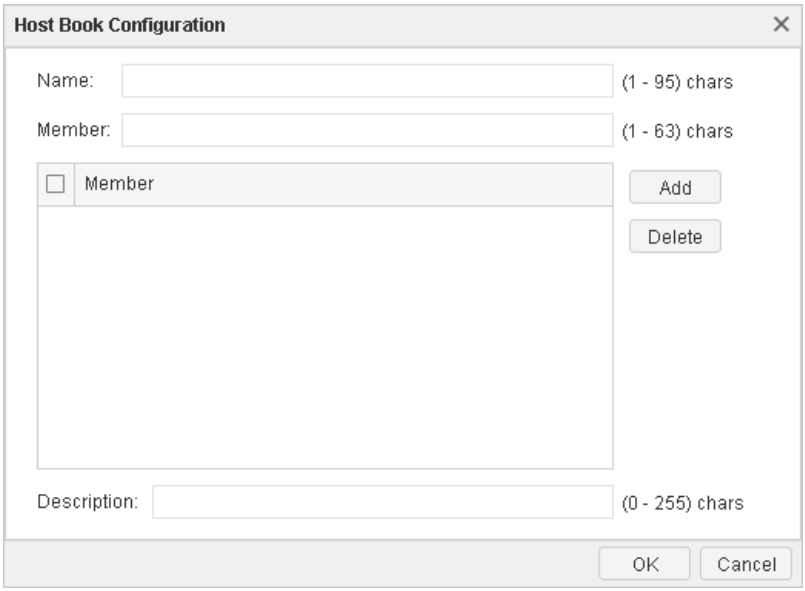
- The maximum number of host entries is one fourth of the maximum number of address entries.
- Up to one host entry can be configured for each PBR rule.

Creating a Host Book

To create a host book, take the following steps:

1. Select **Object** > **Host Book**.

2. Click **New**.



In the Host Book Configuration dialog box, configure the following options.

Option	Description
Name	Type a name for the host book.
Member	Specify the host entry member. Enter IP address or domain name in the **Member** text box and then click **Add**. The configured member will be added to the host entry member list below. If needed, you can add multiple host entries in the host book.
Description	Type the description of the host book.

3. Click **OK**. The new host book will be displayed in the host book list.

Schedule

System supports a schedule. This function allows a policy rule to take effect in a specified time and controls the duration of the connection between a PPPoE interface and the Internet. The schedule consists of a periodic schedule and an absolute

schedule. The periodic schedule specifies a time point or time range for periodic schedule entries, while the absolute schedule decides a time range in which the periodic schedule will take effect.

Periodic Schedule

Periodic schedule is the collection of periods specified by all of the schedule entries within the schedule. You can add up to 16 schedule entries to a periodic schedule. These entries can be divided into 3 types:

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

Absolute Schedule

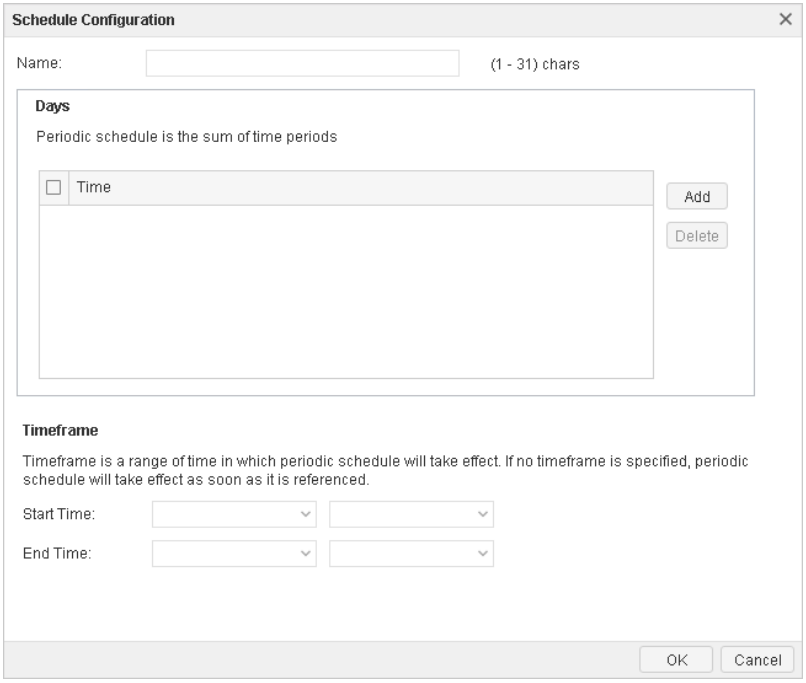
An absolute schedule is a time range in which a periodic schedule will take effect. If no absolute schedule is specified, the periodic schedule will take effect as soon as it is used by some module.

Creating a Schedule

To create a schedule, take the following steps:

1. Select **Object** > **Schedule**.

2. Click **New**.



In the Schedule Configuration dialog box, configure the following options.

Schedule Configuration	
Name	Specify a name for the new schedule.
Days	
Add	Add a periodic schedule entry. Type: Specify a type for the periodic schedule in Add Periodic Schedules section, including Daily, Days or Duration. • Daily - The specified time of every day. Click this radio button, and then in the Time section, select a start time and end time from the **Start Time** and **End Time** drop-down list respectively.

Schedule Configuration			
			• Days - The specified time of a specified day during a week. Click this radio button, and then select a day/days in the Days and Time section, and finally select a start time and end time from the **Start Time** and **End Time** drop-down list respectively. • Duration - A continuous period during a week. Click this radio button, and then in the Duration section select a start day/time and end day/time from the **Start Time** and **End Time** drop-down list respectively.
		Preview	If needed, Click **Preview** to preview the detail of the configured periodic schedule in the Preview section.
		OK	Save your settings, and the new periodic schedule will be displayed in the periodic schedule list.
Delete	Select the entry you want to delete from the periodic schedule list below, and click **Delete**.。		
Timeframe			
Start Time	Specify the start date and time of the absolute schedule.		
End Time	Specify the end date and time of the absolute schedule.		

3. Click **OK**. The new schedule will be displayed in the schedule list.

AAA Server

An AAA server is a server program that handles user requests to access computer resources, and for an enterprise, this server provides authentication, authorization, and accounting (AAA) services. The AAA server typically interacts with network access and gateway servers and with databases and directories containing user information.

Here in ADC system, authentication supports the following two types of AAA server:

- Local server: a local server is the firewall itself. The firewall stores user identity information and handles requests. A local server authentication is fast and cheap, but its storage space is limited by the firewall hardware size.
- External servers:
  - Radius Server

Configuring a Local AAA Server

1. Select **Object** > **AAA Server**.
2. Click **New** > **Local Server**.

   In the Local Server Configuration dialog box, configure the following.

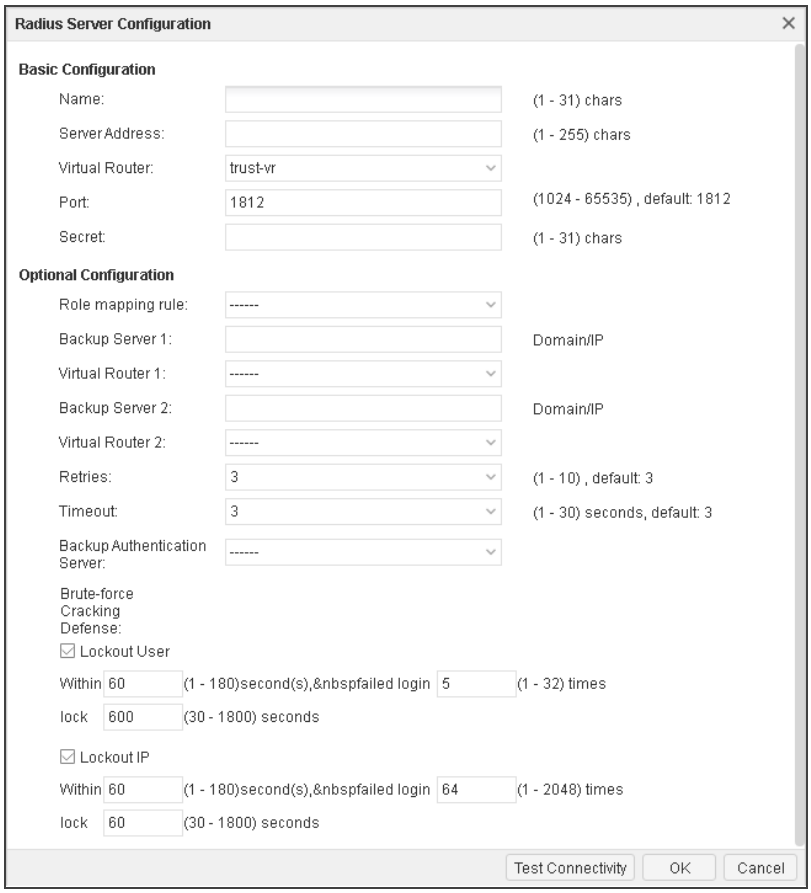
Option	Description
Name	Type the name for the new server into the text box.
Role mapping rule	To specify a role mapping rule for the server, select a mapping rule from the drop-down list. With this option selected, system will allocate a role for the users who have been authenticated to the server according to the specified role mapping rule.
Change Password	If needed, select the **Enable** check box. With this function enabled, system allows users to change their own passwords after the successful WebAuth or SCVPN authentication.
Backup Authentication Server	To configure a backup authentication server, select a server from the drop-down list. After configuring a backup authentication server for the local server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in system.

3. Click **OK**.

Configuring Radius Server

1. Select **Object** > **AAA Server**

2. Click **New** > **Radius Server**.



In the Radius Server Configuration dialog box, configure the following.

Basic Configuration	
Name	Specify a name for the Radius server.
Server Address	Specify an IP address or domain name for the Radius server.
Virtual Router	Specify a VR for the Radius server.
Port	Specify a port number for the Radius server. The value range is 1024 to 65535. The default value is 1812.
Secret	Specify a secret for the Radius server.

Basic Configuration	
Optional Configuration	
Role mapping rule	To specify a role mapping rule for the server, select a mapping rule from the drop-down list. With this option selected, system will allocate a role for the users who have been authenticated to the server according to the specified role mapping rule.
Backup Server 1/Backup Server 2	A Radius server for backup. The server and primary server are the backup for each other.
Virtual Router 1/Virtual Router 2	Specify a VR for the backup server.
Retries	Specify a retry time for the authentication packets sent to the AAA server. The value range is 1 to 10. The default value is 3.
Timeout	Specify a timeout for the server response. The value range is 1 to 30 seconds. The default value is 3.
Backup Authentication Server	Specify a backup authentication server. After configuring a backup authentication server for the Radius server, the backup authentication server will take over the authentication task when the primary server malfunctions or authentication fails on the primary server. The backup authentication server can be any existing local, Active-Directory, RADIUS or LDAP server defined in system.
Enable Accounting	Select the **Enable** check box to enable accounting for the Radius server, and then configure options in the sliding out area.

Server Address	Specify an IP address or domain name for the accounting server.
Virtual Router	Specify a VR for the accounting server.
Port	Specify a port number for the accounting server. The

Basic Configuration			
			value range is 1024 to 65535. The default value is 1813.
		Password	Specify a password for the accounting server.
		Confirm Password	Enter the password again to confirm.
		Backup Server 1/Backup Server 2	Specify an IP address or domain name for backup server 1 or backup server 2.
		Virtual Router 1/Virtual Router 2	Specify a VR for the backup server.

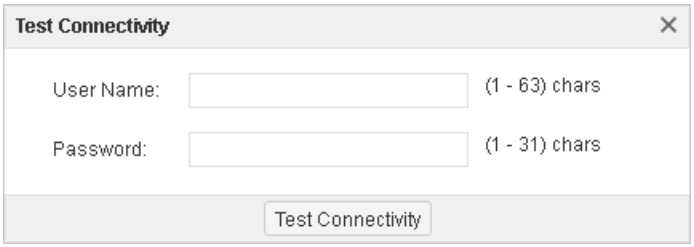
3. Click **OK**.

Connectivity Test

When AAA server parameters are configured, you can test if they are correct by testing server connectivity.

To test server connectivity, take the following steps:

1. Select **Object** > **AAA Server**, and click **New**.
2. Select your AAA server type, which can be Radius. The local server does not need the connectivity test.
3. After filling out the fields, click **Test Connectivity**.
4. For the Radius server, enter a username and password in the pop-up Test Connectivity dialog box.



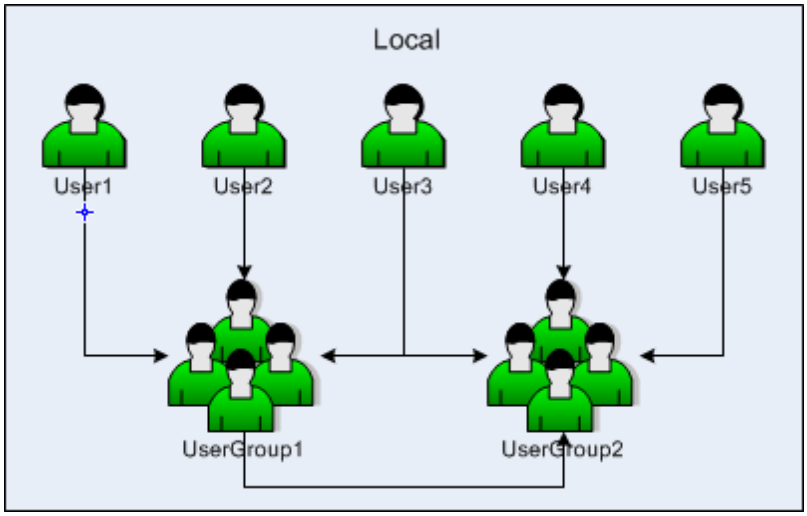
5. Click **Test Connectivity**. If "Test connectivity success" message appears, the AAA server settings are correct.

If there is an error message, here are the causes:

- Connect AAA server timeout: Wrong server address, port or virtual router.
- AAA server configuration error: Secret is wrong.
- Wrong name or password: Username or password for testing is wrong.

User

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



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

Configuring a Local User

This section describes how to configure a local user and user group.

Click the **Local Server** drop-down list in the upper left corner of the page to switch the local user's server.

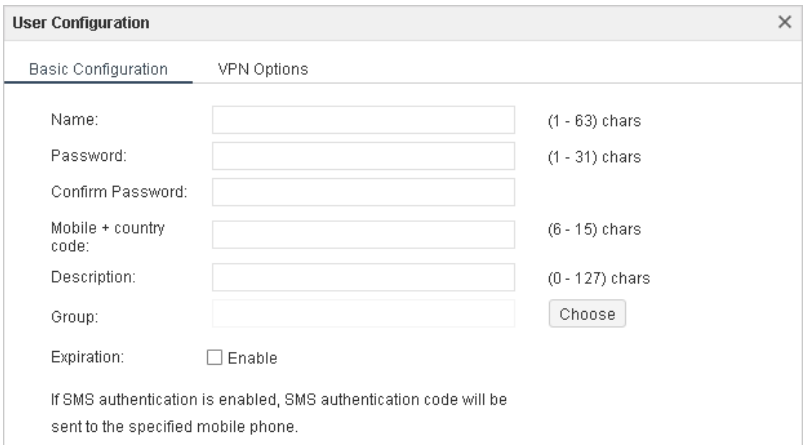
Red Expired, orange Will expire within a week and yellow Will expire within a month colors are used to mark the expired users, expired within a week, expired within a month in the list

Creating a Local User

To create a local user, take the following steps:

1. Select **Object** > **User** > **Local User**.

2. Click **New** > **User**, and the User Configuration dialog box will appear.



In the Basic Configuration tab, configure the following options.

Option	Description
Name	Specify a name for the user.
Password	Specify a password for the user.
Confirm password	Type the password again to confirm.
Mobile + country code	Specify the user's mobile number. When users log into the SCVPN client, system will send the verification code to the mobile number.
Description	If needed, type the description for the user.
Group	Add the user to a selected usergroup. Click **Choose**, and in the Choose User Group dialog box, select the usergroup you want from the Available list and click **Add**.
Expiration	Select the **Enable** check box to enable expiration for the user, and then specify a date and time. After expiration, the user cannot be authenticated,

Option	Description
	therefore cannot be used in system. By default expiration is not enabled.

In the VPN Options tab, configure network parameters for the PnPVPN client.

Option	Description
IKE ID	Specify an IKE ID type for dial-up VPN users. If FQDN, ASN1DN or KEY-ID is selected, type the ID's content into the text box below.
DHCP Start IP	Specify a start IP for the DHCP address pool.
DHCP End IP	Specify an end IP for the DHCP address pool.
DHCP Netmask	Specify a netmask for the DHCP address pool.
DHCP Gateway	Specify a gateway for the DHCP address pool. The IP address of the gateway corresponds to the IP address of PnPVPN client's Intranet interface and PC's gateway address. The PC's IP address is determined by the segment and netmask configured in the above DHCP address pool. Therefore, the gateway's address and DHCP address pool should be in the same segment.
DNS1	Specify an IP address for the DNS server. You can specify one primary DNS server (DNS1) and up to three alternative DNS servers.
DNS2	
DNS3	
DNS4	
WINS1	Specify an IP address for the WINS server. You can specify one primary WINS server (WINS1) and one alternative WINS server.
WINS2	
Tunnel IP 1	Specify an IP address for the master PnPVPN client's tunnel interface. Select the **Enable SNAT** check box to enable SNAT.
Tunnel IP 2	Specify an IP address for the backup PnPVPN client's tunnel interface.

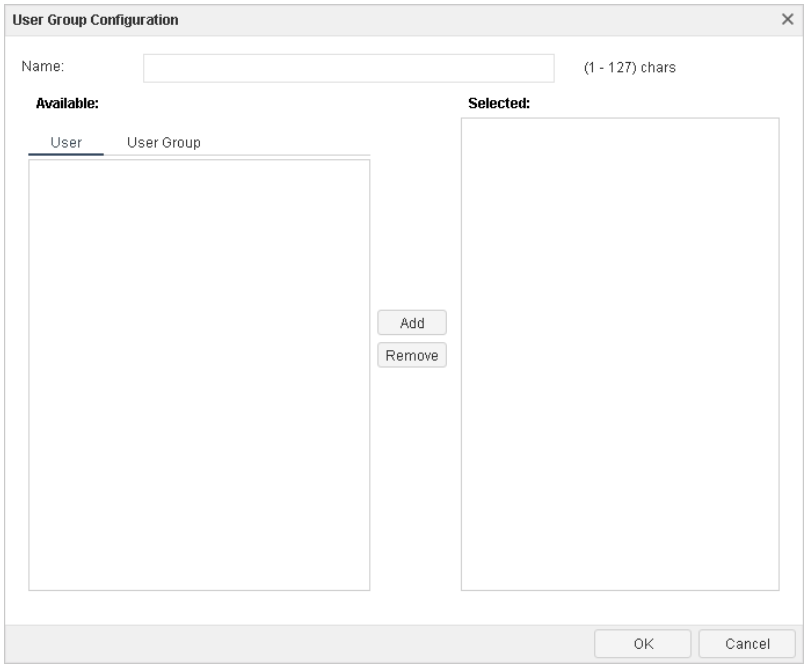
3. Click **OK**. The new user will be displayed in the user list.

Creating a User Group

To create a user group, take the following steps:

1. Select **Object** > **User** > **Local User**.

2. Click **New** > **User Group**.



In the User Group Configuration dialog box, configure the following options.

Option	Description
Name	Type the name of the user group into the **Name** box.
Add	Specify members for the user group. Expand User or User Group in the Available list, select a user or user group and click **Add** to add it to the Selected list on the right. One user group can contain multiple users or user groups, but system only supports up to 12 layers of nested user groups and does not support the loopback nest. Therefore, a user group should not nest the upper-layer user group it belongs to.
Remove	Remove the specified user or user group. To remove a specified user or user group, select it in the Selected list and then click **Remove**.

3. Click **OK**.

Import User Password List

To import a user password list to system, take the following steps:

1. Select **Object** > **User** > **Local User**.
2. Click **Import User Password List**, and the Import User Password List dialog box will appear.
3. Click **Browse** to select the file name needed to be imported.
4. Click **OK** to finish import.

Export User Password List

To export a user password list from system to local, take the following steps:

1. Select **Object** > **User** > **Local User**.
2. Click **Export User Password List**, and an export progress bar will pop up.
3. After the export is completed, a downloaded file will be generated locally.

Note:

- The user password in the import/export file is in encrypted text.
- Please try to keep the import file format consistent with the export file.
- When importing, if the same user name exists under the same server, the original user password will be overwritten.

Configuring a LDAP User

This section describes how to configure a LDAP user. You can click the **LDAP Server** drop-down list in the upper left corner of the page to switch the LDAP user's server.

Synchronizing Users

To synchronize users in a LDAP server to the device, first you need to configure a LDAP server (refer to "AAA Server" on Page 332). To synchronize users, take the following steps:

1. Select **Object** > **User** > **LDAP User**.
2. Select a server from the **LDAP Server** drop-down list, and click **Sync Users**.

Note: By default, after creating a LDAP server, system will synchronize the users of the LDAP server automatically, and then continue to synchronize every 30 minutes.

Configuring an Active Directory User

This section describes how to configure an active directory (AD) user. You can click the **Active Directory** drop-down list in the upper left corner of the page to switch the AD user's server.

Synchronizing Users

To synchronize users in an AD server to the device, first you need to configure an AD server (refer to "AAA Server" on Page 332). To synchronize users, take the following steps:

1. Select **Object** > **User** > **AD User**.
2. Select an AD server from the **Active Directory** drop-down list, and click **Sync Users**.

Note: By default, after creating an AD server, system will synchronize the users of the AD server automatically, and then continue to synchronize every 30 minutes.

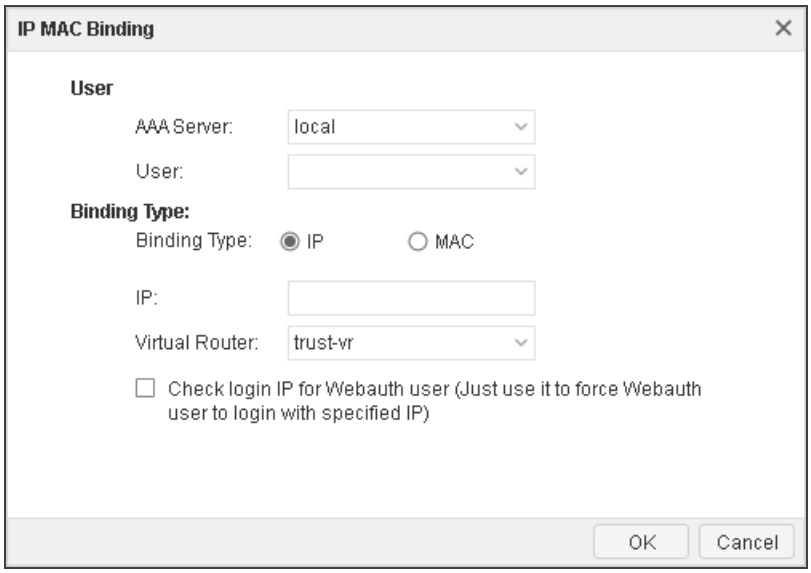
Configuring a IP-User Binding

This section describes how to configure the IP-user binding.

Adding User Binding

To bind an IP or MAC address to a user, take the following steps:

1. Select **Object** > **User** > **IP-User Binding**.
2. Click **Add User Binding**.



In the IP MAC Binding dialog box, configure the following options..

User	
AAA Server	Select an AAA server from the drop-down list.
User	Select a user for the binding from the drop-down list, and click **OK**. To clear the selected user, click **Clear**.
Binding Type	
Binding Type	By specifying the binding type, you can bind the user to an IP address or MAC address. • IP - If IP is selected, type the IP address into the **IP** text box. And select a VR from the **Virtual Router** drop-down list. Select the **Check login IP for Webauth User** check box to apply the IP-User mapping

User	
	only to the check for IP-user mapping during Web authentication if needed. • MAC - If MAC is selected, type the MAC address into the **MAC** text box. And select a VR from the **Virtual Router** drop-down list.

3. Click **OK**.

Import Binding

To import a user binding list to system, take the following steps:

1. Select **Object** > **User** > **IP-User Binding**.
2. Click **Import**, and the Import User Binding List dialog box will appear.
3. Click **Browse** to select the file name needed to be imported.
4. Click **OK** to finish import.

Export Binding

To export a user binding list from system to local, take the following steps:

1. Select **Object** > **User** > **IP-User Binding**.
2. Select a user category you want to export (includes local User, LDAP User, AD User and Export All) from the **Export** drop-down list, and an export progress bar will pop up.
3. After the export is completed, a downloaded file will be generated locally.

Role

Roles are designed with certain privileges. For example, a specific role can gain access to some specified network resources, or make exclusive use of some bandwidth. In ADC, users and privileges are not directly associated. Instead, they are associated by roles.

The mappings between roles and users are defined by role mapping rules. In function configurations, different roles are assigned with different services. Therefore, the mapped users can gain the corresponding services as well.

System supports role combination, i.e., the AND, NOT or OR operation on roles. If a role is used by different modules, the user will be mapped to the result role generated by the specified operation.

System supports the following role-based functions:

- Role-based policy rules: Implements access control for users of different types.
- Role-based QoS: Implements QoS for users of different types.
- Role-based statistics: Collects statistics on bandwidth, sessions and new sessions for users of different types.
- Role-based session limits: Implements session limits for specific users.
- Role-based PBR: Implements routing for users of different types.

Configuring a Role

Creating a Role

To create a role, take the following steps:

1. Select **Object** > **Role** > **Role**.
2. Click **New**.

Option	Description
Role Name	Type the role name into the **Role Name** box.
Description	Type the description for the role into the **Description** box.

3. Click **OK**. The new role will be displayed in the role list.

Mapping to a Role Mapping Rule

You can map the role to user, user group, CN or OU through this function or Creating a Role Mapping Rule. After Creating a Role Mapping Rule, you can click Mapping To to map the selected role again.

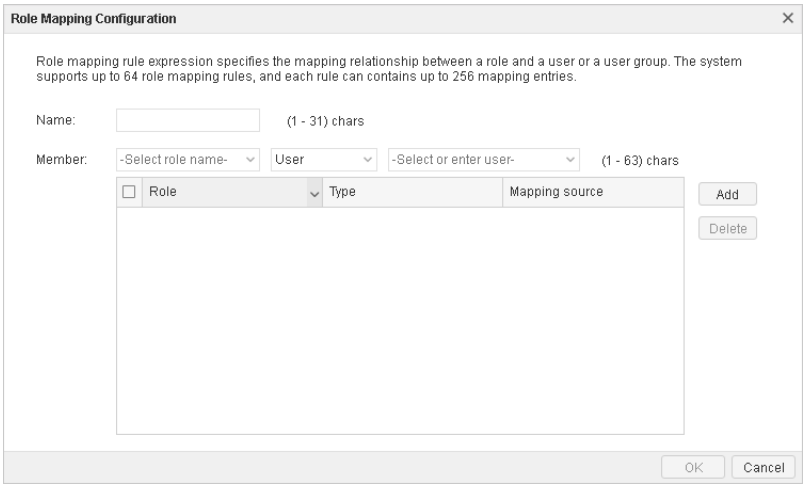
To map the selected role again, take the following steps:

1. Select **Object** > **Role** > **Role**.
2. Select the role needs to be mapped, and click **Mapping To**. A dialog box will appear.
3. In the Mapping name section, select a created mapping rule name from the first drop-down list (For detailed information of creating a role mapping role, see Creating a Role Mapping Rule.), and then select a user, user group, certificate name (the CN field of USB Key certificate), organization unit (the OU field of USB Key certificate) or any from the second drop-down list. If User, User group, CN or OU is selected, also select or enter the corresponding user name, user group name, CN or OU into the box behind.
4. Click **Add** to add the mapping to the role mapping list. If needed, repeat Step 3 and Step 4 to add more mappings.
5. To delete a role mapping, select the role mapping you want to delete from the mapping list, and click **Delete**.
6. Click **OK**. The new role mapping rule will be displayed both in the role list and role mapping list.

Creating a Role Mapping Rule

To create a role mapping rule, take the following steps:

1. Select **Object** > **Role** > **Role Mapping**.
2. Click **New**, and the Role Mapping Configuration dialog box will appear.



3. Type the name for the rule mapping rule into the **Name** box.

4. In the Member section, select a role name from the first drop-down list, and then select a user, user group, certificate name (the CN field of USB Key certificate) or organization unit (the OU field of USB Key certificate) from the second drop-down list. If User, User group, CN or OU is selected, also select or enter the corresponding user name, user group name, CN or OU into the box behind.

5. Click **Add** to add the mapping to the role mapping list. If needed, repeat Step 3 and Step 4 to add more mappings.

6. To delete a role mapping, select the role mapping you want to delete from the mapping list, and click **Delete**.

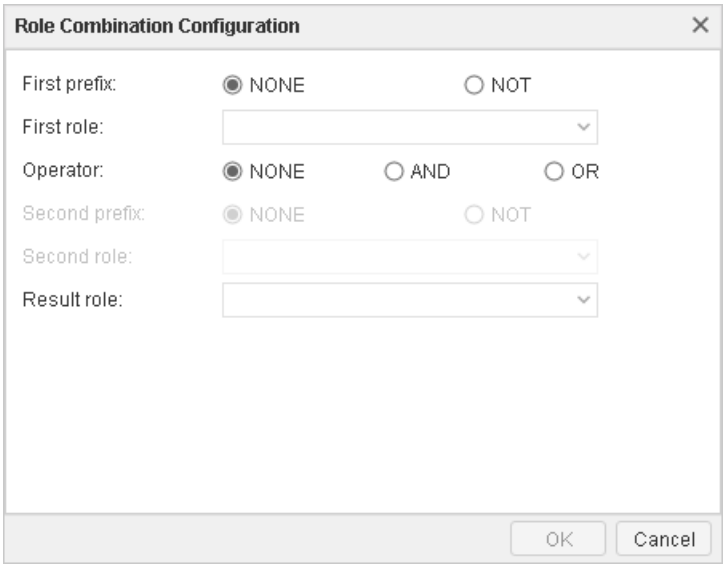
7. Click **OK**. The new role mapping rule will be displayed both in the role list and role mapping list.

Creating a Role Combination

To create a role combination, take the following steps:

1. Select **Object** > **Role** > **Role Combination**.

2. Click **New**.



In the Role Configuration dialog box, configure the following options.

Option	Description
First Prefix	Select the **NONE** or **NOT** radio button to specify a prefix for the first role in the role regular expression.
First Role	Select a role name from the **First Role** drop-down list to specify a name for the first role in the role regular expression.
Operator	Select the **NONE**, **AND** or **OR** radio button to specify an operator for the role regular expression.
Second Prefix	After selecting **AND** or **OR** for the Operator, you can select the **NONE** or **NOT** radio button to specify a prefix for the second role in the role regular expression.
Second Role	After selecting **AND** or **OR** for the Operator, you can select a role name from the **Second Role** drop-down list to specify a name for the second role in the role regular expression.
Result Role	Select a role name from the **Result Role** drop-down list to specify a name

Option	Description
	for the result role in the role regular expression.

3. Click **OK**.

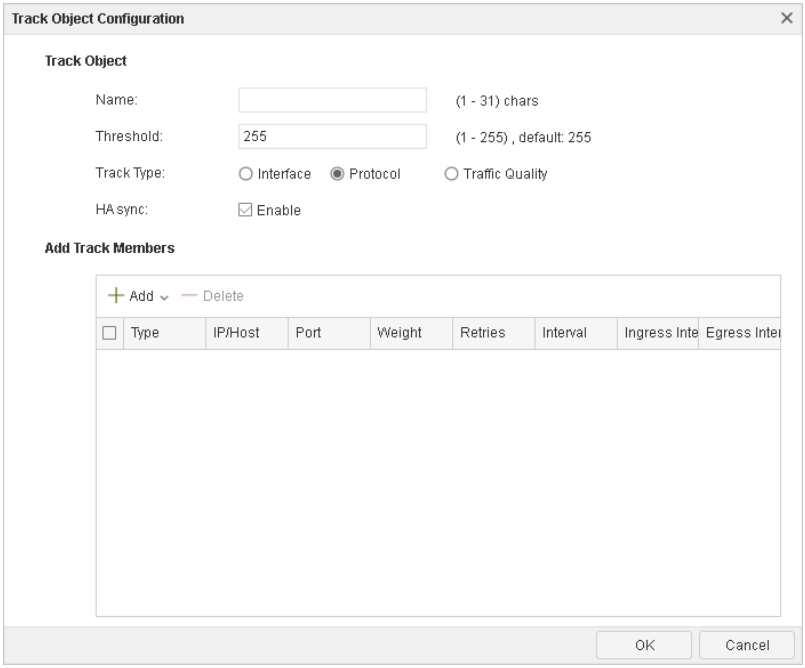
Track Object

The devices provide the track object to track if the specified object (IP address or host) is reachable or if the specified interface is connected. This function is designed to track HA and interfaces.

Creating a Track Object

To create a track object, take the following steps:

1. Select **Object** > **Track Object**.
2. Click **New**.



In the Track Object Configuration dialog box, configure the following options.

Option	Description
Name	Specify a name for the new track object.
Threshold	Type the threshold for the track object into the text box.

Track Type	Select a track object type, including Interface, Protocol or Traffic Quality. One track object can only be configured with one type.
	Select **Interface** radio button:
	• Click **Add** in Add Track Members section and then configure the following options in the Add Interface Member dialog box:
	  • Interface - Select a tracked interface from the drop-down list.
	  • Weight - Specify a weight for the interface, i.e. the weight for overall failure of the whole track object if this track entry fails.
	Select **Protocol** radio button:
	• Click **Add**, select a packet type from the drop-down list, and then configure the following options in the Add HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP Member dialog box:
	  • IP/Host - Specify an IP address or host name for the track object when the track is implemented by HTTP/ICMP/ICMPv6/TCP packets.
	  IP - Specify an IP address for the track object when the track is implemented by ARP/NDP packets.
	  DNS - Specify an IP address for the track object when the track is implemented by DNS packets.
	  • Weight - Specify how important this track failure is to the judgment of track object failure. The value range is 1 to 255. The default value is 255.
	  • Retries: Specify a retry threshold. If no response packet is

Option	Description
	received after the specified times of retries, system will determine this track entry fails, i.e., the track entry is unreachable. The value range is 1 to 255. The default value is 3. • Interval - Specify an interval for sending HTTP/ICMP/ICMPv6/ARP/DNS/TCP packets. The value range is 1 to 255 seconds. The default value is 3. • Egress Interface - Specify an egress interface from which HTTP/ICMP/ICMPv6/ARP/NDP/DNS/TCP packets are sent. • Source Interface - Specify a source interface for HTTP/ICMP/ICMPv6/ARP/DNS/TCP packets. Select **Traffic Quality** radio button: • Click **Add** in Add Track Members section and then configure the following options in the Add Traffic Quality Member dialog box: • Interface - Select a tracked interface from the drop-down list. • Interval - Specify the duration of each track period. The value range is 1 to 255 seconds. The default value is 3. After a track period is finished, system will reset the tracked value of new session. • Retries - Specify the threshold value which concludes the track entry is failed. The value range is 1 to 255. The default value is 3. • Weight - Specify how important this track failure is to the judgment of track object failure. The value range is 1 to 255. The default value is 255. • Low Watermark - Specify the failure threshold value of new session success rate. The value range is 0 to 100. The default value

Option	Description
	is 30. During a track period, when the new session success rate is below the specified low watermark, system will conclude the track is failed. • High Watermark - Specify the failure threshold value of new session success rate. The value range is 0 to 100. The default value is 50. During a track period, when the new session success rate exceeds the specified low watermark, system will conclude the track is successful. **Note**: During a track period, when the new session success rate is greater than or equal to the low watermark, and is less than or equal to the high watermark, system will keep the previous track state.
HA sync	Select this check box to enable HA sync function. The primary device will synchronize its information with the backup device.

3. Click **OK.**

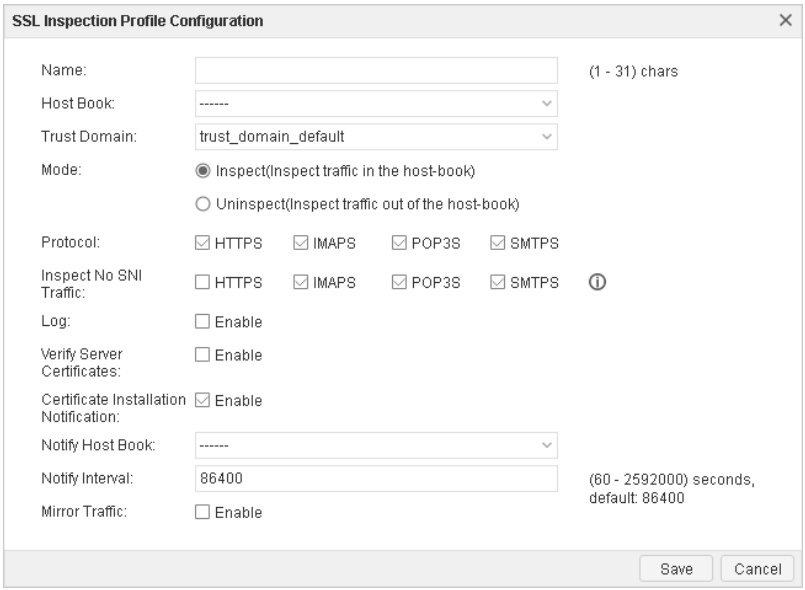
SSL Inspection Profile

System supports to decrypt the HTTP application traffic encrypted with the SSL protocol, and then forward the decrypted traffic to other devices in monitoring modes, such as DLP and IDS. After configuring the SSL inspection profile, you need to bind the profile to a policy or security zone to make it take effect. If the profile is bound to a security zone, system will decrypt and mirror the traffic of the zone (the source security zone) according to the profile configuration. If the profile is bound to a policy and the source security zone of a policy rule is bound with another SSL inspection profile, the profile bound to the rule will take effect first, while the profile bound to the security zone will be invalid.

Creating a SSL Inspection Profile

To create a SSL inspection profile, take the following steps:

1. Select **Object** > **SSL Inspection Profile**.
2. Click **New**.



In the SSL Inspection Profile Configuration dialog box, configure the following options.

Option	Description
Name	Specify the name of the SSL inspection profile. The new profile needs to be bound to a policy or security zone to take effect.

Option	Description
Host Book	Specify the host book to be matched for decryption.
Trust Domain	Select a configured trust domain from the drop-down list. To create a trust domain, see PKI. Note: After the CA certificate is generated, you need to export it and install it in the client browser for verification when the ADC establishes an SSL connection with the client.
Mode	The mode includes Inspect and Uninspect. Inspect means that system will decrypt a client connection after it matches the host book; while Uninspect means that the connection matching the host book will not be decrypted.
Log	Enable the function to record the SSL inspection logs. The function is disabled by default.
Verify Server Certificates	After the function is enabled, the ADC will establish an SSL connection with the server after the server certificate passes verification. The function is disabled by default.
Mirror Traffic	After the function is enabled, if the destination MAC address or destination IP of a client request is not the ADC address, but the traffic passes through the ADC and matches the host book, the device will decrypt the matched traffic. The function is disabled by default. Select an egress interface for the mirrored traffic from the **Interface** drop-down list. Type the destination port number of the client request into the **Destination Port** text box. The destination port you entered will replace the destination port of the mirrored packet. Type the destination MAC address of the mirrored packet into the **Destination MAC** text box.

3. Click **OK**.

Chapter 11 Policy

The Policy module provides the following functions:

- Security policy: Security policy is the function designed to control the traffic forwarding between security zones/segments. By default, all traffic between security zones/segments will be permitted.
- NAT: NAT, Network Address Translation, translates the IP address within an IP packet header to another IP address. When the IP packets pass through the devices or routers, the devices or routers will translate the source IP address and/or the destination IP address in the IP packets.
    - iQoS: iQoS is used to provide different priorities to different traffic, in order to control the delay and flapping, and decrease the packet loss rate. iQoS can assure the normal transmission of critical business traffic when the network is overloaded or congested.
- Session limit: The session limit function limits the number of sessions and controls the session rate to the source IP address, destination IP address, specified IP address, service, or role/user/user group in security zones, thereby protecting the connection table from DoS attacks and controlling the bandwidth of some applications.

Security Policy

Security policy is the function designed to control the traffic forwarding between security zones/segments. Without security policy rules, the ADC device will permit all traffic between security zones/segments by default. After configuring the security policy rule, the device can identify what traffic between security zones or segments will be permitted, and the others will be denied.

The basic elements of policy rules:

- The source zone and address of the traffic
- The destination zone and address of the traffic
- The service type of the traffic
- Actions that the devices will perform when processing the specific type of traffic, including Permit and Deny.

Generally a security policy rule consists of two parts: filtering conditions and actions. You can set the filtering conditions by specifying traffic's source zone/address, destination zone/address and service type. Each policy rule is labeled with a unique ID which is automatically generated when the rule is created. You can also specify a policy rule ID at your own choice. All policy rules in system are arranged in a specific order. When traffic flows into a device, the device will query for policy rules by turn, and processes the traffic according to the first matched rule.

The max global security policy rule numbers may vary in different ADC models.

Security policy supports IPv4 and IPv6 address.

This section contains the following contents:

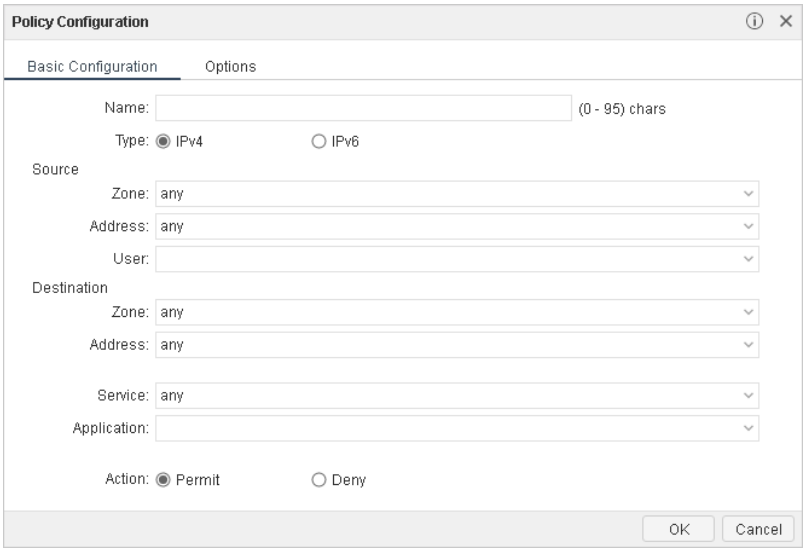
- Configure a security policy rule
- Manage the security policy rules: enable/disable a policy rule, clone a policy rule, adjust security rule position, configure default action, view and clear policy hit count, rule redundancy check, hit count check, schedule validity check and show disabled policies.
- Configure a security policy group
- View and search the security policy rules/security policy groups

Configuring a Security Policy Rule

To configure a security policy rule, take the following steps:

1. Select **Firewall** > **Security Policy**.

2. Click **New**, and the Policy Configuration dialog box will appear.



In the Basic tab, configure the corresponding options.

Option	Description
Name	Type the name of the security policy.
Type	Select the IP type, including IPv4 or IPv6. Only the IPv6 firmware can configure the IPv6 type IP.
Source Information	
Zone	Specify a source zone.
Address	Specify the source addresses. 1. Select an address type from the **Type** drop-down list, which can be Address Book, IP/Netmask, IP/Range or Hostname. 2. Select or type the source addresses based on the selected type.

Option	Description
	3. Click → to add the addresses to the right pane. If you click **Add**, you can create an address entry you need in the pop-up Address Book Configuration dialog box. 4. After adding the desired addresses, click the blank area in this dialog box to complete the source address configuration.
Destination	
Zone	Specify a destination zone.
Address	Specify the destination addresses.
Other Information	
Service	Specify a service or service group. 1. From the **Member Type** drop-down list, select a type: Service or Service Group. 2. You can search the desired service/service group, or expand the service/service group list. 3. After selecting the desired services/service groups, click → to add them to the right pane. To add a new service group, click **Add**. 4. After adding the desired services, click the blank area in this dialog box to complete the service configuration.
Application	Specify an application/application group/application filters of the policy rules. 1. From the **Application** drop-down list, you can search the desired application/application group/application filter, or expand the list of applications/application groups/application filters. 2. After selecting the desired applications/application groups/application filters, click → to add them to the right pane.

Option	Description
	3. After adding the desired objects, click the blank area in this dialog box to complete the application configuration. To create a new application group or application filter, click **New AppGroup** or **New AppFilter**.
Action	Specify an action for the traffic that is matched to the policy rule, including: • Permit - Select **Permit** radio button to permit the traffic to pass through. • Deny - Select **Deny** radio button to deny the traffic.

3. In the Options tab, configure the corresponding options.

Option	Description
ssli_profile_config	After the function is enabled, system can decrypt the HTTP application traffic encrypted with the SSL protocol, and then forward the decrypted traffic to other devices in monitoring modes, such as DLP and IDS. You can select a configured SSL Inspection profile from the **Profile** drop-down list.
Schedule	Specify a schedule when the security policy rule takes effect. Select a desired schedule from the **Schedule** drop-down list. After selecting the desired schedules, click the blank area in this dialog box to complete the schedule configuration. To create a new schedule, click **New Schedule**.
Log	You can log policy rule matching in the system logs according to your needs. • For the policy rules of Permit, logs will be generated in two conditions: the traffic that is matched to the policy rules starts its session (Select the **Session start** check box) and ends its session (Select the **Session end** check box).

Option	Description
	• For the policy rules of Deny, logs will be generated when the traffic that is matched to the policy rules is denied (Select the **Deny** check box). Select one or more check boxes to enable the corresponding log types.
Position	Select a rule position from the **Position** drop-down list. Each policy rule is labeled with a unique ID or name. When traffic flows into a device, the device will query for the policy rules by turn, and processes the traffic according to the first matched rule. However, the policy rule ID is not related to the matching sequence during the query. The sequence displayed in policy rule list is the query sequence for policy rules. The rule position can be an absolute position, i.e., at the top or bottom, or a relative position, i.e., before or after an ID or a name.
Description	Type the description for the security policy.

4. Click **OK** to save your settings.

Managing Security Policy Rules

This sections describes how to manage security policy rules, including: enable/disable a policy rule, clone a policy rule, adjust security rule position, configure default action, view and clear policy hit count, rule redundancy check, hit count check, schedule validity check and show disabled policies.

Enabling/Disabling a Policy Rule

By default the configured policy rule will take effect immediately. You can terminate its control over the traffic by disabling the rule.

To enable/disable a policy rule, take the following steps:

1. Select **Firewall** > **Security Policy**.

2. Click **Policy** at the top-right corner of the list to enter the **Security Policy** page. Then select the security policy rule that

you want to enable/disable.

3. Click **...**, and then select **Enable** or **Disable** to enable or disable the rule.

The disabled rule will not be displayed in the list. To view the disabled rules, click **...**, and then select **Show Disabled Policies**.

Cloning a Policy Rule

To clone a policy rule, take the following steps:

1. Select **Firewall** > **Security Policy**.
2. Click **Policy** at the top-right corner of the list to enter the Policy Rule page. Then select the security policy rule that you want to clone, and click **Copy**.
3. Click **Paste**. In the pop-up dialog box, select the desired position. Then the rule will be cloned to the desired position.

Adjusting Security Policy Rule Position

To adjust the rule position, take the following steps:

1. Select **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy** to enter the **Security Policy** page.
3. Select the security policy whose position will be adjusted, and click **Move**.
4. In the pop-up menu, type the rule ID or name, and click **Before ID**, **After ID**, **Before Name** or **After Name**. Then the rule will be moved before or after the specified ID or name.

Configuring Default Action

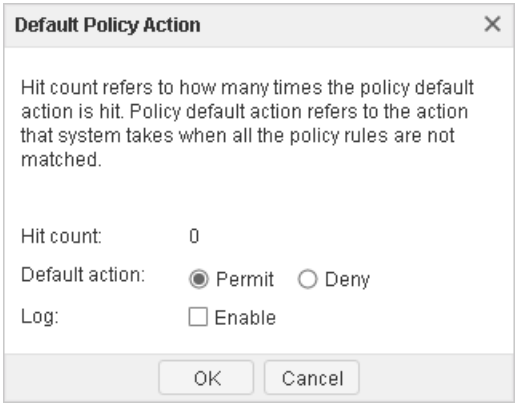
You can specify a default action for the traffic that is not matched with any configured policy rule. System will process the traffic according to the specified default action. By default system will deny such traffic.

To specify a default policy action, take the following steps:

1. Select **Firewall** > **Security Policy**.

2. At the top-right corner of the list, click **Policy** to enter the **Security Policy** page.

3. Click **...** and select **Default Policy Action**.



In the Default Policy Action dialog box, configure the following options.

Option	Description
Hit count	Shows the statistics on policy matching.
Default action	Specify a default action for the traffic that is not matched with any configured policy rule. • Click **Permit** to permit the traffic to pass through. • Click **Deny** to deny the traffic.
Log	Configure whether to generate logs for the traffic that is not matched with any configured policy rule. By default system will not generate logs for such traffic. To enable log, select the **Enable** check box, and system will generate logs for such traffic.

4. Click **OK** to save your settings.

Viewing and Clearing Policy Hit Count

System supports statistics on policy hit counts, i.e., statistics on the matching between traffic and policy rules. Each time the inbound traffic is matched with a certain policy rule, the hit count will increase by 1 automatically.

To view a policy hit count, select **Firewall** > **Security Policy**. In the policy rule list, view the statistics on policy hit counts under the Hit Count column.

To clear a policy hit count, take the following steps:

1. Select **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy** to enter the **Security Policy** page.
3. Click **...** and select **Clearing Policy Hit Count**.
4. In the Clearing Hit Count dialog box, configure the following options:
   - All policies: Clears the hit counts for all policy rules.
   - Default policy: Clears the hit counts for the default action policy rules.
   - Policy ID: Clears the hit counts for a policy rule with the specified ID. Type the ID of the policy rule into the text box.
   - Name: Clears the hit counts for a specified name policy rule. Type the name of the policy rule into the text box.
5. Click **OK** to save your settings.

Rule Redundancy Check

In order to make the rules in the policy effective, system provides a method to check the conflicts among rules in a policy. With this method, administrators can check whether the rules overshadow each other.

To start a rule redundancy check, take the following steps:

1. Select **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy** to enter the **Security Policy** page.
3. Click **...** and select **Redundancy Check**. After the check, system will highlight the policy rule which is overshadowed. You can view the ID of the overwritten policy rule under the Overwritten column.

Note: Status will be shown below the policy list when redundancy check is started. It is not recommended to edit a policy rule during the redundancy check. You can click  to stop the check manually. After clicking, confirm whether to terminate the rule redundancy check in the pop-up dialog box. Click **OK** to stop the check.

Hit Count Check

System supports to check policy rule hit counts.

To check hit count, take the following steps:

1. Select **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy** to enter the **Security Policy** page.
3. Click **...** and select **Hit Count Check**. After the check, the policy rules whose hit count is 0 will be highlighted, that is to say, they are not used in system.

Schedule Validity Check

In order to make sure that the policies based on schedule are effective, system provides a method to check the validity of policies. After checking the policy, the invalid policies based on schedule will be highlighted by yellow.

To check schedule validity, take the following steps:

1. Select **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy** to enter the **Security Policy** page.
3. Click **...** and select **Schedule Validity Check**. After the check, system will highlight the invalid policy based on schedule by yellow. Meanwhile, you can view the validity status under the Validity column in the policy list.

Showing Disabled Policies

To show disabled policies, take the following steps:

1. Select **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy** to enter the **Security Policy** page.
3. Click **...** and select **Show Disabled Policies**. The disabled policies will be highlighted by green in the policy list.

Note:

- By default (the "Schedule Validity Check" and "Show Disabled Policies" are not selected), the policy list only displays the enabled policies which are not highlighted.
- When you select both "Schedule Validity Check" and "Show Disabled Policies", the policy is managed as follows:
  - The policy list will display the Validity column, which shows the validity status of policies.
  - The invalid policy based on schedule will be highlighted by yellow no matter if the policy is disabled or not.
  - If the valid policy based on schedule is disabled, it will be highlighted by green.

Configuring a Policy Group

You can organize some policy rules together to form a policy group, and configure the policy group directly.

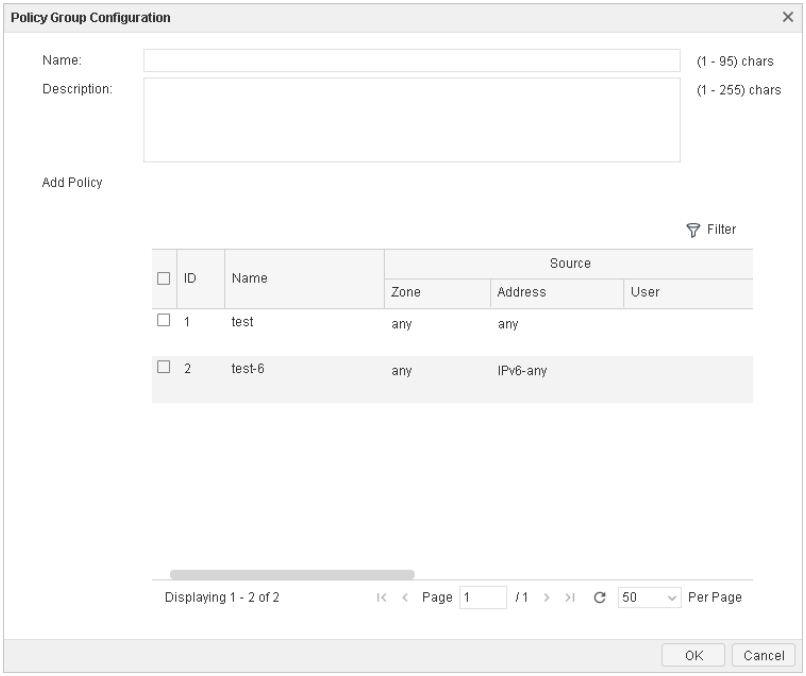
Configuring a security policy group include the following matters: creating a policy group, deleting a policy group, enable/disable a policy group, add/delete a policy rule member, edit a policy group and show disabled policy group.

Creating a Policy Group

To create a policy group, take the following steps:

1. Select **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy Group** to enter the **Security Policy Group** page.

3. Click **New**.



In the Policy Group Configuration dialog box, configure the following options.

Option	Description
Name	Specify the name of the policy group. The length is 1 to 95 characters.
Description	Specify the description for the policy group. The length is 1 to 255 characters.
Add Policy	In the policy rule list, select the security policy rule you want to add to the policy group.

4. Click **OK** to save your settings.

Deleting a Policy Group

To delete a policy group, take the following steps:

1. Select **Firewall** > **Security Policy**.

2. At the top-right corner of the list, click **Policy Group** to enter the **Security Policy Group** page.

3. Select the policy group that you want to delete, and click **Delete**.

Enabling/Disabling a Policy Group

By default the configured policy group will take effect immediately.

To enable/disable a policy group, take the following steps:

1. Select **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy Group** to enter the **Security Policy Group** page.
3. Select the policy group that you want to enable or disable, and click the enable button under the Status column. The enabled state is displayed as  , and the disabled state is displayed as  .

Adding/Deleting a Policy Rule Member

To add a policy rule member to the policy group, take the following steps:

1. Select **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy Group** to enter the **Security Policy Group** page.
3. In the policy group list, click the "+" in front of the policy group item to expand the member list of the policy group.
4. Click **Add Member** to open the **Policy Group-Add policy** dialog box, which displays the list of policy rules that are not added to the policy group.
5. Select the policy rules that you want to add to the policy group.
6. Click **OK** to save your settings.

 **Note:** A policy rule only can be added to a policy group.

To delete a policy rule member from the policy group, take the following steps:

1. Select **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy Group** to enter the **Security Policy Group** page.
3. In the policy group list, click the "+" in front of the policy group item to expand the member list of the policy group.
4. Select the policy group that you want to delete, and click **Delete**.

Editing a Policy Group

To modify the name or description of a policy group, take the following steps::

1. Select **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy Group** to enter the **Security Policy Group** page.
3. Select the policy group that you want to edit, and click **Edit**.
4. In the Policy Group Configuration dialog box, modify the name or description of the policy group.

Showing Disabled Policy Group

To show disabled policy groups, take the following steps:

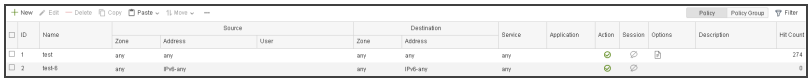
1. Select **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy Group** to enter the **Security Policy Group** page.
3. Select the check box of **Show Disabled Policy Group** above the list. The disabled policy group will be displayed in the policy group list, otherwise the policy group list will show only the enabled policy group.

Viewing and Searching Security Policy Rules/Policy Groups

You can view and search the policy rules or policy groups in the policy/policy group list.

Viewing the Policy/Policy Group

View the security policy rules in the policy rule list:



- Each column displays the corresponding configurations.
- Click the button under the Session column in the policy list, and then the Session Detail dialog box will appear. You can view the current session status of the selected policy rule.
- Hover over your mouse on the configuration in a certain column. Then based on the configuration type, the WebUI displays either the icon or the detailed configurations.
    - You can view the detailed configurations directly.
    - You can click the icon. Based on the configuration type, the WebUI displays **Filter** or **Detail**.
        - Click **Detail** to see the detailed configurations.
        - Click **Filter**, the filter condition of the configuration you are hovering over with your mouse appears on the top of the list, and then you can filter the policy rule according to the filter condition. For detailed information of filtering policy rules, see Searching Security Policy Rules/Policy Groups.

View the policy groups in the policy group list:

- Each column displays the corresponding configurations.
- You can view the current policy group status under the Status column. The enabled state is displayed as , and the disabled state is displayed as .

Searching Security Policy Rules/Policy Groups

Use the Filter to search for the policy rules that match the filter conditions.

1. Click **Firewall** > **Security Policy**.
2. At the top-right corner of the list, click **Policy/Policy Group** to enter the **Security Policy/Security Policy Group** page.

3. At the top-right corner of the **Security Policy/Security Policy Group** page, click **Filter**. Then a new row appears at the top.
4. Click **+Filter**, and select a filter condition from the drop-down list, and then enter a value.
5. Press **Enter** to search for the policy rules that match the filter conditions.
6. Repeat the above two steps to add more filter conditions. The relationship between each filter condition is **AND**.
7. To delete a filter condition, hover your mouse on that condition and then click the ✕Remove All icon. To close the filter, click the ✕ icon on the right side of the row.

Save the filter conditions.

1. After adding the filter conditions, click the down arrow behind the **+Filter**, and click the Save Filters button in the drop-down list.
2. Specify the name of the filter condition you want to save. The maximum length of the name is 32 characters, and the name supports only Chinese and English characters and underscores.
3. Click **Save** on the right side of the text box.
4. To use the saved filter condition, double click the name of the saved filter condition.
5. To delete the saved filter condition, click ✕ on the right side of the filter condition.

Note:

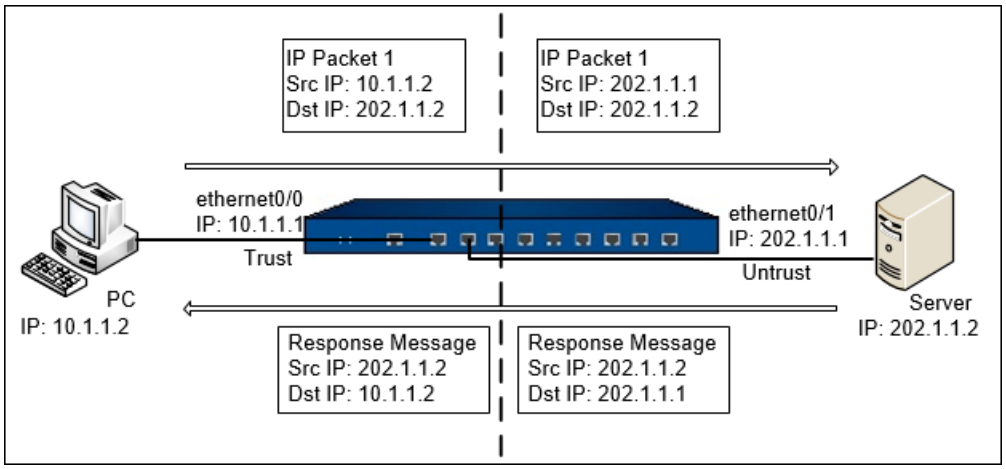
- You can add up to 20 filter conditions as needed.
- After the device has been upgraded, the saved filter conditions will be cleared.

NAT

NAT, Network Address Translation, translates the IP address within an IP packet header to another IP address. When the IP packets pass through the devices or routers, the devices or routers will translate the source IP address and/or the destination IP address in the IP packets. In practice, NAT is mostly used to allow the private network to access the public network, vice versa.

Basic Translation Process of NAT

When a device is implementing the NAT function, it lies between the public network and the private network. The following diagram illustrates the basic translation process of NAT.



As shown above, the device lies between the private network and the public network. When the internal PC at 10.1.1.2 sends an IP packet (IP packet 1) to the external server at 202.1.1.2 through the device, the device checks the packet header. Finding that the IP packet is destined to the public network, the device translates the source IP address 10.1.1.2 of packet 1 to the public IP address 202.1.1.1 which can get routed on the Internet, and then forwards the packet to the external server. At the same time, the device also records the mapping between the two addresses in its NAT table. When the response packet of IP packet 1 reaches the device, the device checks the packet header again and finds the mapping records in its NAT table, and replaces the destination address 202.1.1.1 with the private address 10.1.1.2. In this process, the device is transparent to the PC and the Server. To the external server, it considers that the IP address of the internal PC is 202.1.1.1 and knows nothing about the private address 10.1.1.2. Therefore, NAT hides the private network of enterprises.

Implementing NAT

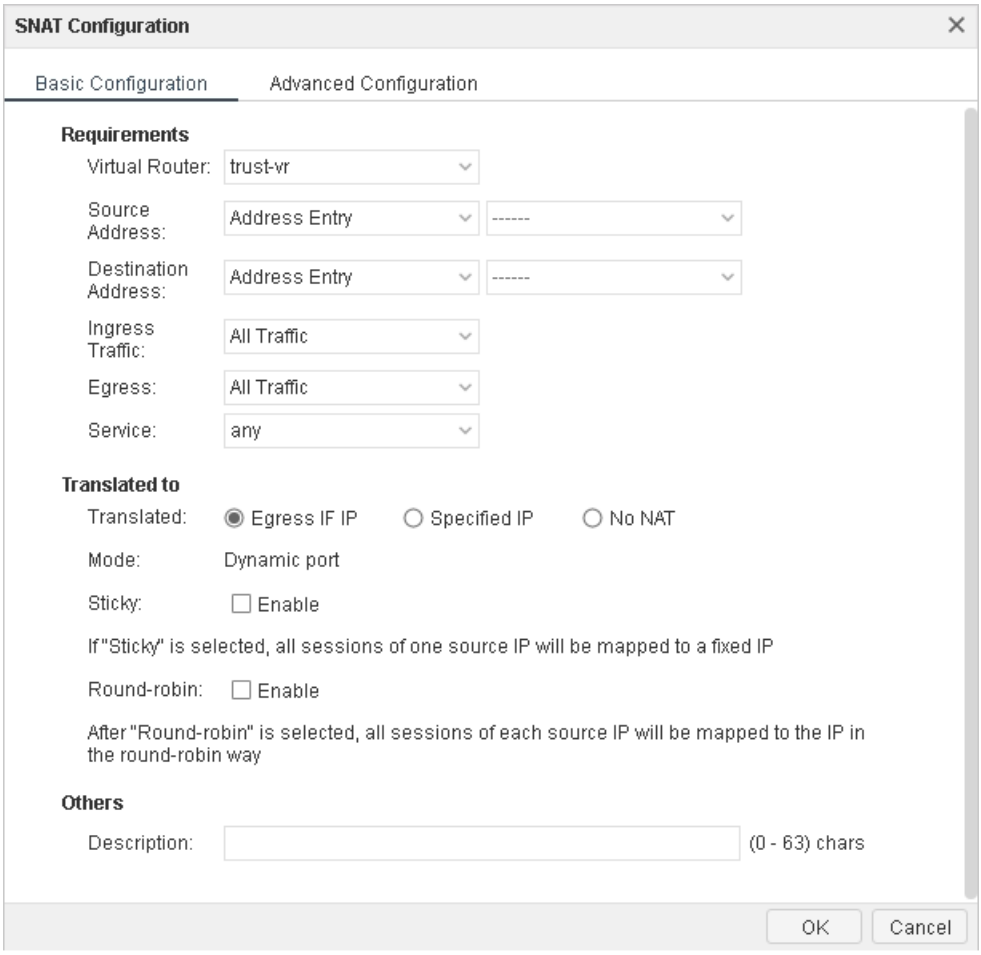
The devices translate the IP address and port number of the internal network host to the external network address and port number, and vice versa. This is the translation between the "private IP address + port number" and "public IP address + port number".

The devices achieve the NAT function through the creation and implementation of NAT rules. For example, SNAT translates source IP addresses, thereby hiding the internal IP addresses or sharing the limited IP addresses.

Configuring SNAT

To create an SNAT rule, take the following steps:

1. Select **Network** > **NAT** > **SNAT**.
2. Click **New**. The SNAT Configuration dialog box will appear.



In the Basic tab, configure the following options.

Requirements	
Virtual Router	Specify a VRouter for the SNAT rule.
Source Address	Specify the source IP address of the traffic, including: • Address Entry - Select an address entry from the drop-down list. • IP Address - Type an IP address into the box. • IP/Netmask - Type an IP address and its netmask into the box.
Destination Address	Specify the destination IP address of the traffic, including: • Address Entry - Select an address entry from the drop-down list. • IP Address - Type an IP address into the box.

Requirements	
	• IP/Netmask - Type an IP address and its netmask into the box.
Ingress Traffic	Specify the ingress traffic. The default value is all traffic. • All traffic - Specify all traffic as the ingress traffic. Traffic from any ingress interfaces will continue to match this SNAT rule. • Ingress Interface - Specify the ingress interface of traffic. Select an interface from the drop-down list. When the interface is specified, only the traffic from this interface will continue to match this SNAT rule, while traffic from other interfaces will not.
Egress	Specify the egress traffic. The default value is all traffic. • All traffic - Specify all traffic as the egress traffic. Traffic from all egress interfaces will continue to match this SNAT rule. • Egress Interface - Specify the egress interface of traffic. Select an interface from the drop-down list. When the interface is specified, only the traffic from this interface will continue to match this SNAT rule, while traffic from other interfaces will not.
Service	Specify the service type of the traffic. You can search the desired service, or click **Add** to create a service or service group.
Translated to	
Translated	Specify the translated NAT IP address, including: • Egress IF IP - Specify the NAT IP address to be an egress interface IP address. • Specified IP - Specify the NAT IP address to be a specified IP address. After selecting this option, select **Address Entry**, **IP Address** or **IP/Netmask** from the **Address** drop-down list, and specify the corresponding value. • No NAT - Do not implement NAT.

Requirements	
Mode	Specify the translation mode, including: • Static - Static mode means one-to-one translation. This mode requires the translated address entry to contain the same number of IP addresses as that of the source address entry. • Dynamic IP - Dynamic IP mode means multiple-to-one translation. This mode translates the source address to a specific IP address. Each source address will be mapped to a unique IP address, until all specified addresses are occupied. • Dynamic port - Called PAT. Multiple source addresses will be translated to one specified IP address in an address entry. If Sticky is not enabled, the first address in the address entry will be used first; when the port resources of the first address are exhausted, the second address will be used. If Sticky is enabled, all sessions from an IP address will be mapped to the same fixed IP address. Click the **Enable** check box behind Sticky to enable Sticky. You can also track if the public address after NAT is available, i.e., use the translated address as the source address to track if the destination website or host is accessible. Select the **Enable** check box behind Track to enable the function, and select a track object from the drop-down list.
Others	
Description	Type the description for the SNAT rule.

In the Advanced Configuration tab, configure the corresponding options.

Option	Description
NAT Log	Select the **Enable** check box to enable the log function for this SNAT rule. System will generate log information when there is traffic matching this NAT rule.
Position	Specify the position of the rule. Each SNAT rule has a unique ID. When the traffic flows into the device, the device will search the SNAT rules in order, and then implement NAT on the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the SNAT rule list is the order of the rule matching. Select one of the following items from the drop-down list: • Bottom - The rule is located at the bottom of all the rules in the SNAT rule list. By default, system will put the newly-created SNAT rule at the bottom of all SNAT rules. • Top - The rule is located at the top of all the rules in the SNAT rule list. • Before ID - Type the ID number into the text box. The rule will be located before the ID you specified. • After ID - Type the ID number into the text box. The rule will be located after the ID you specified.
ID	Specify the method you get the rule ID. Each SNAT rule has its unique ID. It can be automatically assigned by system or manually assigned by yourself. If you select **Manually assign**, type an ID number into the text box behind.

3. Click **OK** to save the settings.

Enabling/Disabling a SNAT Rule

By default the configured SNAT rule will take effect immediately. You can terminate its control over the traffic by disabling the rule

To enable/disable a policy rule:

1. Select **Network** > **NAT** > **SNAT**.
2. Select the SNAT rule that you want to enable/disable.
3. Click **Enable** or **Disable** to enable or disable the rule.

Copying/Pasting a SNAT Rule

To copy/paste a SNAT rule, take the following steps:

1. Select **Network** > **NAT** > **SNAT**.
2. Select the SNAT rule that you want to clone and click **Copy**.
3. Click **Paste**. In the pop-up drop-down list, select the desired position. Then the rule will be cloned to the desired position.

Option	Description
Top	The rule is pasted to the top of all the rules in the SNAT rule list.
Bottom	The rule is pasted to the bottom of all the rules in the SNAT rule list.
Before the Rule Selected	The rule will be pasted before the Rule selected.
After the Rule Selected	The rule will be pasted after the Rule selected.

Note: When pasting SNAT rules, if multiple SNAT rules are selected or no rules are selected in the desired position, the **Before the Rule Selected** and **After the Rule Selected** options will be unavailable.

Adjusting Priority

Each SNAT rule has a unique ID. When the traffic flows into the device, the device will search the SNAT rules in order, and then implement NAT on the source IP of the traffic according to the first matched rule. The sequence of the ID shown in the SNAT rule list is the order of the rule matching.

To adjust priority, take the following steps:

1. Select **Network** > **NAT** > **SNAT**.
2. Select the rule you want to adjust its priority and click **Priority**. In the Priority dialog box, move the selected rule to:

Option	Description
Top	The rule is moved to the top of all of the rules in the SNAT rule list.
Bottom	The rule is moved to the bottom of all of the rules in the SNAT rule list.
Before ID	Specify an ID number. The rule will be moved before the ID you specified.
After ID	Specify an ID number. The rule will be moved after the ID you specified.

3. Click **OK** to save the settings.

NAT Hit Analysis

System supports statistics on hit counts of SNAT rules, the first hit time, the last hit time, and the days since last hit, which can help you identify the NAT rules that need to be cleared. You can view the hit counts of specified NAT rules by setting up filters.

To check the SNAT rule hit counts, take the following steps:

1. Select **Network** > **NAT** > **SNAT Hit Analysis**.
2. Select filter conditions from the **+Filter** drop-down list, and configure filter conditions as needed.

   Configure the options as follows.

Option	Description
Virtual Router	Specify a virtual router. Then the NAT rules with the virtual router will be displayed.
ID	Specify an ID. Then the NAT rule with the ID will be displayed.
Days Since First Hit>	Specify the days after the first hit. Then the NAT rules whose number of days since the first hit is greater than the specified number of days will be displayed.
Unhit Rules	The rules that were never hit will be displayed.
Days Since Last	Specify the days after the last hit. Then the NAT rules whose number of

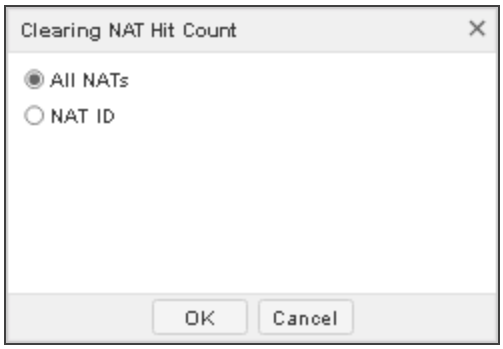
Option	Description
Hit>	days since the last hit is greater than the specified number of days will be displayed.
Days Since NAT Created>	Specify the days after the NAT rule is created. Then the NAT rules whose number of days since creation is greater than the specified number of days will be displayed.

3. Click **Analyze** to view the latest result of NAT Hit Analysis.
4. Click the icon in front of a NAT rule ID to view the details of the NAT rule.
5. Click the icon on the left side of **+Filter** to save the selected filters. Click **Save Filters**, type the name of the filters and click **Save**. After saved, the combined filters can be selected directly in the drop-down list.
6. To delete a filter condition, hover your mouse on that condition and then click the icon. To delete all filter conditions, click the icon on the right side of the row.

Note: "Virtual Router" is a required filter condition.

To clear the SNAT rule hit counts, take the following steps:

1. Select **Network** > **NAT** > **SNAT Hit Analysis**.
2. Click **Clear**.



In the Clearing NAT Hit Count dialog box, configure the following options.

Option	Description
All NATs	Clears the hit counts of all NAT rules.
NAT ID	Clears the hit counts of a specified NAT rule ID. You need to type the ID of the NAT rule into the text box.

3. Click **OK**.

You can also perform other operations:

- Click the icon to delete the NAT rule.
- Click the icon to disable the NAT rule.

Configuring DNAT

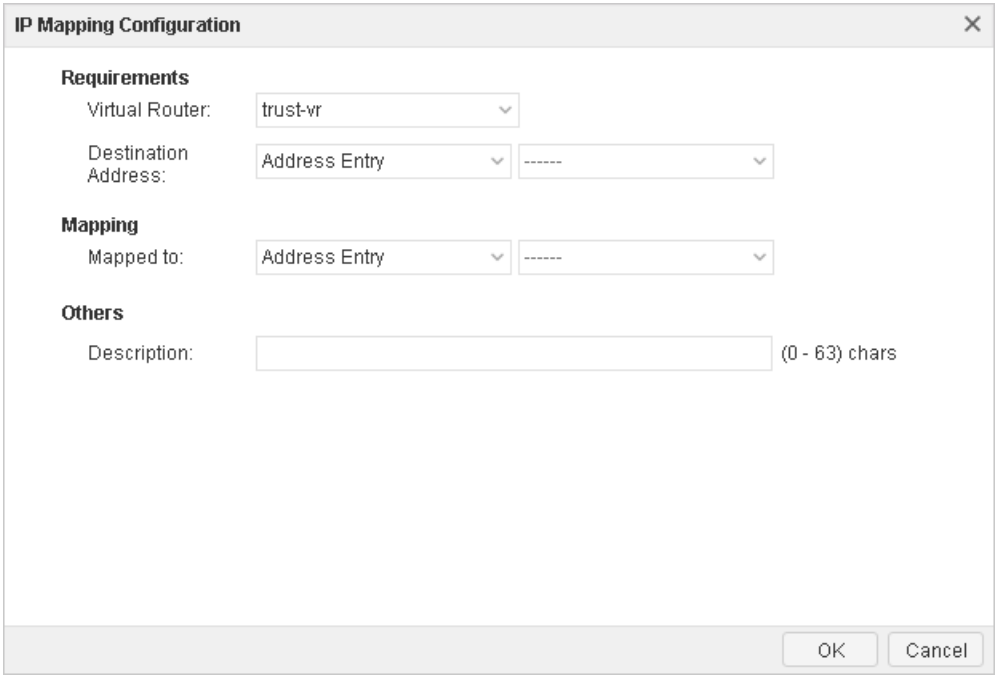
DNAT translates destination IP addresses, usually the IP addresses of internal servers (such as the WWW server or SMTP server) protected by the device are translated to the public IP addresses.

Configuring an IP Mapping Rule

To configure an IP mapping rule, take the following steps:

1. Select **Network** > **NAT** > **DNAT**.

2. Click **New** and select **IP Mapping**.



In the IP Mapping Configuration dialog box, configure the corresponding options.

Requirements	
Virtual Router	Specify a VRouter for the DNAT rule.
Destination Address	Specify the destination IP address of the traffic, including: • Address Entry - Search or select an address entry from the drop-down list, and click **OK**. To clear the selected address entry, click **Clear**. • IP Address - Type an IP address into the box. • IP/Netmask - Type an IP address and its netmask into the box. • Dynamic IP (Physical Interface): In the drop-down list, search or select an interface which obtains IP via the DHCP and PPPoE protocols, and click **OK**.
Mapping	
Mapped to	Specify the translated NAT IP address, including **Address Entry**, **IP**

Requirements	
	Address, and **IP/Netmask**. The number of the translated NAT IP addresses you specified must be the same as the number of the destination IP addresses of the traffic.
Others	
Description	Type the description for the DNAT rule.

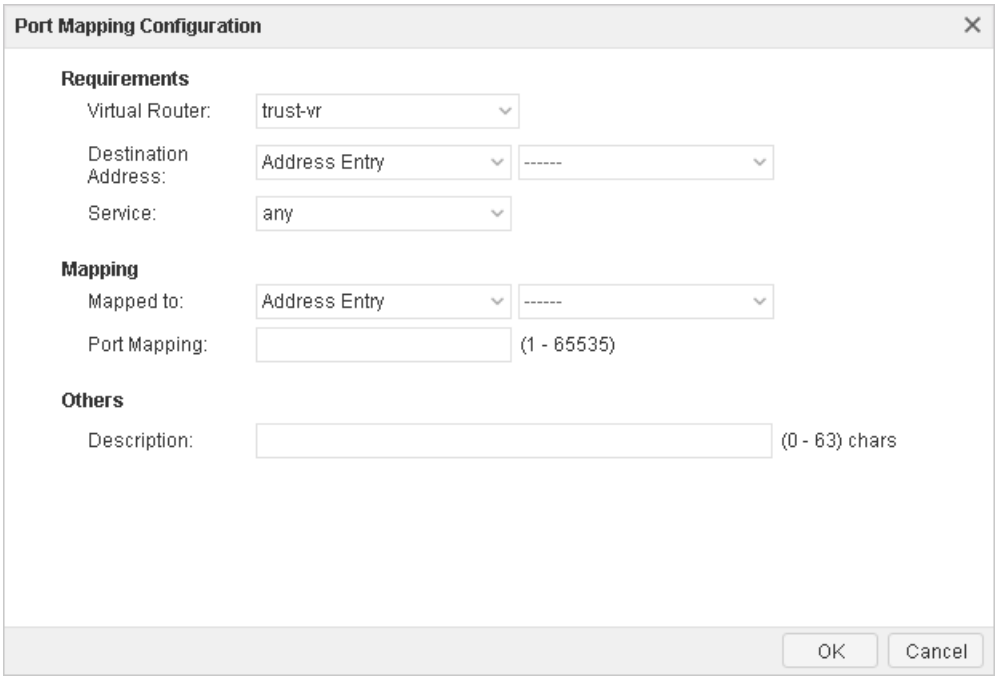
3. Click **OK** to save the settings.

Configuring a Port Mapping Rule

To configure a port mapping rule, take the following steps:

1. Select **Network** > **NAT** > **DNAT**.

2. Click **New** and select **Port Mapping**.



In the Port Mapping Configuration dialog box, configure the corresponding options.

Requirements	
Virtual Router	Specify a VRouter for the DNAT rule.
Destination Address	Specify the destination IP address of the traffic, including: • Address Entry - Search or select an address entry from the drop-down list, and click **OK**. To clear the selected address entry, click **Clear**. • IP Address - Type an IP address into the box. • IP/Netmask - Type an IP address and its netmask into the box. • Dynamic IP (Physical Interface): In the drop-down list, search or select an interface which obtains IP via the DHCP and PPPoE protocols, and click **OK**.
Service	Specify the service type of the traffic. You can search the desired service, or click **Add** to create a service or service group.
Mapping	
Mapped to	Specify the translated NAT IP address, including **Address Entry**, **IP Address**, and **IP/Netmask**. The number of the translated NAT IP addresses you specified must be the same as the number of the destination IP addresses of the traffic.
Port Mapping	Type the translated port number of the Intranet server. The available range is 1 to 65535.
Others	
Description	Type the description for the DNAT rule.

3. Click **OK** to save the settings.

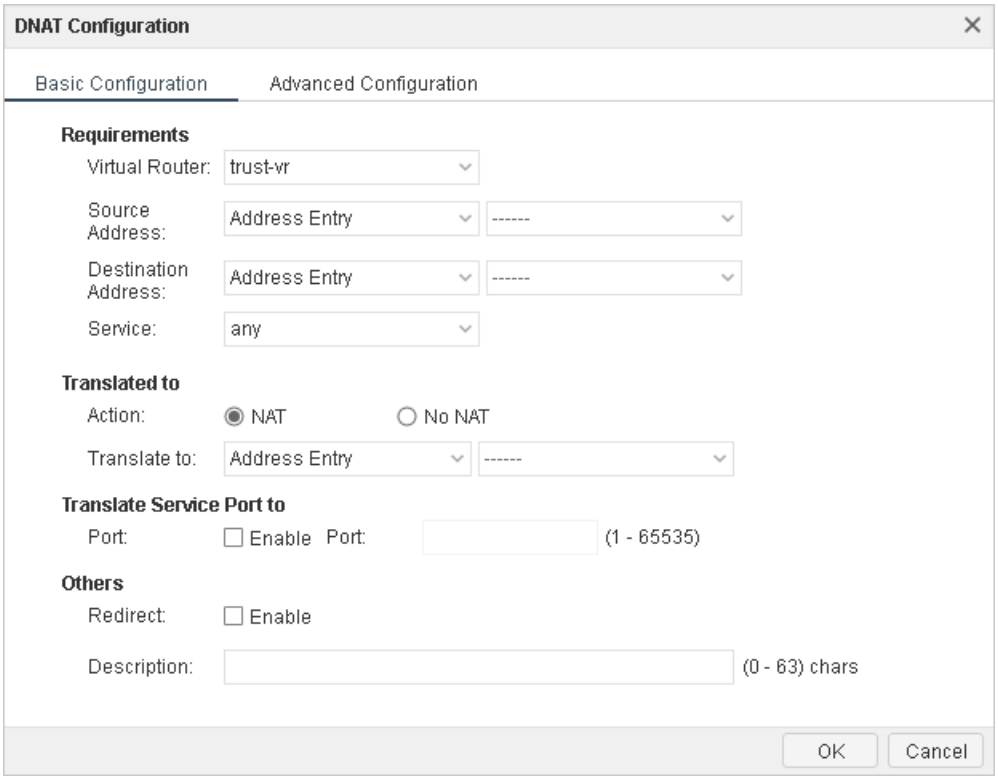
Configuring an Advanced NAT Rule

You can create a DNAT rule and configure the advanced settings, or you can edit the advanced settings of an existing DNAT rule.

To create a DNAT rule and configure the advanced settings, take the following steps:

1. Select **Network** > **NAT** > **DNAT**.

2. Click **New** and select **Advanced Configuration**. To edit the advanced settings of an existing DNAT rule, select it and click **Edit**. The DNAT Configuration dialog box will appear.



In the Basic tab, configure the corresponding options.

Requirements	
Virtual Router	Specify a VRouter for the DNAT rule.
Source Address	Specify the source IP address of the traffic, including: • Address Entry - Search or select an address entry from the drop-down list, and click **OK**. To clear the selected address entry, click **Clear**. • IP Address - Type an IP address into the box. • IP/Netmask - Type an IP address and its netmask into the box.
Destination	Specify the destination IP address of the traffic, including:

Requirements	
Address	• Address Entry - Search or select an address entry from the drop-down list, and click **OK**. To clear the selected address entry, click **Clear**. • IP Address - Type an IP address into the box. • IP/Netmask - Type an IP address and its netmask into the box. • Dynamic IP (Physical Interface): In the drop-down list, search or select an interface which obtains IP via the DHCP and PPPoE protocols, and click **OK**.
Service	Specify the service type of the traffic. You can search the desired service, or click **Add** to create a new service or service group.
Translated to	
Action	Specify the action for the traffic you specified, including: • NAT - Implements NAT for the eligible traffic. • No NAT - Do not implement NAT for the eligible traffic.
Translate to	After selecting **NAT**, you need to specify the type of the translated IP address, including **Address Entry**, **IP Address**, and **IP/Netmask**. Then select an entry or specify the value.
Translate Service Port to	
Port	Select **Enable** and type the translated port number into the text box behind. The value range is 1 to 65535.
Others	
Redirect	Select **Enable** to enable the function. When the number of this **Translate to** is different from the **Destination Address** of the traffic or the **Destination Address** is **any**, you should enable the redirect function for this DNAT rule.

Requirements	
Description	Type the description for the DNAT rule.

In the Advanced Configuration tab, configure the corresponding options.

Track Server	
Track Ping Packets	After enabling this function, system will send Ping packets to check whether the Intranet servers are reachable.
Track TCP Packets	After enabling this function, System will send TCP packets to check whether the TCP ports of Intranet servers are reachable.
TCP Port	Specify the TCP port number of the monitored Intranet server.
Others	
NAT Log	Enable the log function for this DNAT rule to generate the log information when traffic matches this NAT rule.
Position	Specify the position of the rule. Each DNAT rule has a unique ID. When the traffic flows into the device, the device will search the DNAT rules in order, and then implement NAT on the destination IP of the traffic according to the first matched rule. The sequence of the ID shown in the DNAT rule list is the order of the rule matching. Select one of the following items from the drop-down list: • Bottom - The rule is located at the bottom of all of the rules in the DNAT rule list. By default, the system will put the newly-created DNAT rule at the bottom of all of the DNAT rules. • Top - The rule is located at the top of all of the rules in the DNAT rule list. • Before ID - Type the ID number into the text box. The rule will be located before the ID you specified. • After ID - Type the ID number into the text box. The rule will be located after the ID you specified.
ID	Specify the method you get the rule ID. Each DNAT rule has a unique ID.

Track Server	
	It can be automatically assigned by system or manually assigned by yourself. If you select **Manually assign**, type an ID number into the text box behind.

3. Click **OK** to save the settings.

Enabling/Disabling a DNAT Rule

By default, the configured DNAT rule will take effect immediately. You can terminate its control over the traffic by disabling the rule.

To enable/disable a DNAT rule, take the following steps:

1. Select **Network** > **NAT** > **DNAT**.
2. Select the DNAT rule that you want to enable/disable.
3. Click **Enable** or **Disable** to enable or disable the rule.

Copying/Pasting a DNAT Rule

When there are a large number of NAT rules in system, to create a NAT rule which is similar to a configured NAT rule easily, you can copy the NAT rule and paste it to the specified location.

To copy/paste a DNAT rule, take the following steps:

1. Select **Network** > **NAT** > **DNAT**.
2. Select the DNAT rule that you want to clone and click **Copy**.
3. Click **Paste**. In the pop-up drop-down list, select the desired position. Then the rule will be cloned to the desired position.

Option	Description
Top	The rule is pasted to the top of all of the rules in the DNAT rule list.
Bottom	The rule is pasted to the bottom of all of the rules in the DNAT rule list.
Before the Rule Selected	The rule will be pasted before the Rule selected.

Option	Description
After the Rule Selected	The rule will be pasted after the Rule selected.

Adjusting Priority

Each DNAT rule has a unique ID. When the traffic flows into the device, the device will search the DNAT rules in order, and then implement NAT on the destination IP of the traffic according to the first matched rule. The sequence of the ID shown in the DNAT rule list is the order of the rule matching.

To adjust priority, take the following steps:

1. Select **Network** > **NAT** > **DNAT**.
2. Select the rule you want to adjust its priority from the DNAT rule list, and click **Priority**. In the Priority dialog box, move the selected rule to:

Option	Description
Top	The rule is moved to the top of all of the rules in the DNAT rule list.
Bottom	The rule is moved to the bottom of all of the rules in the DNAT rule list.
Before ID	Specify an ID number. The rule will be moved before the ID you specified.
After ID	Specify an ID number. The rule will be moved after the ID you specified.

3. Click **OK** to save the settings.

NAT Hit Analysis

System supports statistics on hit counts of DNAT rules, the first hit time, the last hit time, and the days since last hit, which can help you identify the NAT rules that need to be cleared. You can view the hit counts of specified NAT rules by setting up filters.

To check the DNAT rule hit counts, take the following steps:

1. Select **Network** > **NAT** > **DNAT Hit Analysis**.
2. Select filter conditions from the **+Filter** drop-down list, and configure filter conditions as needed.

Configure the options as follows.

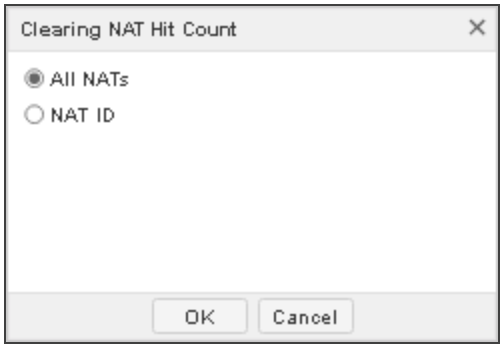
Option	Description
Virtual Router	Specify a virtual router. Then the NAT rules with the virtual router will be displayed.
ID	Specify an ID. Then the NAT rule with the ID will be displayed.
Days Since First Hit>	Specify the days after the first hit. Then the NAT rules whose number of days since the first hit is greater than the specified number of days will be displayed.
Unhit Rules	The rules that were never hit will be displayed.
Days Since Last Hit>	Specify the days after the last hit. Then the NAT rules whose number of days since the last hit is greater than the specified number of days will be displayed.
Days Since NAT Created>	Specify the days after the NAT rule is created. Then the NAT rules whose number of days since creation is greater than the specified number of days will be displayed.

3. Click **Analyze** to view the latest result of NAT Hit Analysis.
4. Click the icon in front of a NAT rule ID to view the details of the NAT rule.
5. Click the icon on the left side of **+Filter** to save the selected filters. Click **Save Filters**, type the name of the filters and click **Save**. After saved, the combined filters can be selected directly in the drop-down list.
6. To delete a filter condition, hover your mouse on that condition and then click the icon. To delete all filter conditions, click the icon on the right side of the row.

Note: "Virtual Router" is a required filter condition.

To clear the DNAT rule hit counts, take the following steps:

1. Select **Network** > **NAT** > **DNAT Hit Analysis**.
2. Click **Clear**.



In the Clearing NAT Hit Count dialog box, configure the following options.

Option	Description
All NATs	Clears the hit counts of all NAT rules.
NAT ID	Clears the hit counts of a specified NAT rule ID. You need to type the ID of the NAT rule into the text box.

3. Click **OK**.

You can also perform other operations:

- Click the icon to delete the NAT rule.
- Click the icon to disable the NAT rule.

iQoS

System provides iQoS (intelligent quality of service) that manages and optimizes network bandwidth, as well as improves users' network experience and bandwidth resource utilization.

iQoS is used to provide different priorities to different traffic, in order to control the delay and flapping, and decrease the packet loss rate. iQoS can assure the normal transmission of critical business traffic when the network is overloaded or congested. iQoS is controlled by license. To use iQoS, apply and install the iQoS license.

Pipes and Traffic Control Levels

System supports two-level traffic control: level-1 control and level-2 control. In each level, the traffic control is implemented by pipes.

Pipes

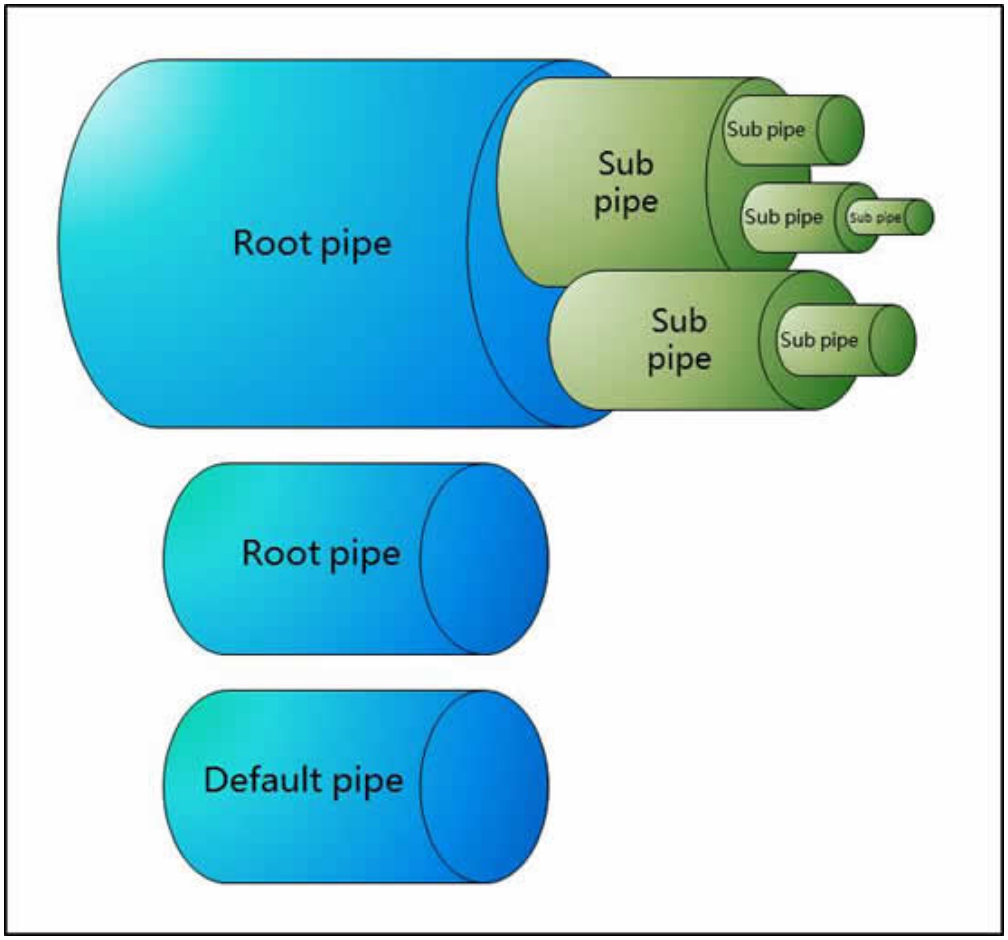
By configuring pipes, the devices implement iQoS. Pipe, which is a virtual concept, represents the bandwidth of transmission path. System classifies the traffic by using the pipe as the unit, and controls the traffic crossing the pipes according to the actions defined for the pipes. For all traffic crossing the device, they will flow into virtual pipes according to the traffic matching conditions they match. If the traffic does not match any condition, they will flow into the default pipe predefined by system.

Pipes, except the default pipe, include two parts of configurations: traffic matching conditions and traffic management actions:

- Traffic matching conditions: Defines the traffic matching conditions to classify the traffic crossing the device into matched pipes. System will limit the bandwidth to the traffic that matches the traffic matching conditions. You can define multiple traffic matching conditions to a pipe. The logical relation between each condition is OR. When the traffic matches a traffic matching condition of a pipe, it will enter this pipe.
- Traffic management actions: Defines the actions adopted to the traffic that has been classified to a pipe. The data stream control includes the forward control and the backward control. Forward control controls the traffic that flows from the source to the destination; backward control controls the traffic flows from the destination to the source.

To provide flexible configurations, system supports the multiple-level pipes. Configuring multiple-level pipes can limit the bandwidth of different applications of different users. This can ensure the bandwidth for the key services and users. Pipes

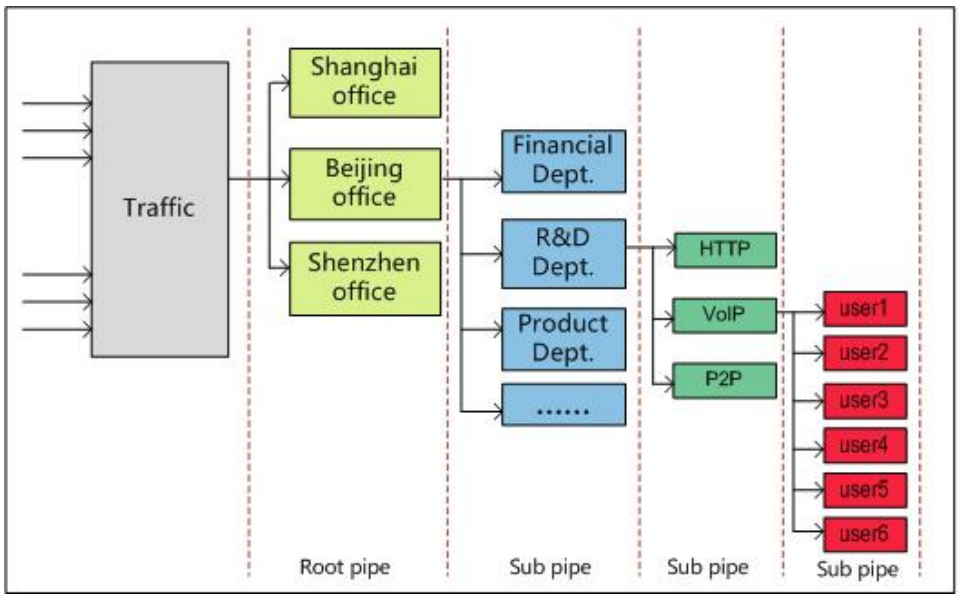
can be nested to at most four levels. Sub pipes cannot be nested to the default pipe. The logical relation between pipes is shown as below:



- You can create multiple root pipes that are independent. At most three levels of sub pipes can be nested to the root pipe.
- For the sub pipes at the same level, the total of their minimum bandwidth cannot exceed the minimum bandwidth of their upper-level parent pipe, and the total of their maximum bandwidth cannot exceed the maximum bandwidth of their upper-level parent pipe.
- If you have configured the forward or backward traffic management actions for the root pipe, all sub pipes that belong to this root pipe will inherit the configurations of the traffic direction set on the root pipe.
- The root pipe that is only configured with the backward traffic management actions cannot work.

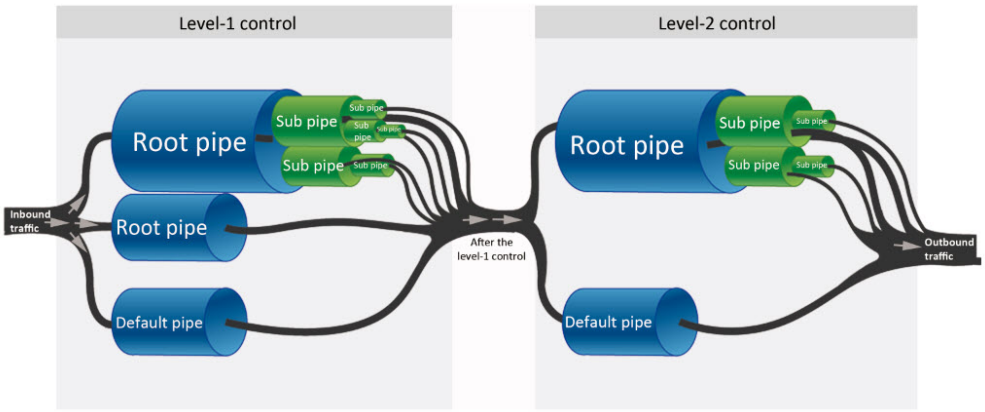
The following chart illustrates the application of multiple-level pipes in a company. The administrator can create the following pipes to limit the traffic:

1. Create a root pipe to limit the traffic of the office located in Beijing.
2. Create a sub pipe to limit the traffic of its R&D department.
3. Create a sub pipe to limit the traffic of the specified applications so that each application has its own bandwidth.
4. Create a sub pipe to limit the traffic of the specified users so that each user owns the defined bandwidth when using the specified application.



Traffic Control Levels

System supports two-level traffic control: level-1 control and level-2 control. In each level, the traffic control is implemented by pipes. Traffic that is dealt with by level-1 control flows into the level-2 control, and then system performs the further management and control according to the pipe configurations of level-2 control. After the traffic flowing into the device, the process of iQoS is shown as below:



According to the chart above, the process of traffic control is described below:

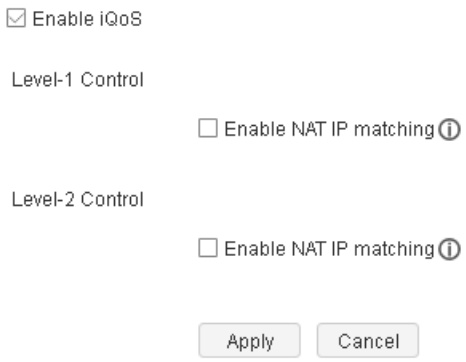
1. The traffic first flows into the level-1 control, and then system classifies the traffic into different pipes according to the traffic matching conditions of the pipe of level-1 control. The traffic that cannot match any pipe will be classified into the default pipe. If the same conditions are configured in different root pipes, the traffic will first match the root pipe listed at the top of the Level-1 Control list in the **Network** > **iQoS** page. After the traffic flows into the root pipe, system classifies the traffic into different sub pipes according to the traffic matching conditions of each sub pipe.
2. According to the traffic management actions configured for the pipes, system manages and controls the traffic that matches the traffic matching conditions.
3. The traffic dealt with by level-1 control flows into the level-2 control. System manages and controls the traffic in level-2 control. The principles of traffic matching, management and control are the same as the one of the level-1 control.
4. Complete the process of iQoS.

Enabling iQoS

To enable iQoS, take the following steps:

1. Select **Policy** > **iQoS** > **Configuration**.

2. Select the **Enable iQoS** check box.



3. If you select the **Enable NAT IP matching** check box in **Level-1 Control** or **Level-2 Control**, system will use the IP addresses between the source NAT and the destination NAT as the matching items. If the matching is successful, system will limit the speed of these IP addresses.

> **Note:** Before enabling NAT IP matching, you should configure the NAT rules. Otherwise, the configuration will not take effect.

4. Click **Apply** to save the configurations.

Configuring iQoS

By using pipes, devices implement iQoS to manage and optimize network bandwidth. Pipes in different traffic control levels will take effect in different stages.

Configuring pipes includes the following sections:

1. Enable iQoS. Select **Network** > **iQoS** > **Configuration** to enable this function.

2. Create the traffic matching conditions, which are used to capture the traffic that matches these conditions. If configuring multiple traffic matching conditions for a pipe, the logical relation between each condition is OR.

3. Create a white list according to your requirements. After the white list is created, system will not perform iQoS on the specified traffic in the list. Meanwhile, only root pipe and the default pipe support the white list.

4. Specify the traffic management actions, which are used to deal with the traffic that is classified into a pipe.

5. Specify the schedule. The pipe will take effect during the specified time period.

Basic Operations

Select **Network** > **iQoS** > **Policy** to enter the **Policy** page.

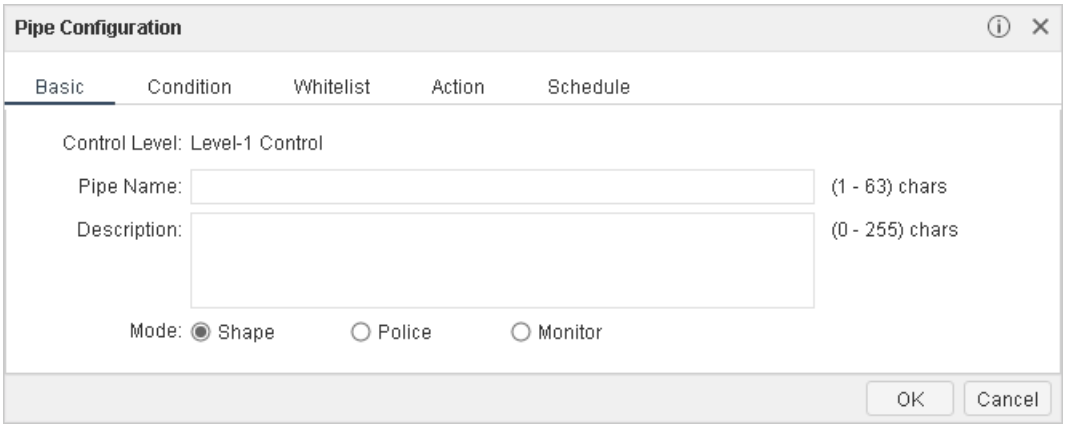
You can perform the following actions in this page:

- Disable the level-2 traffic control: Click **Disable second level control**, then the pipes in the level-2 traffic control will not take effect. The Level-2 Control tab will not appears in this page.
- View pipe information: The pipe list displays the name, mode, action, schedule, and the description of the pipes.
  - Click the icon to expand the root pipe and display its sub pipes.
  - Click the icon to view the condition settings.
  - Click the icon to view the white list settings.
  - represents the root pipe is usable, represents the root pipe is unusable, represents the sub pipe is usable, represents the sub pipe is unusable, flow-two the gray text represents the pipe is disabled.
- Create a root pipe: Select the **Level-1 Control** or **Level-2 Control** tab, then click **New** to create a new root pipe.
- Create a sub pipe: Click the icon of the root pipe or the sub pipe to create the corresponding sub pipe.
- Edit a pipe: Click **Edit** to edit the selected pipe.
- Enable a pipe: Click **Enable** to enable the selected pipe. By default, the newly-created pipe will be enabled.
- Disable a pipe: Click **Disable** to disable the selected pipe. The disabled pipe will not take effect.
- Delete a pipe: Click **Delete** to delete the selected pipe. The default pipe cannot be deleted.

Configuring a Pipe

To configure a pipe, take the following steps:

1. According to the methods above, create a root pipe or sub pipe. The Pipe Configuration dialog box will appear.



2. In the Basic tab, specify the basic pipe information.

Option	Description
Parent Pipe/Control Level	Displays the control level or the parent pipe of the new pipe.
Pipe Name	Specify a name for the new pipe.
Description	Specify the description of this pipe.
Mode	Shape, Police, or Monitor: • The Shape mode can limit the data transmission rate and smoothly forward the traffic. This mode supports the bandwidth borrowing and priority adjusting for the traffic within the root pipe. • The Police mode will drop the traffic that exceeds the bandwidth limit. This mode does not support the bandwidth borrowing and priority adjusting, and cannot guarantee the minimum bandwidth. • The Monitor mode will monitor the matched traffic, generate the statistics, and will not control the traffic. • Bandwidth borrowing: All of the sub pipes in a root pipe can lend their idle bandwidth to the pipes that are lacking bandwidth. The prerequisite is that their bandwidth must be enough to forward the traffic in their pipes.

Option	Description
	• Priority adjusting: When there is traffic congestion, system will arrange the traffic to enter the waiting queue. You can set the traffic to have higher priority and system will deal with the traffic in order of precedence.

3. In the Condition tab, click **New**. In the Condition Configuration dialog box, configure the corresponding options.

Option	Description
Type	Select the IP type, including IPv4 and IPv6. Only the IPv6 firmware supports to configure IPv6 type IP. If IPv6 is selected, all the IP/netmask, IP range, address entry configured should be in the IPv6 format.
Source Information	
Zone	Specify the source zone of the traffic. Select the zone name from the drop-down list.
Interface	Specify the source interface of the traffic. Select the interface name from the drop-down list and click **OK**. To delete the selected interface, click **Clear**.
Address	Specify the source address of the traffic. 1. Select an address type from the **Address** drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click → to add the addresses to the right pane. 4. After adding the desired addresses, click the blank area in this dialog box to complete the address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click **Add** to create a new address entry. • The default address configuration is any. To restore the configuration

Option	Description
	to this default one, select the **any** check box.
Destination Information	
Zone	Specify the destination zone of the traffic. Select the zone name from the drop-down list.
Interface	Specify the destination interface of the traffic. Select the interface name from the drop-down list and click **OK**. To delete the selected interface, click **Clear**.
Address	Specify the destination address of the traffic. 1. Select an address type from the **Address** drop-down list. 2. Select or type the source addresses based on the selected type. 3. Click → to add the addresses to the right pane. 4. After adding the desired addresses, click the blank area in this dialog box to complete the address configuration. You can also perform other operations: • When selecting the **Address Book** type, you can click **Add** to create a new address entry. • The default address configuration is any. To restore the configuration to this default one, select the **any** check box.
User Information	Specify a user or user group that the traffic belongs to. 1. From the **User** drop-down list, select the AAA server to which the users and user groups belong. 2. Based on different types of AAA server, you can execute one or more actions: search a user/user group/role, expand the user/user group list, and enter the name of the user/user group.

Option	Description
	3. After selecting users/user groups/roles, click  to add them to the right pane. 4. After adding the desired objects, click the blank area in this dialog box to complete the user information configuration.
Service	Specify a service or service group to which the traffic belongs. 1. From the **Service** drop-down list, select a type: Service or Service Group. 2. You can search the desired service/service group, or expand the service/service group list. 3. After selecting the desired services/service groups, click  to add them to the right pane. 4. After adding the desired objects, click the blank area in this dialog box to complete the service configuration. You can also perform other operations: • To add a new service or service group, click **Add**. • The default service configuration is any. To restore the configuration to this default one, select the **any** check box.
Application	Specify an application, application group, or application filters that the traffic belongs to. 1. From the **Application** drop-down list, you can search the desired application/application group/application filter, or expand the list of applications/application groups/application filters. 2. After selecting the desired applications/application groups/application filters, click  to add them to the right pane.

Option	Description
	3. After adding the desired objects, click the blank area in this dialog box to complete the application configuration. To create a new application group or application filter, click **New AppGroup** or **New AppFilter**.
Advanced	
VLAN	Specify the VLAN information of the traffic.
TOS	Specify the TOS fields of the traffic; or click **Configure** to specify the TOS fields of the IP header of the traffic in the TOS Configuration dialog box. • Precedence: Specify the precedence. • Delay: Specify the minimum delay. • Throughput: Specify the maximum throughput. • Reliability: Specify the highest reliability. • Cost: Specify the minimum cost. • Reserved: Specify the normal service.
TrafficClass	Specify the TOS fields of the traffic.

4. If you are configuring root pipes, you can specify the white list settings based on the description of configuring conditions

5. In the Action tab, configuring the corresponding actions.

Forward (From source to destination)	
The following configurations control the traffic that flows from the source to the destination. For the traffic that matches the conditions, system will perform the corresponding actions.	
Pipe Bandwidth	When configuring the root pipe, specify the pipe bandwidth. When configuring the sub pipe, specify the maximum bandwidth and the minimum bandwidth of the pipe:

	• Min Bandwidth: Specify the minimum bandwidth. If you want this minimum bandwidth to be reserved for the sub pipe, select **Enable Reserved Bandwidth**. This reserved minimum bandwidth cannot be borrowed. • Max Bandwidth: Specify the maximum bandwidth.

Limit type	Specify the maximum bandwidth and minimum bandwidth of the pipe for each user/IP:
	• Type: Select the type of the bandwidth limitation: **No Limit**, **Limit Per IP**, or **Limit Per User**.
	  • **No Limit** represents that system will not limit the bandwidth for each IP or each user.
	  • **Limit Per IP** represents that system will limit the bandwidth for each IP. After selecting the radio button, in the Limit by section, select **Source IP** and specify the minimum and maximum bandwidth for each source IP in this pipe; or select **Destination IP** and specify the minimum and maximum bandwidth for each destination IP in this pipe.
	  • **Limit Per User** represents that system will limit the bandwidth for each user. After selecting the radio button, in the Limit by section, specify the minimum/maximum bandwidth for each user in this type.
	• When configuring the root pipe, you can select the **Enable Average Bandwidth** check box to make each source IP, destination IP, or user to share an average bandwidth.

Limit by	When the Limit type is **Limit Per IP** or **Limit Per User**, you need to specify the minimum bandwidth and the maximum bandwidth for each user or each IP:

	• Min Bandwidth: Specify the minimum bandwidth. • Max Bandwidth: Specify the maximum bandwidth. • Delay: Specify the delay time, whose value ranges from 1 second to 3600 seconds. After this parameter is specified, the maximum bandwidth limit of each IP/user will not take effect within the delay time range.
Priority	In the Advanced section, specify the priority for the pipes. Select a number, between 0 and 7, from the drop-down list. The smaller the value is, the higher the priority will be. When a pipe has higher priority, system will first deal with the traffic in it and borrow the extra bandwidth from other pipes for it. The priority of the default pipe is 7.
TOS	In the Advanced section, specify the TOS fields of the traffic; or click **Configure** to specify the TOS fields of the IP header of the traffic in the pop-up TOS Configuration dialog box. • Precedence: Specify the precedence. • Delay: Specify the minimum delay. • Throughput: Specify the maximum throughput. • Reliability: Specify the highest reliability. • Cost: Specify the minimum monetary cost. • Reserved: Specify the normal service.
Limit Opposite Bandwidth	In the Advanced section, select the **Limit Opposite Bandwidth** check box to configure the value of the limit-strength. This function is disabled by default. After this function is enabled, the device will be allocated with the traffic in proportional to the bandwidth allocated to the user to reduce packet loss on the device. The default limit is 1, and the value range is 1 to 8. The larger the value is, the greater the limit is, and the lesser packet loss will be.

	Note: This function can only be enabled in one direction (i.e., forward or backward) and only be supported by the pipes at the last level.
Backward (From condition's destination to source)	
The following configurations control the traffic that flows from the destination to the source. For the traffic that matches the conditions, system will perform the corresponding actions.	
Pipe Bandwidth	When configuring the root pipe, specify the pipe bandwidth. When configuring the sub pipe, specify the maximum bandwidth and the minimum bandwidth of the pipe: • Min Bandwidth: Specify the minimum bandwidth. If you want this minimum bandwidth to be reserved for the sub pipe, select **Enable Reserved Bandwidth**. This reserved minimum bandwidth cannot be borrowed. • Max Bandwidth: Specify the maximum bandwidth.

Limit type	Specify the maximum bandwidth and minimum bandwidth of the pipe for each user/IP:
	• Type: Select the type of the bandwidth limitation: **No Limit**, **Limit Per IP**, or **Limit Per User**.
	  • **No Limit** represents that system will not limit the bandwidth for each IP or each user.
	  • **Limit Per IP** represents that system will limit the bandwidth for each IP. After selecting the radio button, in the Limit by section, select **Source IP** and specify the minimum and maximum bandwidth for each source IP in this pipe; or select **Destination IP** and specify the minimum and maximum bandwidth for each destination IP in this pipe.
	  • **Limit Per User** represents that system will limit the bandwidth for each user. After selecting the radio button, in the Limit by

	section, specify the minimum/maximum bandwidth for each user in this type. • When configuring the root pipe, you can select the **Enable Average Bandwidth** check box to make each source IP, destination IP, or user to share an average bandwidth.
Limit by	When the Limit type is **Limit Per IP** or **Limit Per User**, you need to specify the minimum bandwidth and the maximum bandwidth for each user or each IP: • Min Bandwidth: Specify the minimum bandwidth. • Max Bandwidth: Specify the maximum bandwidth. • Delay: Specify the delay time, whose value ranges from 1 second to 3600 seconds. After this parameter is specified, the maximum bandwidth limit of each IP/user will not take effect within the delay time range.
Priority	In the Advanced section, specify the priority for the pipes. Select a number, between 0 and 7, from the drop-down list. The smaller the value is, the higher the priority will be. When a pipe has higher priority, system will first deal with the traffic in it and borrow the extra bandwidth from other pipes for it. The priority of the default pipe is 7.
ToS	In the Advanced section, specify the TOS fields of the traffic; or click **Configure** to specify the TOS fields of the IP header of the traffic in the pop-up TOS Configuration dialog box. • Precedence: Specify the precedence. • Delay: Specify the minimum delay. • Throughput: Specify the maximum throughput. • Reliability: Specify the highest reliability. • Cost: Specify the minimum monetary cost.

	• Reserved: Specify the normal service.
Limit Opposite Bandwidth	In the Advanced section, select the **Limit Opposite Bandwidth** check box to configure the value of the limit-strength. This function is disabled by default. After this function is enabled, the device will be allocated with the traffic in proportional to the bandwidth allocated to the user to reduce packet loss on the device. The default limit is 1, and the value range is 1 to 8. The larger the value is, the greater the limit is, and the lesser packet loss will be. Note: This function can only be enabled in one direction (i.e., forward or backward) and only be supported by the pipes at the last level.

6. In the Schedule tab, configure the time period when the pipe takes effect.

Schedule	
Schedule	Specify the schedule. The pipe will take effect within the time period specified by the schedule. To create a new schedule, click **New Schedule**.

7. Click **OK** to save the settings.

Viewing Statistics of Pipe Monitor

To view the statistics of pipe monitor, see "iQoS Monitor" on Page 468.

Session Limit

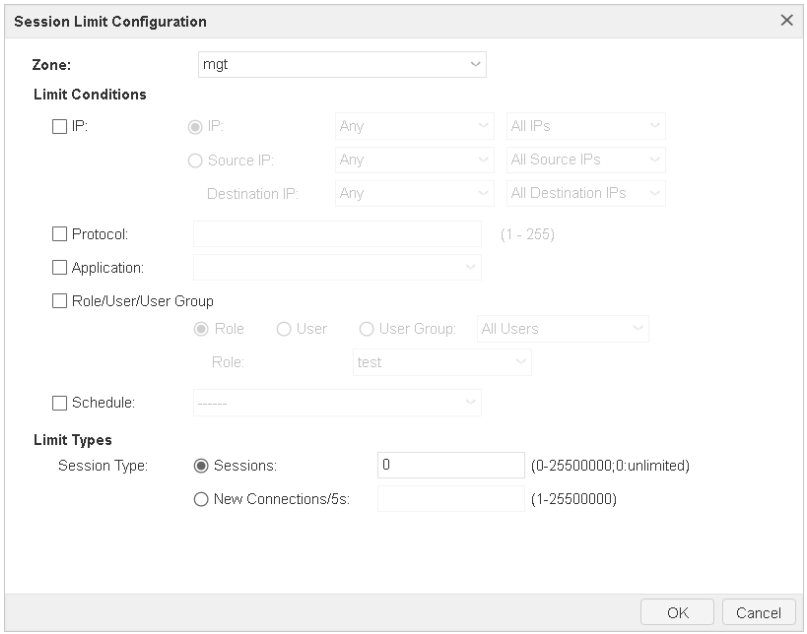
The devices support zone-based session limit function. You can limit the number of sessions and control the session rate to the source IP address, destination IP address, specified IP address, applications or role/user/user group in security zones, thereby protecting the connection table from DoS attacks and controlling the bandwidth of some applications, such as IM or P2P.

Configuring a Session Limit Rule

To configure a session limit rule, take the following steps:

1. Select **Firewall** > **Session Limit**.

2. Click **New**, and the Session Limit Configuration dialog box will appear.



3. Select the zone where the session limit rule is located from the **Zone** drop-down list.

4. Configure the limit conditions.

IP	
Select the **IP** check box to configure the IP limit conditions.	
IP	Select the **IP** radio button, and specify the IP address entry, and then

IP	
	click **OK** to limit the number of sessions of the IP address segment in the zone. To clear the selected address entry, click **Clear** in the drop-down list. • Select **All IPs** from the drop-down list to limit the maximum number of sessions or the number of sessions created per 5 seconds to all IP addresses. • Select **Per IP** from the drop-down list to limit the maximum number of sessions to each IP address.
Source IP	Select the **Source IP** radio button, and specify the source IP address entry and destination IP address entry, and then click **OK**. To clear the selected address entry, click **Clear** in the drop-down list. When the session's source IP and destination IP are both within the specified range, system will limit the number of sessions/new sessions as follows: • Select **Per Source IP** from the drop-down list to limit the maximum number of sessions or the number of sessions created per 5 seconds to each source IP address. • Select **Per Destination IP** from the drop-down list to limit the maximum number of sessions or the number of sessions created per 5 seconds to each destination IP address.
Protocol	
Protocol	Select the **Protocol** check box, and type the value for the protocol into the text box.
Application	
Application	Select the **Application** check box to enable the application limit condition. And Select the type of the application whose number of sessions needs to be limited.

IP	
Role/User/User Group	
Select the **Role/User/User Group** check box to configure the corresponding limit conditions.	
Role	Select the **Role** radio button and a role from the **Role** drop-down list to limit the number of sessions of the selected role.
User	Select the **User** radio button and a user from the **User** drop-down list, and then click **OK** to limit the number of sessions of the selected user. You can select the AAA server to which the user belongs from the **AAA Server** drop-down list. To clear the selected user, click **Clear** in the drop-down list.
User Group	Select the **User Group** radio button and a user group from the **User Group** drop-down list, and then click **OK** to limit the number of sessions of the selected user group. You can the AAA server to which the user group belongs from the **AAA Server** drop-down list. To clear the selected user group, click **Clear** in the drop-down list. • Next to the **User Group** radio button, select **All Users** to limit the maximum number of sessions or the number of sessions created per 5 seconds to all of the users in the user group. • Next to the **User Group** radio button, select **Per User** to limit the maximum number of sessions to each user.
Schedule	
Schedule	Select the **Schedule** check box and choose a schedule you need from the drop-down list to make the session limit rule take effect within the time period specified by the schedule.

5. Configure the limit types.

Session Type	
Session Number	Select the radio button and type a value into the text box to specify the maximum number of sessions. The value of 0 indicates no limitation

Session Type	
New Connections/5s	Select the radio button and type a value into the text box to specify the maximum number of sessions created per 5 seconds.

6. Click **OK** to save the settings.

7. Click **Switch Mode** to select a matching mode:
   If you select **Use the Minimum Value** and an IP address matches multiple session limit rules, the maximum number of sessions of this IP address is limited to the minimum number of sessions of all matched session limit rules;
   If you select **Use the Maximum Value** and an IP address matches multiple session limit rules, the maximum number of sessions of this IP address is the maximum number of sessions of all matched session limit rules.

Clearing Statistic Information

After configuring a session limit rule, the sessions which exceed the maximum number of sessions will be dropped. You can clear the statistical information of the dropped sessions of specified session limit rule according to your need.

To clear statistic information, take the following steps:

1. Select **Firewall** > **Session Limit**.

2. Select the rule whose session's statistical information you want to clear.

3. Click **Clear**.

Chapter 12 VPN

System supports the following VPN functions:

- "IPSec VPN" on Page 413: IPSec is a security framework defined by the Internet Engineering Task Force (IETF) for securing IP communications. It is a Layer 3 virtual private network (VPN) technology that transmits data in a secure tunnel established between two endpoints.
- IKEv2 VPN: Configurations related to IKEv2 VPN.

IPSec VPN

IPSec is a widely used protocol suite for establishing a VPN tunnel. IPSec is not a single protocol, but a suite of protocols for securing IP communications. It includes Authentication Headers (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE) and some authentication methods and encryption algorithms. IPSec protocol defines how to choose the security protocols and algorithms, as well as the method for exchanging security keys among communicating peers, while offering the upper layer protocols with network security services, including access control, data source authentication, data encryption, etc.

Basic Concepts

- Security association
- Encapsulation modes
- Establishing SA
- Using IPSec VPN

Security Association (SA)

IPSec provides encrypted communication between two peers which are known as IPSec ISAKMP gateways. Security Association (SA) is the basis and essence of IPSec. SA defines some factors of communication peers like the protocols, operational modes, encryption algorithms (DES, 3DES, AES-128, AES-192 and AES-256), shared keys of data protection in particular flows and the life cycle of SA, etc.

SA is used to process data flow in one direction. Therefore, in a bi-directional communication between two peers, you need at least two security associations to protect the data flow in both of the directions.

There are two ways to establish SA: manual and IKE auto negotiation (ISAKMP).

Encapsulation Modes

IPSec supports the following IP packet encapsulation modes:

- Tunnel mode - IPSec protects the entire IP packet, including both the IP header and the payload. It uses the entire IP packet to calculate an AH or ESP header, and then encapsulates the original IP packet and the AH or ESP header with a

new IP header. If you use ESP, an ESP trailer will also be encapsulated. Tunnel mode is typically used for protecting gateway-to-gateway communications.

- Transport mode - IPSec only protects the IP payload. It only uses the IP payload to calculate the AH or ESP header, and inserts the calculated header between the original IP header and payload. If you use ESP, an ESP trailer will also be encapsulated. The transport mode is typically used for protecting host-to-host or host-to-gateway communications.

Establishing SA

Manually configuring SA is complicated as all the information will be configured by yourself and some advanced features of IPSec are not supported (e.g. timed refreshing), but the advantage is that manually configured SA can independently fulfill IPSec features without relying on IKE. This method applies to a situation with a small number of devices or an environment of static IP addresses.

IKE auto negotiation method is comparatively simple. You only need to configure information of IKE negotiation and leave the rest jobs of creating and maintaining SA to the IKE auto negotiation function. This method is for medium and large dynamic networks. Establishing SA by IKE auto negotiation consists of two phases. The Phase 1 negotiates and creates a communication channel (ISAKMP SA) and authenticates the channel to provide confidentiality, data integrity and data source authentication services for further IKE communication; the Phase 2 creates IPSec SA using the established ISAKMP. Establishing SA in two phases can speed up key exchanging.

Using IPSec VPN

To apply VPN tunnel feature in the device, you can use policy-based VPN or route-based VPN, so as to achieve the encryption, decryption and secure transmission for the traffic.

- Policy-based VPN - Applies the configured VPN tunnel to a policy so that the data flow which conforms to the policy settings can pass through the VPN tunnel.
- Route-based VPN - Binds the configured VPN tunnel to the tunnel interface and define the next hop of static route as the tunnel interface.

Related Topics:

- "Configuring an IKE VPN" on Page 416
- "Configuring a Manual Key VPN" on Page 430
- "Configuring IPSec-XAUTH Address Pool" on Page 435
- "Viewing IPSec VPN Monitoring Information" on Page 433

Configuring an IKE VPN

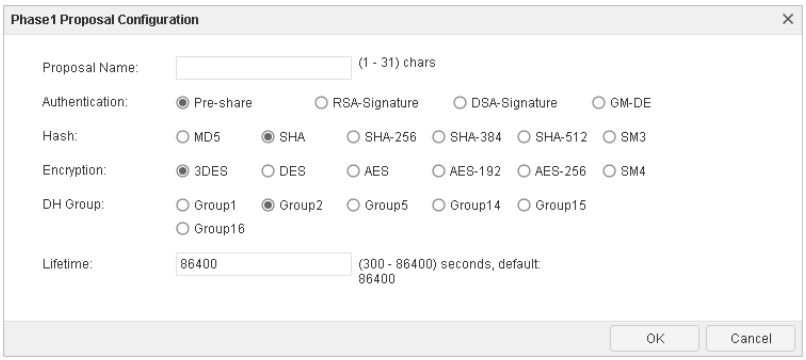
IKE auto negotiation method is comparatively simple. You only need to configure information of IKE negotiation and leave the rest jobs of creating and maintaining SA to the IKE auto negotiation function. This method is for medium and large dynamic network. Establishing SA by IKE auto negotiation consists of two phases. The Phase 1 negotiates and creates a communication channel (ISAKMP SA) and authenticates the channel to provide confidentiality, data integrity and data source authentication services for further IKE communication; the Phase 2 creates IPSec SA using the established ISAKMP. Establishing SA in two phases can speed up key exchanging.

To configure an IKE VPN, you need to confirm the Phase 1 proposal, the Phase 2 proposal, and the VPN peer. After confirming these three contents, you can proceed with the configuration of IKE VPN settings.

Configuring a Phase 1 Proposal

The P1 proposal is used to negotiate the IKE SA. To configure a P1 proposal, take the following steps:

1. Select **Network** > **VPN** > **IKEv1 and Manual**.
2. In the IKEv1 VPN Configuration section, click the **P1 Proposal** tab.
3. Click **New**.



In the Phase1 Proposal Configuration dialog box, configure the corresponding options.

Option	Description
Proposal Name	Specify the name of the Phase1 proposal.
Authentication	Specify the IKE identity authentication method. IKE identity authentication is used to verify the identities of both communication parties.

Option	Description
	There are four methods for authenticating identity: pre-shared key, RSA signature, DSA signature and GM-DE. The default option is pre-shared key. For the pre-shared key method, the key is used to generate a secret key and the keys of both parties must be the same so that it can generate the same secret keys.
Hash	Specify the authentication algorithm for Phase1. Select the algorithm you want to use. • MD5 - Uses MD5 as the authentication algorithm. Its hash value is 128-bit. • SHA - Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm. • SHA-256 - Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 - Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit. • SHA-512 - Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit.
Encryption	Specify the encryption algorithm for Phase1. • 3DES - Uses 3DES as the encryption algorithm. The key length is 192-bit. This is the default encryption algorithm. • DES - Uses DES as the encryption algorithm. The key length is 64-bit. • AES - Uses AES as the encryption algorithm. The key length is 128-bit. • AES-192 - Uses 192-bit AES as the encryption algorithm. The key length is 192-bit.

Option	Description
	• AES-256 - Uses 256-bit AES as the encryption algorithm. The key length is 256-bit.
DH Group	Specify the DH group for Phase1. • Group1 - Uses Group1 as the DH group. The key length is 768-bit (MODP Group). • Group2 - Uses Group2 as the DH group. The key length is 1024-bit (MODP Group). Group2 is the default value. • Group5 - Uses Group5 as the DH group. The key length is 1536-bit (MODP Group). • Group14 - Uses Group14 as the DH group. The key length is 2048-bit (MODP Group). • Group15 - Uses Group15 as the DH group. The key length is 3072-bit (MODP Group). • Group16 - Uses Group16 as the DH group. The key length is 4096-bit (MODP Group).
Lifetime	Specify the lifetime of SA Phase1. The value range is 300 to 86400 seconds. The default value is 86400. Type the lifetime value into the **Lifetime** box. When the SA lifetime runs out, the device will send a SA P1 deleting message to its peer, notifying that the P1 SA has expired and it requires a new SA negotiation.

4. Click **OK** to save the settings.

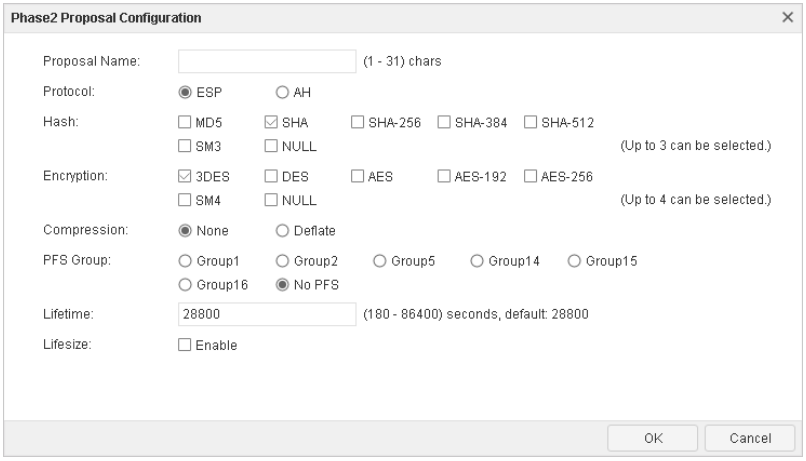
Configuring a Phase 2 Proposal

The P2 proposal is used to negotiate the IPSec SA. To configure a P2 proposal, take the following steps:

1. Select **Network** > **VPN** > **IKEv1 and Manual**.

2. In the IKEv1 VPN Configuration section, click the **P2 Proposal** tab.

3. Click **New**.



In the Phase2 Proposal Configuration dialog box, configure the corresponding options.

Option	Description
Proposal Name	Specify the name of the Phase2 proposal.
Protocol	Specify the protocol type for Phase2. The options are ESP and AH. The default value is ESP.
Hash	Specify the preferred authentication algorithm for Phase2. You can specify up to 3 authentication algorithms. • MD5 - Uses MD5 as the authentication algorithm. Its hash value is 128-bit. • SHA - Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm. • SHA-256 - Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 - Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit. • SHA-512 - Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit. • NULL - No authentication.

Option	Description
Encryption	Specify the preferred encryption algorithm for Phase2. You can specify up to 4 encryption algorithms. • 3DES - Uses 3DES as the encryption algorithm. The key length is 192-bit. This is the default encryption algorithm. • DES - Uses DES as the encryption algorithm. The key length is 64-bit. • AES - Uses AES as the encryption algorithm. The key length is 128-bit. • AES-192 - Uses 192-bit AES as the encryption algorithm. The key length is 192-bit. • AES-256 - Uses 256-bit AES as the encryption algorithm. The key length is 256-bit. • NULL - No encryption.
Compression	Specify the compression algorithm for Phase2. By default, no compression algorithm is used.
PFS Group	Specify the PFS function for Phase2. PFS is used to protect DH algorithm. • Group1 - Uses Group1 as the DH group. The key length is 768-bit (MODP Group). • Group2 - Uses Group2 as the DH group. The key length is 1024-bit (MODP Group). • Group5 - Uses Group5 as the DH group. The key length is 1536-bit (MODP Group). • Group14 - Uses Group14 as the DH group. The key length is 2048-bit (MODP Group).

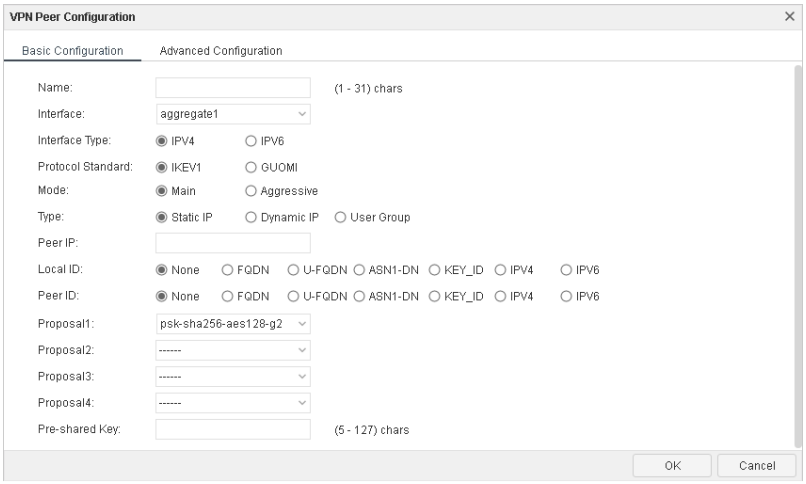
Option	Description
	• Group15 - Uses Group16 as the DH group. The key length is 3072-bit (MODP Group). • Group16 - Uses Group16 as the DH group. The key length is 4096-bit (MODP Group). • No PFS - Disables PFS. This is the default value.
Lifetime	You can evaluate the lifetime by two standards which are the time length and the traffic volume. Type the lifetime length of the P2 proposal into the box. The value range is 180 to 86400 seconds. The default value is 28800.
Lifesize	Select **Enable** to enable the P2 proposal traffic-based lifetime. By default, this function is disabled. • Lifesize - Specify the traffic volume of lifetime. The value range is 1800 to 4194303 KBs. The default value is 1800. Type the traffic volume value into the text box.

4. Click **OK** to save the settings.

Configuring a VPN Peer

To configure a VPN peer, take the following steps:

1. Select **Network** > **VPN** > **IKEv1 and Manual**.
2. In the IKEv1 VPN Configuration section, click the **VPN Peer List** tab.
3. Click **New**.



In the VPN Peer Configuration dialog box, configure the corresponding options.

Basic Configuration	
Name	Specify the name of the ISAKMP gateway.
Interface	Specify the interface bound to the ISAKMP gateway.
Interface Type	Select the interface type, including IPv4 or IPv6.
Protocol Standard	Specify the protocol standard, including IKEv1 and GUOMI. The default protocol standard is IKEv1. If you select GUOMI, specify the version: Note: If you specify the version as 1.0 or 1.1, the version of the two peers which negotiate with each other should be the same, or system will fail to negotiate.
Mode	Specify the mode of IKE negotiation. There are two IKE negotiation modes: **Main** and **Aggressive**. The main mode is the default mode. The aggressive mode cannot protect identity. You have no choice but use the aggressive mode in the situation where the IP address of the center device is static and the IP address of client device is dynamic.
Type	Specify the type of the peer IP. • If the peer IP is static, select **Static IP** and type the IP address into the **Peer IP** box;

Basic Configuration	
	• If the peer IP type is user group, select **User Group** and select the AAA server you need from the **AAA Server** drop-down list; • If the peer IP is dynamic, select **Dynamic IP**.
Local ID	Specify the local ID. System supports five types of ID: FQDN, U-FQDN, Asn1dn (only for license), KEY-ID and IP. Select the ID type you want, and then type the content for this ID into the **Local ID** box or the **Local IP** box.
Peer ID	Specify the peer ID. System supports five types of ID: FQDN, U-FQDN, Asn1dn (only for license), KEY-ID and IP. Select the ID type you want, and then type the content for this ID into the **Peer ID** box or the **Peer IP** box. If you want to use the Radius server for authentication, you need to select the **Wildcard** check box.
Proposal1	Specify a P1 proposal for the ISAKMP gateway. You can define up to four P1 proposals for an ISAKMP gateway.
Proposal2	Specify a P1 proposal for the ISAKMP gateway. You can define up to four P1 proposals for an ISAKMP gateway.
Proposal3	Specify a P1 proposal for the ISAKMP gateway. You can define up to four P1 proposals for an ISAKMP gateway.
Proposal4	Specify a P1 proposal for the ISAKMP gateway. You can define up to four P1 proposals for an ISAKMP gateway.
Pre-shared Key	If you choose to use pre-shared key to authenticate, type the key into the box.
Self-signed Trust Domain	If you choose to use RSA signature or DSA signature, select a trust domain.
Advanced Configuration	
Connection Type	Specify the connection type for the ISAKMP gateway, including: • Bidirectional - Specify that the ISAKMP gateway serves as both the

Basic Configuration	
	initiator and responder. This is the default value. • Initiator - Specify that the ISAKMP gateway serves as the initiator only. • Responder - Specify that the ISAKMP gateway serves as the responder only.
NAT Traversal	This option must be enabled when there is a NAT device in the IPSec or IKE tunnel and the device implements NAT. By default, this function is disabled.
Any Peer ID	Makes the ISAKMP gateway accept any peer ID and not check the peer IDs.
Generate Route	Select the **Enable** check box to enable the auto routing function. By default, this function is disabled. This function allows the device to automatically add routing entries which are from the center device to the branch, avoiding the problems caused by manual configured routing.
DPD	Select the **Enable** check box to enable the DPD (Delegated Path Discovery) function. By default, this function is disabled. When the responder does not receive the peer's packets for a long period, it can enable DPD and initiate a DPD request to the peer so that it can test if the ISAKMP gateway exists. • DPD Interval - The interval of sending DPD request to the peer. The value range is 1 to 10 seconds. The default value is 10 seconds. • DPS Retries - The times of sending DPD request to the peer. The device will keep sending discovery requests to the peer until it reaches the specified times of DPD retires. If the device does not receive response from the peer after the retry times, it will determine that the peer ISAKMP gateway is down. The value range is 1 to 10 times. The default value is 3.

Basic Configuration	
Description	Type the description for the ISAKMP gateway.
XAUTH Server	Select **Enable** to enable the XAUTH server in the device. Then select an address pool from the **Address Pool** drop-down list. After enabling the XAUTH server, the device can verify the users that try to access the IPSec VPN network by integrating the configured AAA server.

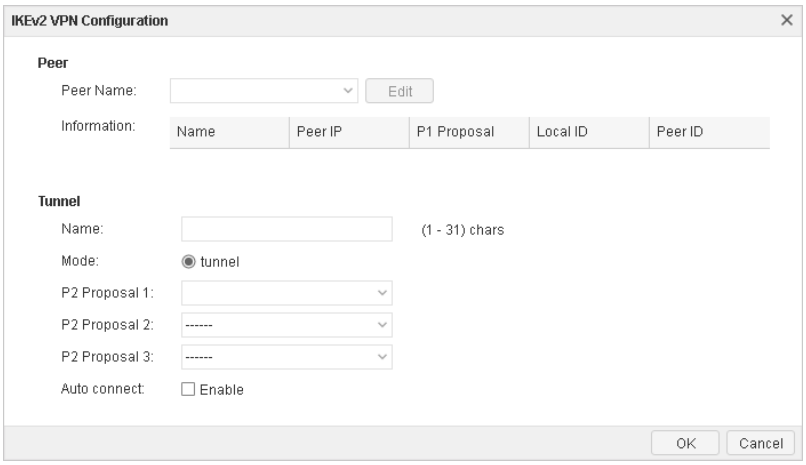
4. Click **OK** to save the settings.

Configuring an IKE VPN

Use IKE to negotiate IPSec SA automatically. To configure an IKE VPN, take the following steps:

1. Select **Network** > **VPN** > **IKEv1 and Manual**.

2. In the IKEv1 VPN Configuration section, click the **IKE VPN List** tab. Then click **New**, and the IKE VPN Configuration dialog box will appear.



In the Basic Configuration tab, configure the corresponding options.

Peer	
Peer Name	Specify the name of the ISAKMP gateway. To create an ISAKMP gateway, click **New** in the drop-down list; or to edit an ISAKMP gateway, click **Edit**.

Peer	
Information	Shows the information of the selected peer.
Tunnel	
Name	Type a name for the tunnel.
Mode	Specify the mode, including tunnel mode and transport mode.
P2 Proposal	Specify the P2 proposal for the tunnel.

Proxy ID	Specify ID of Phase 2 for the tunnel which can be Auto or Manual.
	• Auto - The Phase 2 ID is automatically designated.
	• Manual - The Phase 2 ID is manually designated. Manual configuration of P2 ID includes the following options:
	  • Local IP/Netmask - Specify the local ID of Phase 2.
	  • Remote IP/Netmask - Specify the Phase 2 ID of the peer device.
	  • Service - Specify the service. To create a new service, click **Add**.

In the Advanced Configuration tab, configure the corresponding options.

Option	Description
DNS1	Specify the IP address of the primary DNS server allocated to the client by the PnPVPN server.
DNS2	Specify the IP address of the backup DNS server allocated to the client by the PnPVPN server.
DNS3	Specify the IP address of the backup DNS server allocated to the client by the PnPVPN server.
DNS4	Specify the IP address of the backup DNS server allocated to the client by the PnPVPN server.
WINS1	Specify the IP address of the primary WINS server allocated to the client by the PnPVPN server.

Option	Description
WINS2	Specify the IP address of the backup WINS server allocated to the client by the PnPVPN server.
Enable Idle Time	Select the **Enable** check box to enable the idle time function. By default, this function is disabled. This time length is the longest time the tunnel can exist without traffic passing through. When the time is over, SA will be cleared.
DF-Bit	Specify whether to allow the forwarding device to execute IP packet fragmentation. The options are: • Copy - Copies the IP packet DF options from the sender directly. This is the default value. • Clear - Allows the device to execute packet fragmentation. • Set - Disallows the device to execute packet fragmentation.
Anti-Replay	Anti-replay is used to prevent hackers from attacking the device by resending the sniffed packets, i.e., the receiver rejects the obsolete or repeated packets. By default, this function is disabled. • Disable - Disables this function. This is the default value. • 32 - Specify the anti-replay window as 32. • 64 - Specify the anti-replay window as 64. • 128 - Specify the anti-replay window as 128. • 256 - Specify the anti-replay window as 256. • 512 - Specify the anti-replay window as 512.
Commit Bit	Select the **Enable** check box to make the corresponding party configure the commit bit function, which can avoid packet loss and time difference. However, commit bit may slow the responding speed.
Accept-all-proxy-ID	With this function enabled, the device which is working as the initiator

Option	Description
	will use the peer's ID as its Phase 2 ID in the IKE negotiation, and return the ID to its peer.
Auto Connect	Select the **Enable** check box to enable the auto connection function. By default, this function is disabled. The device has two methods of establishing SA: auto and intrigued traffic mode. When it is in auto mode, the device will check the SA status every 60 seconds and initiate a negotiation request when SA is not established; when it is in intrigued traffic mode, the tunnel will send negotiation request only when there is traffic passing through the tunnel. By default, the intrigued traffic mode is enabled.
Tunnel Route	This item can be modified only after this IKE VPN is created. Click **Choose** to add one or more tunnel routes in the pop-up Tunnel Route Configuration dialog box. You can add up to 128 tunnel routes.
Description	Type the description for the tunnel.
Tunnel State Notify	Select the **Enable** check box to enable the tunnel state notification function. With this function enabled, for route-based VPN, system will inform the routing module about the information of the disconnected VPN tunnel and update the tunnel route once any VPN tunnel disconnection is detected; for policy-based VPN, system will inform the policy module about the information of the disconnected VPN tunnel and update the tunnel policy once any VPN tunnel disconnection is detected.
VPN Track	Select the **Enable** check box to enable the VPN track function. The device can monitor the connectivity status of the specified VPN tunnel, and also allows backup or load sharing between two or more VPN tunnels. This function is applicable to both route-based and policy-based VPNs. The options are: • Track Interval - Specify the interval of sending Ping packets.

Option	Description
	• Threshold - Specify the threshold for determining the track failure. If system did not receive the specified number of continuous response packets, it will identify a track as failure, i.e., the target tunnel is disconnected. • Source Address - Specify the source IP address that sends Ping packets. • Destination Address - Specify the IP address of the tracked object.

3. Click **OK** to save the settings.

Related Topics:

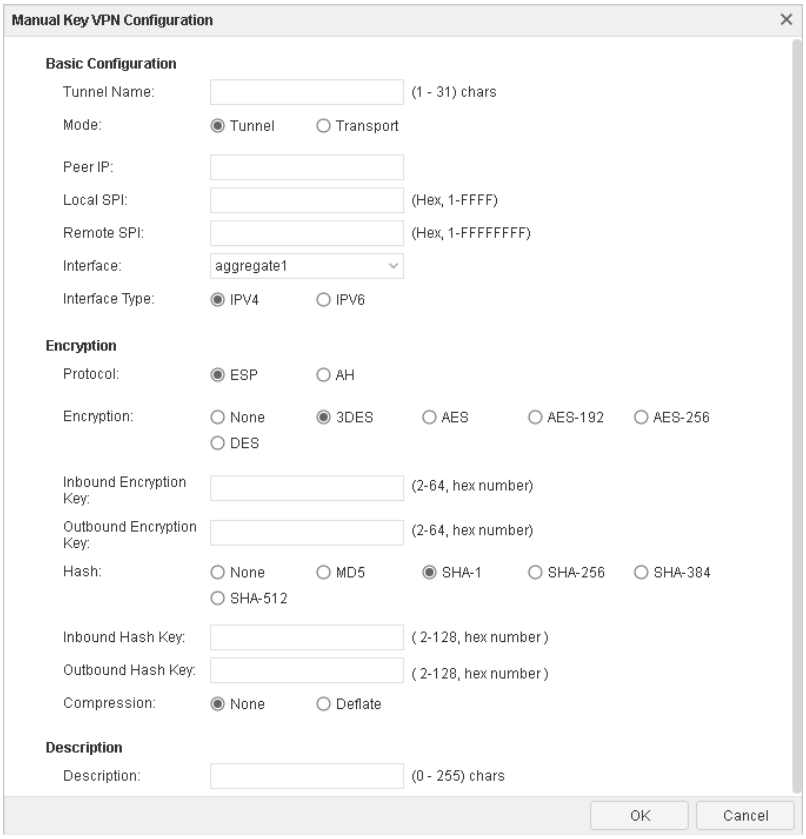
- "Configuring a Manual Key VPN" on Page 430
- "Configuring PnPVPN" on Page 438
- "Configuring IPSec-XAUTH Address Pool" on Page 435
- "Viewing IPSec VPN Monitoring Information" on Page 433

Configuring a Manual Key VPN

Use the manual key VPN to negotiate IPSec SA manually. To configure the manual key VPN, take the following steps:

1. Select **Network** > **VPN** > **IKEv1 and Manual**.

2. In the Manual Key VPN Configuration section, click **New**.



In the Manual Key VPN Configuration dialog box, configure the corresponding options.

Basic Configuration	
Tunnel Name	Specify the name of the new manual key VPN.
Mode	Specify the mode, including Tunnel and Transport. The tunnel mode is the default mode.
Peer IP	Specify the IP address of the peer.
Local SPI	Type the local SPI value. SPI is a 32-bit value transmitted in AH and ESP header, which uniquely identifies a security association. SPI is used to seek

Basic Configuration	
	corresponding VPN tunnel for decryption.
Remote SPI	Type the remote SPI value. **Note**: When configuring an SA, you should configure the parameters of both the inbound and outbound direction. Furthermore, SA parameters of the two ends of the tunnel should be totally matched. The local inbound SPI should be the same with the outbound SPI of the other end; the local outbound SPI should be the same with the inbound SPI of the other end.
Interface	Specify the egress interface for the manual key VPN. Select the interface you want from the **Interface** drop-down list.
Interface Type	Select the interface type, including IPv4 or IPv6. Only the IPv6 firmware supports to configure IPv6 type interface.
Encryption	
Protocol	Specify the protocol type. ESP is the default protocol type.
Encryption	Specify the encryption algorithm. 3DES is the default encryption algorithm.
Inbound Encryption Key	Type the encryption key of the inbound direction. You should configure the keys of both ends of the tunnel. The local inbound encryption key should be the same with the peer's outbound encryption key, and the local outbound encryption key should be the same with the peer's inbound encryption key.
Outbound Encryption Key	Type the encryption key of the outbound direction.
Hash	Specify the authentication algorithm. SHA-1 is the default algorithm.
Inbound Hash Key	Type the hash key of the inbound direction. You should configure the keys of both ends of the tunnel. The local inbound hash key should be the same with the peer's outbound hash key, and the local outbound hash key should be the same with the peer's inbound hash key.
Outbound Hash Key	Type the hash key of the outbound direction.

Basic Configuration	
Compression	Select a compression algorithm. By default, no compression algorithm is used.
Description	
Description	Type the description for the new manual key VPN.

3. Click **OK** to save the settings.

Related Topics:

- "Configuring an IKE VPN" on Page 416
- "Configuring PnPVPN" on Page 438
- "Configuring IPSec-XAUTH Address Pool" on Page 435
- "Viewing IPSec VPN Monitoring Information" on Page 433

Viewing IPSec VPN Monitoring Information

By using the ISAKMP SA table, IPSec SA table, and Dial-up User table, the IPSec VPN monitoring function can show the SA negotiation results of IPSec VPN Phase1 and Phase2 as well as information of dial-up users.

To view the VPN monitoring information, take the following steps:

1. Select **Network** > **VPN** > **IKEv1 and Manual**.
2. In the IKEv1 VPN Configuration section, click **IPSec VPN Monitor** at the top-right corner. Then you can view the VPN monitoring information in the ISAKMP SA, IPSec SA and Dial-up User sections.
3. Click **Back** to return to the IPSec VPN configuration page.

Options in these tabs are described as follows:

ISAKMP SA

Option	Description
Cookie	Displays the negotiation cookies which are used to match SA Phase 1.
Status	Displays the status of SA Phase1.
Peer	Displays the IP address of the peer.
Port	Displays the port number used by the SA Phase1. 500 indicates that no NAT has been found during the SA Phase 1; 4500 indicates that NAT has been detected.
Algorithm	Displays the algorithm of the SA Phase1, including authentication method, encryption algorithm and verification algorithm.
Lifetime	Displays the lifetime of SA Phase1. The unit is second.

IPSec SA

Option	Description
ID	Displays the tunnel ID number which is auto assigned by the system.
VPN Name	Displays the name of VPN.
Direction	Displays the direction of VPN.

Option	Description
Peer	Displays the IP address of the peer.
Port	Displays the port number used by the SA Phase2.
Algorithm	Displays the algorithm used by the tunnel, including protocol type, encryption algorithm, verification algorithm and depression algorithm.
SPI	Displays the local SPI and the peer SPI. The direction of inbound is local SPI, while outbound is peer SPI.
CPI	Displays the compression parameter index (CPI) used by SA Phase2.
Lifetime (s)	Displays the lifetime of SA Phase2 in seconds, i.e. SA Phase2 will restart negotiations after X seconds.
Lifetime (KB)	Displays the lifetime of SA Phase2 in KB, i.e. SA Phase2 will restart negotiations after X kilobytes of data flow.
Status	Displays the status of SA Phase2.

Dial-up User

Option	Description
Peer	Displays the statistical information of the peer user. Select the peer you want from the **Peer** drop-down list.
User ID	Displays the IKE ID of the user selected.
IP	Displays the corresponding IP address.
Encrypted Packets	Displays the number of encrypted packets transferred through the tunnel.
Encrypted Bytes	Displays the number of encrypted bytes transferred through the tunnel.
Decrypted Packets	Displays the number of decrypted packets transferred through the tunnel.
Decrypted Bytes	Displays the number of decrypted bytes transferred through the tunnel.

Configuring IPSec-XAUTH Address Pool

XAUTH server assigns the IP addresses in the address pool to users. After the client has established a connection to the XAUTH server successfully, the XAUTH server will choose an IP address along with other related parameters (such as DNS server address, WINS server address, etc.) from the address pool, and will assign them to the client.

XAUTH server provides fixed IP addresses by creating and implementing IP binding rules that consist of a static IP binding rule and an IP-role binding rule. The static IP binding rule binds the client user to a fixed IP address in the address pool. Once the client has established a connection successfully, system will assign the binding IP to the client. The IP-role binding rule binds the role to a specific IP range in the address pool. Once the client has established a connection successfully, system will assign an IP address within the IP range to the client.

When the XAUTH server is allocating IP addresses in the address pool, system will check the IP binding rule and determine how to assign IP addresses to the client based on the specific checking order below:

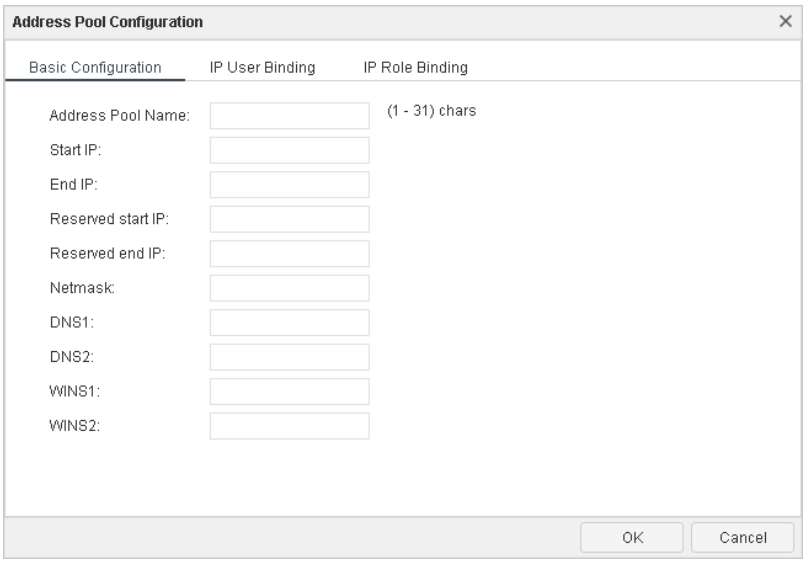
1. Check if the client is configured with any static IP binding rule. If so, assign the binding IP address to the client; otherwise, check the other configuration. Note: if the binding IP address is in use, the user will be unable to log in.
2. Check if the client is configured with any IP-role binding rule. If so, assign an IP address within the binding IP range to the client; otherwise, the user will be unable to log in.

Note: The IP addresses defined in the static IP binding rule and IP-role binding rule should not be overlapped.

To configure the IPSec-XAUTH address pool, take the following steps:

1. Select **Network** > **VPN** > **IKEv1 and Manual**.
2. In the IKEv1 VPN Configuration section, select **IPSec-XAUTH Address Pool** at the top-right corner.

3. In the XAUTH Address Pool Configuration dialog box, click **New**, and the Address Pool Configuration dialog box will appear.



In the Basic Configuration tab, configure the corresponding options.

Option	Description
Address Pool Name	Specify the name of the address pool.
Start IP	Specify the start IP of the address pool.
End IP	Specify the end IP of the address pool.
Reserved Start IP	Specify the reserved start IP of the address pool.
Reserved End IP	Specify the reserved end IP of the address pool.
Netmask	Specify the netmask of the IP address.
DNS1	Specify the DNS server IP address for the address pool. It is optional. You can configure up to two DNS servers for one address pool.
DNS2	Specify the DNS server IP address for the address pool. It is optional. You can configure up to two DNS servers for one address pool.
WINS1	Specify the WINS server IP address for the address pool. It is optional. You can configure up to two WINS servers for one address pool.

Option	Description
WINS2	Specify the WINS server IP address for the address pool. It is optional. You can configure up to two WINS servers for one address pool.

In the IP User Binding tab, configure the corresponding options.

Option	Description
User	Type the user name into the **User** box.
IP	Type the IP address into the **IP** box.
Add	Click **Add** to add the item that binds the specified user to the IP address.

In the IP Role Binding tab, configure the corresponding options.

Option	Description
Role	Select a role from the **Role** drop-down list.
Start IP	Type the start IP address into the **Start IP** box.
End IP	Type the end IP address into the **End IP** box.
Add	Click **Add** to add the item that binds the specified role to the IP address range.
Up/Down/Top/Bottom	To change the rule display order, click the button you desire to move the selected IP-role binding rule. For the user that is bound to multiple roles that are also configured with their corresponding IP-role binding rules, system will query the IP-role binding rules in order, and assign an IP address based on the first matched rule.

4. Click **OK** to save the settings.

Configuring PnPVPN

IPSec VPN requires sophisticated operational skills and high maintenance cost. To relieve network administrators from the intricate work, system provides an easy-to-use VPN technology - PnPVPN (Plug-and-Play VPN). PnPVPN consists of two parts: PnPVPN Server and PnPVPN Client.

- PnPVPN Server: Normally deployed in the headquarters and maintained by an IT engineer, the PnPVPN Server sends most of the configuration commands to the clients. The device usually works as a PnPVPN Server and one device can serve as multiple servers.
- PnPVPN Client: Normally deployed in the branch offices and controlled remotely by a headquarters engineer, the PnPVPN Client can obtain configuration commands (e.g. DNS, WINS, DHCP address pool, etc.) from the PnPVPN Server with simple configurations, such as client ID, password, and server IP settings.

The device can serve as both a PnPVPN Server and a PnPVPN Client. When working as a PnPVPN Server, the maximum number of VPN instances and the supported client number of each device may vary according to the platform series.

PnPVPN Workflow

The workflow for PnPVPN is as follows:

1. The client initiates a connection request and sends its own ID and password to the server.
2. The server verifies the ID and password when it receives the request. If the verification succeeds, the server will send the configuration information, including DHCP address pool, DHCP mask, DHCP gateway, WINS, DNS and tunnel routes, etc., to the client.
3. The client distributes the received information to corresponding functional modules.
4. The client PC automatically gains an IP address, IP mask, gateway address and other network parameters and connects itself to the VPN.

PnPVPN Link Redundancy

The PnPVPN server supports dual VPN link dials for a PnPVPN client, and automatically generates the routing to the client. Also, it can configure the VPN monitor for the client. Two ISAKMP gateways and two tunnel interfaces need to be con-

figured in the server. The two VPN tunnels need to refer different ISAKMP gateways and be bound to different tunnel interfaces.

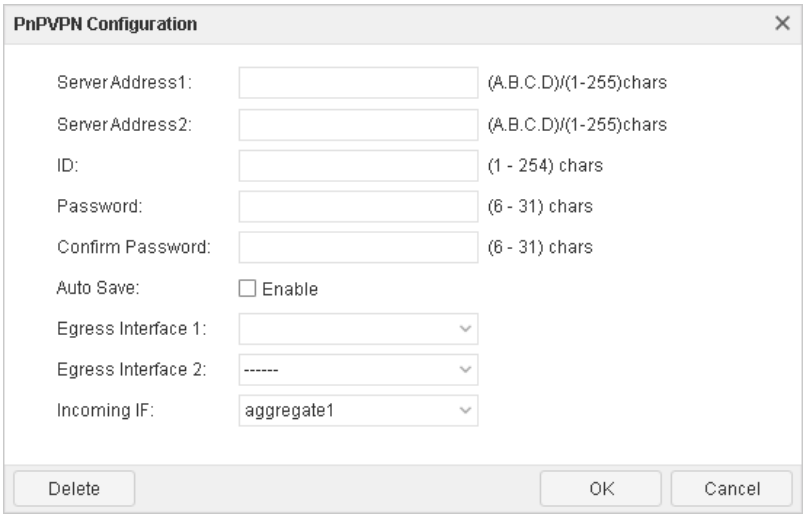
The client supports to configure dual VPN dials, VPN monitoring and redundant routing. When the two VPN tunnels are negotiating with the server, the client generates routes with different priority according to the tunnel routing configuration at the server side. The high priority tunnel acts as the master link and the tunnel with low priority as the backup link, so as to realize redundant routing. The master VPN tunnel will be in the active state first. When master tunnel is interrupted, the client will use the backup tunnel to transfer the data. When the master tunnel restores to be normal, it will transfer the data again.

Configuring a PnPVPN Client

To configure a PnPVPN client, take the following steps:

1. Select **Network** > **VPN** > **IKEv1 and Manual**.

2. In the IKEv1 VPN Configuration section, click **PnPVPN Client** at the top-right corner.



In the PnPVPN Configuration dialog box, configure the following options.

Option	Description
Server Address1	Specify the IP address of the PnPVPN Server. PnPVPN client supports dual link dials to the server side. This option is required.
Server Address2	Specify the IP address of the PnPVPN Server. The server address 1 and the server address 2 can be the same or different. It is optional.

Option	Description
ID	Specify the IKE ID assigned to the client by the server.
Password	Specify the password assigned to the client by the server.
Confirm Password	Enter the password again to confirm.
Auto Save	Select the **Enable** check box to auto save the DHCP and WINS information released by the PnPVPN Server after the connection is established.
Egress Interface 1	Specify the interface connecting to the Internet. Select an interface you need from the drop-down list. This option is required.
Egress Interface 2	Specify the interface connecting to the Internet. Select an interface you need from the drop-down list. The IF1 and the IF2 can be the same or different. It is optional.
Incoming IF	Specify the interface on the PnPVPN Client accessed by the Intranet PC or the application servers.

3. Click **OK** to save the settings.

Note:

- Server Addresses1 and Egress IF1 both need to be configured. If you want to configure a backup link, you need to configure both the Server Address2 and Egress Interface 2.
- If the server addresses or the Egress IFs are different, two separate VPN links will be generated; and if the server addresses or the Egress IFs are the same, only one VPN link will be generated.
- The configuration of the two servers can be configured on one device, and can also be configured on two different devices (primary and backup). If you configure it on two devices, you need to configure AAA users on the two devices. The DHCP configuration for the AAA users should be the same, otherwise it might cause that the client and server negotiate successfully, but the traffic is blocked.

IKEv2_VPN

The configurations of IKEv2 VPN include:

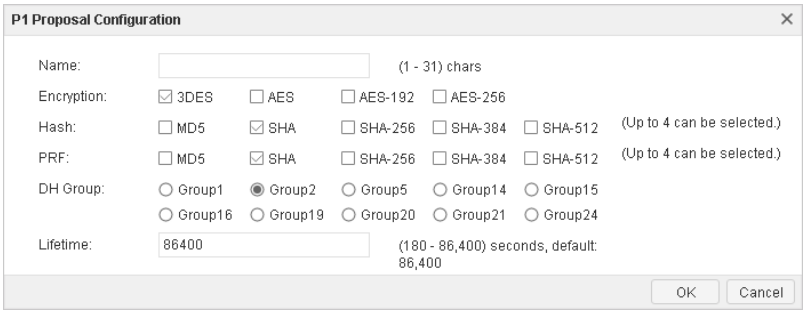
- Configuring a Phase 1 Proposal
- Configuring an IKEv2 Peer
- Configuring a Phase 2 Proposal
- Configuring an IKEv2 VPN

Configuring a Phase 1 Proposal

P1 proposal is the IKEv2 security proposal that is used to store the security parameters during the IKE_SA_INIT exchange, including the encryption algorithm, authentication algorithm, PRF (pseudo-random function) algorithm, and DH algorithm. A complete IKEv2 security proposal should include at least a set of security parameters, including an encryption algorithm, an authentication algorithm, a PRF algorithm, and a DH group.

To configure a P1 proposal, take the following steps:

1. Select **Network** > **VPN** > **IKEv2**.
2. In the IKEv2 VPN Configuration section, click the **P1 Proposal** tab.
3. Click **New**.



In the P1 Proposal Configuration dialog box, configure the corresponding options.

Option	Description
Name	Specify the name of the Phase1 proposal.

Option	Description
Authentication	Specify the IKE identity authentication method. IKE identity authentication is used to verify the identities of both communication parties. There are four methods for authenticating identity: pre-shared key, RSA signature, DSA signature and GM-DE. The default option is pre-shared key. For the pre-shared key method, the key is used to generate a secret key and the keys of both parties must be the same so that it can generate the same secret keys.
Hash	System supports the following authentication algorithms: • MD5 - Uses MD5 as the authentication algorithm. Its hash value is 128-bit. • SHA - Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm. • SHA-256 - Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 - Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit. • SHA-512 - Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit.
PRF	System supports the following authentication algorithms: • MD5 - Uses MD5 as the authentication algorithm. Its hash value is 128-bit. • SHA - Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm. • SHA-256 - Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 - Uses SHA-384 as the authentication algorithm. Its hash

Option	Description
	value is 384-bit. • SHA-512 - Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit.
Encryption	System supports the following four encryption algorithms: 3DES, 128bit AES, 192bit AES and 256bit AES. You can specify one to four encryption algorithms. • 3DES - Uses 3DES as the encryption algorithm. The key length is 192-bit. This is the default encryption algorithm. • AES - Uses AES as the encryption algorithm. The key length is 128-bit. • AES-192 - Uses 192-bit AES as the encryption algorithm. The key length is 192-bit. • AES-256 - Uses 256-bit AES as the encryption algorithm. The key length is 256-bit.
DH Group	Diffie-Hellman (DH) is designed to establish a shared secret key. DH group determines the length of the element generating keys for DH exchange. The strength of keys is partially decided by the robustness of the DH group. • Group1 - Uses Group1 as the DH group. The key length is 768-bit (MODP Group). • Group2 - Uses Group2 as the DH group. The key length is 1024-bit (MODP Group). Group2 is the default value. • Group5 - Uses Group5 as the DH group. The key length is 1536-bit (MODP Group). • Group14 - Uses Group14 as the DH group. The key length is 2048-bit (MODP Group).

Option	Description
	• Group15 - Uses Group15 as the DH group. The key length is 3072-bit (MODP Group). • Group16 - Uses Group16 as the DH group. The key length is 4096-bit (MODP Group). • Group19 - Uses Group19 as the DH group. The key length is 256-bit (ECP Group). • Group2 - Uses Group20 as the DH group. The key length is 384-bit (ECP Group). • Group21 - Uses Group21 as the DH group. The key length is 521-bit (ECP Group). • Group24 - Uses Group24 as the DH group. The key length is 2048-bit (MODP Group with 256-bit Prime Order Subgroup).
Lifetime	Specify the lifetime of IKEv2 SA. The value range is 180 to 86400 seconds. The default value is 28800. The lifetime of IKEv2 SA does not need negotiation, but is determined by individual settings. The side with a less lifetime will re-negotiate and this can avoid the SA redundancy caused by simultaneous re-negotiation at both sides, resulting in inconsistent SA status at both sides.

4. Click **OK** to save the settings.

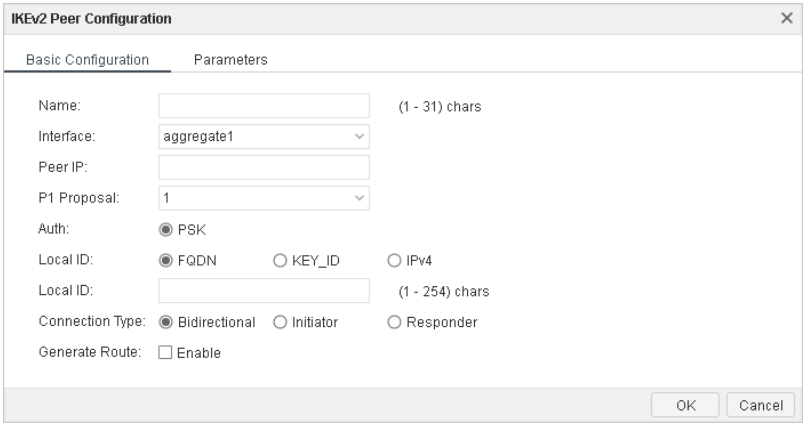
Configuring an IKEv2 Peer

After creating an IKEv2 peer, you can configure the peer's IKE negotiation mode and IP address, IKE security proposal, local ID, etc.

To configure an IKEv2 Peer, take the following steps:

1. Select **Network** > **VPN** > **IKEv2**.
2. In the IKEv2 VPN Configuration section, click the **VPN Peer List** tab.

3. Click **New**.



In the IKEv2 Peer Configuration dialog box, configure the corresponding options.

Basic Configuration	
Name	Specify the name of the IKEv2 Peer.
Interface	Specify the interface bound to the IKEv2 Peer.
Peer IP	Specify the peer IP address for the IKEv2 peer.
P1 Proposal	Specify the P1 Proposal for the IKEv2 peer.
Auth	Specify the authentication method as the pre-shared key for the IKEv2 peer.
Local ID	Specify the local ID. System supports FQDN, KEY_ID and IPv4. Select the ID type you want, and then type the content for this ID into the **Local ID** box or the **Local IP** box.
Connection Type	Specify the connection type for the IKEv2 Peer, including: • Bidirectional - Specify that the ISAKMP gateway serves as both the initiator and responder. This is the default value. • Initiator - Specify that the ISAKMP gateway serves as the initiator only. • Responder - Specify that the ISAKMP gateway serves as the responder only.

Basic Configuration	
Generate Route	Select the **Enable** check box to enable the automatic route generation function. For the IKEv2 VPN, after the function is enabled, each time an IPSec SA is created, the device will add the routing entry whose destination address is in the destination network segment of the protected data stream and whose next hop is the tunnel interface to its own routing table. After deleting an IPSec SA, the corresponding routing entry will also be deleted. By default, this function is disabled.
Parameters	
Name	Specify the name of the IKEv2 profile. An IKEv2 profile can store the IKEv2 SA parameters that do not require negotiation, such as the peer identity, the pre-shared key, and the information of the secured data traffic. You need to configure an IKEv2 profile at both the initiator side and responder side.
Peer ID	Specify the peer ID. System supports FQDN, KEY_ID and IPv4. Select the ID type you want, and then type the content for this ID into the **Local ID** box or the **Local IP** box.
Pre-shared Key	Specify the value of the pre-shared key. Only when the values of the pre-shared keys on both ends are the same can the IKEv2 tunnel be established.
Traffic Selector	Creates the secured data traffic. IKEv2 VPN can secure one or more data streams, i.e., securing the traffic that needs to enter the IPSec tunnel. In some cases, the source and destination addresses of the traffic encrypted with the IPSec tunnel may be on different network segments. Click "+" and double-click the newly added column in the list to add information of the secured data traffic, including the name of the data traffic, and the local address and peer address of the secured data traffic.

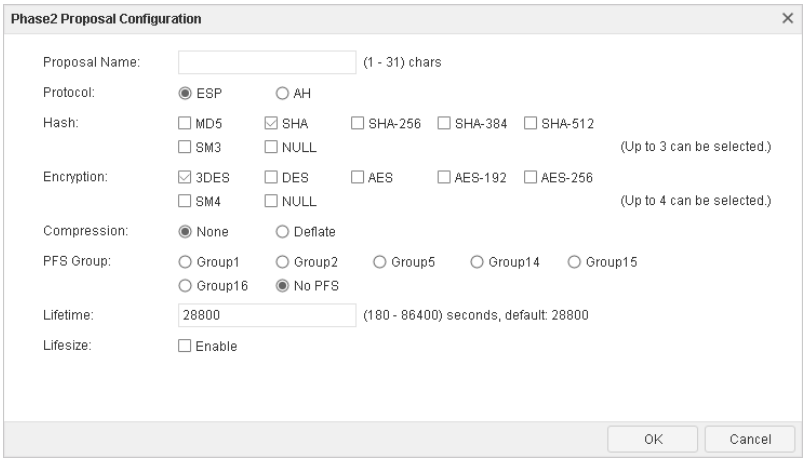
4. Click **OK** to save the settings.

Configuring a Phase 2 Proposal

P2 proposal is the IPSec security proposal that is used to store the security parameters using by IPSec for IPSec SA negotiation, including the security protocol, encryption algorithm, authentication algorithm, etc. The configurations of the P2 proposal include protocol type, encryption algorithm, authentication algorithm, encryption algorithm and lifetime.

To configure a P2 proposal, take the following steps:

1. Select **Network** > **VPN** > **IKEv2**.
2. In the IKEv2 VPN Configuration section, click the **P2 Proposal** tab.
3. Click **New**.



In the P2 Proposal Configuration dialog box, configure the corresponding options.

Option	Description
Name	Specify the name of the Phase2 proposal.
Protocol	Specify the protocol type of Phase2. The default value is ESP.
Hash	Specify the authentication algorithm for Phase2. You can specify one to four algorithms. • MD5 - Uses MD5 as the authentication algorithm. Its hash value is 128-bit. • SHA - Uses SHA as the authentication algorithm. Its hash value is 160-bit. This is the default hash algorithm.

Option	Description
	• SHA-256 - Uses SHA-256 as the authentication algorithm. Its hash value is 256-bit. • SHA-384 - Uses SHA-384 as the authentication algorithm. Its hash value is 384-bit. • SHA-512 - Uses SHA-512 as the authentication algorithm. Its hash value is 512-bit.
Encryption	Specify the encryption algorithm for Phase2. You can specify one to four algorithms. • 3DES - Uses 3DES as the encryption algorithm. The key length is 192-bit. This is the default encryption algorithm. • DES - Uses DES as the encryption algorithm. The key length is 64-bit. • AES-192 - Uses 192-bit AES as the encryption algorithm. The key length is 192-bit. • AES-256 - Uses 256-bit AES as the encryption algorithm. The key length is 256-bit. • null - No encryption.
PFS Group	Specify the PFS function for the P2 proposal. The PFS (Perfect Forward Security) function is designed to determine how to generate the new key instead of the time of generating the new key. PFS ensures that no matter what phase it is in, one key can only be used once, and the element used to generate the key can only be used once. The element will be discarded after generating a key, and will never be reused to generate any other keys. Such a measure will assure that even if a single key is disclosed, the disclosure will only affect the data that is encrypted by the key, and will not threaten the entire communication. PFS is based on the DH algorithm.

Option	Description
	• No PFS - Disables PFS. This is the default value. • Group1 - Uses Group1 as the DH group. The key length is 768-bit (MODP Group). • Group2 - Uses Group2 as the DH group. The key length is 1024-bit (MODP Group). • Group5 - Uses Group5 as the DH group. The key length is 1536-bit (MODP Group). • Group14 - Uses Group14 as the DH group. The key length is 2048-bit (MODP Group). • Group15 - Uses Group15 as the DH group. The key length is 3072-bit (MODP Group). • Group16 - Uses Group16 as the DH group. The key length is 4096-bit (MODP Group). • Group19 - Uses Group19 as the DH group. The key length is 256-bit (ECP Group). • Group20 - Uses Group20 as the DH group. The key length is 384-bit (ECP Group). • Group21 - Uses Group21 as the DH group. The key length is 521-bit (ECP Group).
Lifetime	You can evaluate the lifetime by the time length. When the IPSec SA life-time runs out, the SA will get expired and requires a new SA negotiation. Type the lifetime length of the P2 proposal into the box. The value range is 180 to 86400 seconds. The default value is 28800.

4. Click **OK** to save the settings.

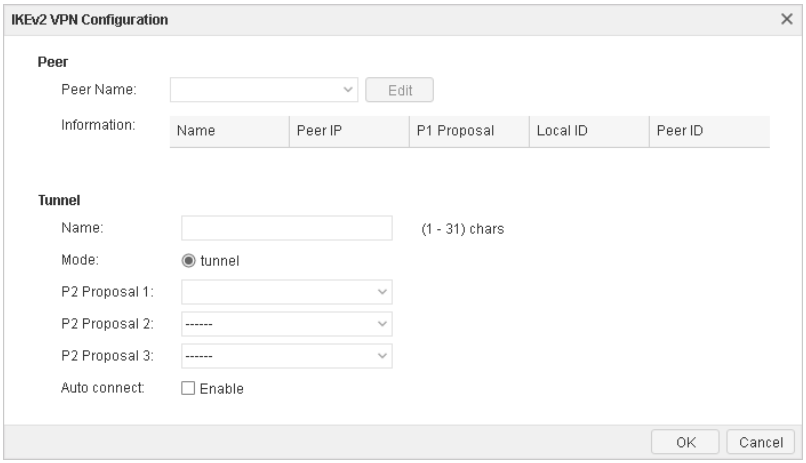
Configuring an IKEv2 VPN

When configuring an IPSec tunnel through IKEv2, you need to configure the following options: the operation mode, IKEv2 peer, IKEv2 security proposal, and auto-connection.

To configure an IKEv2 VPN, take the following steps:

1. Select **Network** > **VPN** > **IKEv2**.

2. In the IKEv2 VPN Configuration section, click the **IKEv2 VPN List tab**. Then click **New**, and the IKEv2 VPN Configuration dialog box will appear.



In the Basic Configuration tab, configure the corresponding options.

Peer	
Peer Name	Specify the name of the IKEv2 Peer.
Information	Shows the information of the selected peer.
Tunnel	
Name	Type a name for the tunnel.
Mode	Specify the mode, including tunnel mode and transport mode.
P2 Proposal 1	Specify the P2 proposal for the IKEv2 tunnel. You can specify up to three P2 proposals for the IKEv2 tunnel to be used by the peer.
P2 Proposal 2	
P2 Proposal 3	

Peer	
Auto Connect	Select the **Enable** check box to establish an SA by using the auto mode. In the auto mode, the device will check the SA status every 60 seconds and initiate a negotiation request when SA is not established. By default, this function is disabled. It works only when the local device is the initiator.

3. Click **OK** to save the settings.

Chapter 13 Monitor

The monitor section includes the following functions:

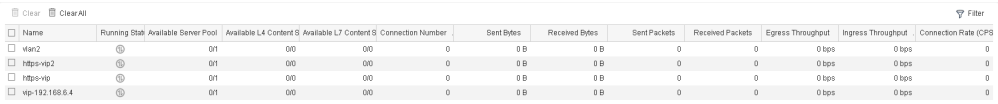
- **Monitor**: The Monitor function statistically analyzes the devices and displays the statistics in a bar chart, line chart, tables, and so on, which helps the users have information about the devices and perform troubleshooting, including:
  - Server Load Balancing
    - Virtual Server
    - Server Pool
    - Real Server
    - Cache/Compression
  - Global Server Load Balancing
  - Link Load Balancing
  - SSL Inspection
  - "User Monitor" on Page 457
  - "Application Monitor" on Page 459
  - "Link Status Monitor" on Page 461
  - "iQoS Monitor" on Page 468
  - "Device Monitor" on Page 466
  - "Authentication User" on Page 459
  - "Monitor Configuration" on Page 471

- **Logging**: Records and exports various system logs, including:
  - "Logging" on Page 473
  - "Configuration Logs" on Page 475
  - "Network Logs" on Page 475
  - "NAT Logs" on Page 477
  - "Health Check Logs" on Page 478
  - "Global Server Load Balance Logs" on Page 484
  - "Threat Logs" on Page 478
  - "Session Logs" on Page 480
  - "Event Logs" on Page 475
  - "PBR Logs" on Page 476
  - "L7 Load Balance Logs" on Page 482
  - "L4 Load Balance Logs" on Page 483
  - "SSL Inspection Logs" on Page 485
  - "Log Configuration" on Page 493
  - "Managing Logs" on Page 485

Virtual Server Monitor

In the virtual server monitor page, the traffic statistics of all virtual servers in the device will be displayed in the list, including the number of connections, the total number of sent /received bytes, the total number of sent/received packets, the upstream and downstream bandwidth and the rate of creating new connections.

Click **Monitor** > **Server Load Balance** > **Virtual Server** to enter the Virtual Server Monitor page.

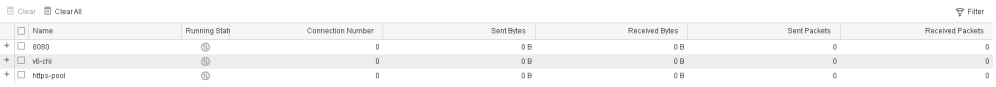


- Click the **Filter** button, and then click +Filter to select **Name** from the drop-down list. Then type the name of the virtual server you desire into the search box, and the list will display the statistics of the specified virtual server.
- Select one or more statistical entries, and click **Clear** to clear the traffic statistics of the specified virtual server.
- Click **Clear All** to clear the traffic statistics of all virtual servers.

Server Pool Monitor

In the server pool monitor page, the traffic statistics of all server pools and their real servers will be displayed in the list, including the number of connections, the total number of sent/received bytes and the total number of sent/received packets.

Click **Monitor** > **Server Load Balance** > **Server Pool** to enter the Server Pool Monitor page.

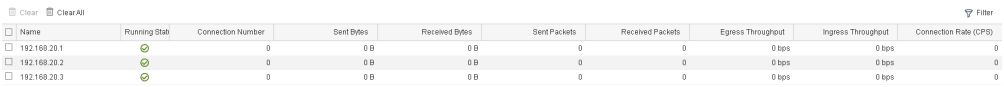


- Click ⊞ in front of a server pool name to view the statistics of real servers in the server pool.
- Click the **Filter** button, and then click +Filter to select **Name** from the drop-down list. Then type the name of the server pool you desire into the search box, and the list will display the statistics of the specified server pool.
- Select one or more statistical entries, and click **Clear** to clear the traffic statistics of the specified server pool.
- Click **Clear All** to clear the traffic statistics of all server pools.

Real Server Monitor

In the real server monitor page, the traffic statistics of all real servers in the device will be displayed in the list, including the number of connections, the total number of sent/received bytes, the total number of sent/received packets, the upstream and downstream bandwidth and the rate of creating new connections.

Click **Monitor** > **Server Load Balance** > **Real Server** to enter the Real Server Monitor page.



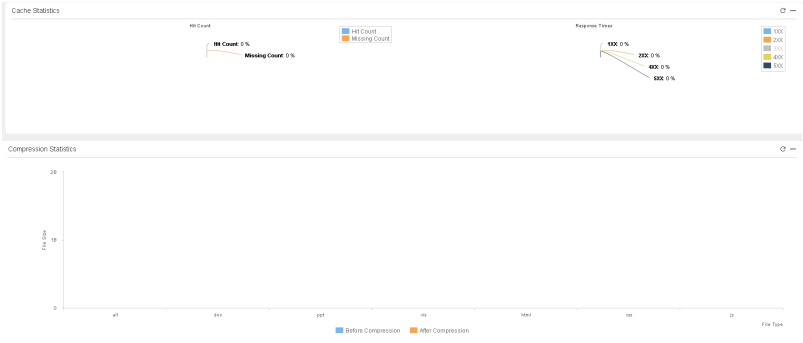
- Click the **Filter** button, and then click +Filter to select **Name** from the drop-down list. Then type the name of the real server you desire into the search box, and the list will display the statistics of the specified real server.
- Select one or more statistical entries, and click **Clear** to clear the traffic statistics of the specified real server.
- Click **Clear All** to clear the traffic statistics of all real servers.

Cache/Compression

The cache/compression monitor function displays the statistics on the HTTP cache and compression, including the number of hits and responses times of the HTTP cache in the specified virtual server; and the statistics on the compressed size for each static resource type.

HTTP cache refers to that system will cache the static resource (such as CSS files, pictures and other resources with a large number of accesses but small changes) returned by the real server to the client. In this way, when the client accesses the same static resource again, the device can directly return the cached content to the client, thereby saving time of subsequent communication with the real server, and reducing the load burden on the real server. HTTP static resource compression refers to that if the client can receive and decompress compressed files, the device will first compress uncompressed files returned by the server, and then send them to the client, thereby reducing the transmission load and shortening the transmission time to accelerate the communication.

Click **Monitor** > **Server Load Balance** > **Cache/Compression**. From the **Virtual Server** drop-down list, select a virtual server that you want to display its cache and compression information. Then the page will display as follows:



- Cache Statistics: Displays the proportion of HTTP cache hits and misses; and the proportion of response times of the HTTP cache.
- Compression Statistics: Displays the file sizes of different types of files before and after compression.

If you click **Clear**, system will clear the cached or compressed statistics.

Related Topics:

- HTTP Cache/Compression

User Monitor

User monitor displays various statistics of different users.

Summary

Summary displays the following contents:

- Top 10 users by traffic.
- Top 10 users by concurrent sessions.

Click **Monitor** > **User Monitor** > **Summary**.

- Click  to refresh the monitoring data in this page.
- Hover your mouse over a bar to view the user's average upstream traffic, downstream traffic, total traffic or concurrent sessions.
- When displaying the user traffic statistics, the Upstream and Downstream legends are used to select the statistical objects in the bar chart.

User Details

To view detailed statistics of all users, click **Monitor** > **User Monitor** > **User Details**.

- Click **+Filter** to select a condition from the drop-down list to search for the desired users.
- To view the detailed information of a certain user, select the user entry in the list, and then the user IP and the statistics will be displayed below.
    - Application(real-time): Select the **Application(real-time)** tab to display the detailed information of the category, sub-category, risk level, technology, upstream traffic, downstream traffic, total traffic,
- Frame a region's trends with the mouse. You can enlarge the scope of the displayed time period. Click **Reset zoom** to restore the default size of the trend.

Authentication User

This page displays the statistics on the authenticated users.

To view the information of the users currently logged in to system, click **Monitor** > **Authenticated User**.

- Click +Filter to select a condition from the drop-down list to search for the desired users.
- Click **Kick Out** under the Operation column to kick the user out.
- Click to refresh the real-time data in the list.

Application Monitor

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

Application monitor displays the statistics of applications, application categories, application subcategories, application risk levels, application technologies, and application characteristics within the specified period (Realtime, latest 1 hour, latest 1 day, latest 1 month,). The statistics include the traffic, and concurrent sessions of applications of the specified interface/security zone.

Summary

Summary displays the following contents of within a specified period:

- The concurrent sessions of top 10 hot and high-risk applications.
- The traffic/concurrent sessions of top 10 applications.
- The traffic/concurrent sessions of top 10 application categories.
- The traffic/concurrent sessions of top 10 application subcategories.
- The traffic/concurrent sessions organized by application risk levels.
- The traffic/concurrent sessions organized by application technologies.
- The traffic/concurrent sessions organized by application characteristics.

Click **Monitor** > **Application Monitor** > **Summary**.

- Select different Statistical Periods to view the statistical information in different periods of time.
- From the drop-down list, specify the type of statistics: Trafficor Concurrent Sessions.
- Click to refresh the monitoring data in this page.
- Hover your mouse over a bar or a pie graph to view the concrete statistical values of or concurrent sessions.

Application Details

To view detailed statistics of all applications, click **Monitor** > **Application Monitor** > **Application Details**.

- Click **+Filter**, and select **Application** from the drop-down list. You can search the desired application by typing the application name into the text box.
- To view the detailed information of a certain application, select the application entry in the list, and then the application name and the statistics will be displayed below.
  - User(real-time): Click the **User(real-time)** tab to display the detailed information of users who are using the selected application. Click in the Details column to see the trends of the upstream traffic, downstream traffic, total traffic, within Statistical Period.
  - Description: Select the **Description** tab to display the detailed information of the selected application.

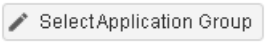
Group Details

To view detailed statistics of all applications, click **Monitor** > **Application Monitor** > **Group Details**.

- Click **+Filter**, and select **Application Group** from the drop-down list. You can search the desired application group by typing the application group name into the text box.
- To view the detailed information of a certain application group, select the application group entry in the list, and then the application group name and statistics will be displayed below.
  - User(real-time): Select the **User(real-time)** tab to display the detailed information of users who are using the selected application group. Click in the Details column to see the trends of the upstream traffic, downstream traffic, total traffic, within the

- Application(real-time): Select the **Application(real-time)** tab to display the detailed information of applications in use which belong to the selected application group. Click  in the Details column to see the trends of the upstream traffic, downstream traffic and total traffic of the selected application.

Select Application Group

Click **Monitor** > **Application Monitor** > **Select Application Group**. Click 

at the top-left corner to configure the application groups required to be counted in the **Select Application Group** dialog box. The left pane lists all global application groups.

In this dialog box, you can perform the following actions:

- Select the application group entries you want to count from the left pane, and click **Add** to add them to the **Selected** list.
- In the **Selected** list, select the application group entries you want to remove, and click **Remove**. The removed application group entries will not be counted.

Statistical Period

System supports the predefined time cycle. Click **Last 24 Hours** at the top-right corner of the monitor page to set the time cycle:

- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.
- Last 30 Days: Displays the statistical information within the latest 1 month.

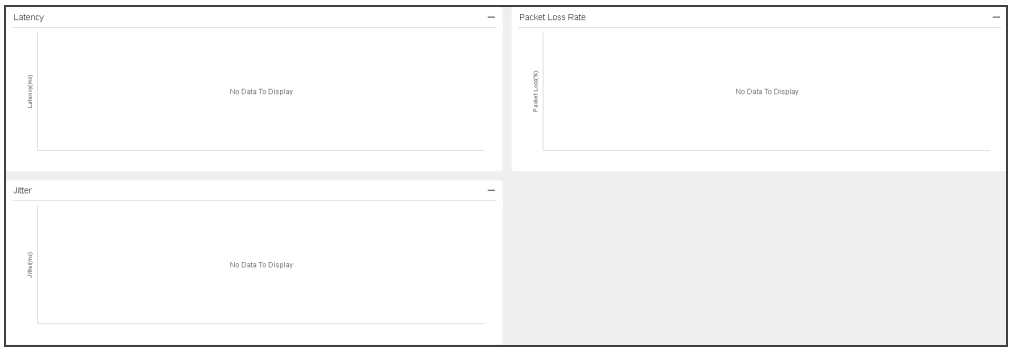
Link Status Monitor

Link status monitoring can calculate the sampling traffic information of the specific interface in the link, including latency, packet loss rate, and jitter, to monitor and display the overall status of the link. System also supports for link detection to calculate the traffic information of the specific destination IP address in the link, including latency and jitter.

Link User Experience

The link user experience page displays the traffic statistics of the interfaces that have been bound within a specified period (Realtime, latest 1 hour, latest 1 day)

Click **Monitor** > **Link Status Monitor** > **Link User Experience**. For more information about configuration of binding interfaces, refer to Link Configuration.



- Select different Statistical Periods to view the statistical information in different periods of time.
- Click the **Binding Interface** drop-down list and select a binding interface to view the link status monitoring statistics for this interface. You can select multiple interfaces.
- Click +Filter, select **Application** from the drop-down list, and then select the TOP 10 or an application/application group. System will display the link status monitoring statistics according to the specified application.

Note:

- "Time" and "Binding Interface" are required in the filter condition.
- If the application switch of the specified interface is not enabled in the link configuration, the **Application** filter condition cannot be added.

Statistical Period

System supports the predefined time cycle. Click **Last 60 Minutes** at the top-left corner of each tab (Last 60 Minutes) to set the time cycle.

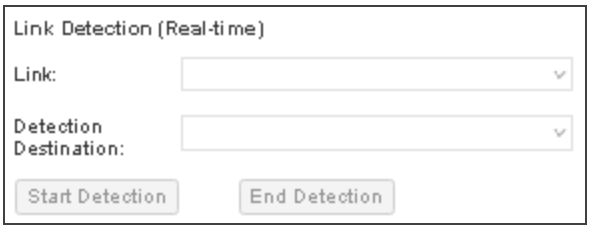
- Real-time: Displays the current statistical information.
- Last 60 Minutes: Displays the statistical information within the latest 1 hour.
- Last 24 Hours: Displays the statistical information within the latest 1 day.

Link Detection

The link detection page displays real-time traffic statistics of the specified detection destination IP to the link or the link to the detection destination IP, including latency and jitter.

To configure the link detection, take the following steps:

1. Click **Monitor** > **Link Status Monitor** > **Link Detection**.

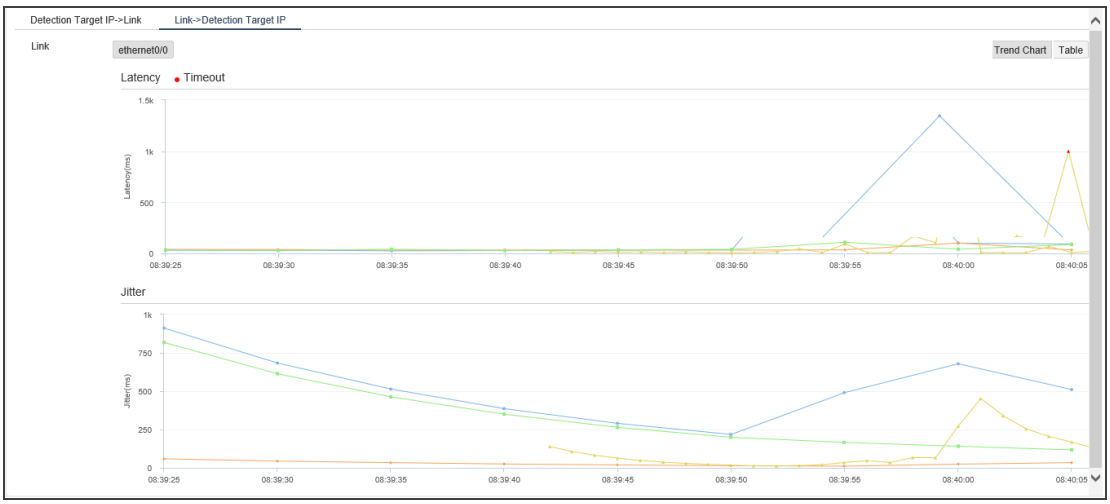


2. Select the interface name to view the link status monitoring statistics for this interface, and you can select up to 8 interfaces. Click **New** to add interfaces, and you can add up to 16 interfaces. For more information about configuration of binding interfaces, refer to Link Configuration.

3. Select the IP address to view the link status monitoring statistics for this destination address, and you can select up to 8 addresses. Click **New** to add destination addresses, and you can add up to 32 addresses. For more information about configuration of destination addresses, refer to Detection Destination.

4. Click **Start Detection**, and view the statistics of the real-time link detection at the bottom of the page. Select **Detection Destination IP** -> **Link** or **Link** -> **Detection Destination IP** tab to view the trend chart of latency and jitter. Click

Trend Chart and **Table** to switch between the trend chart and table.



5. Click **End Detection** to end the real-time link detection.

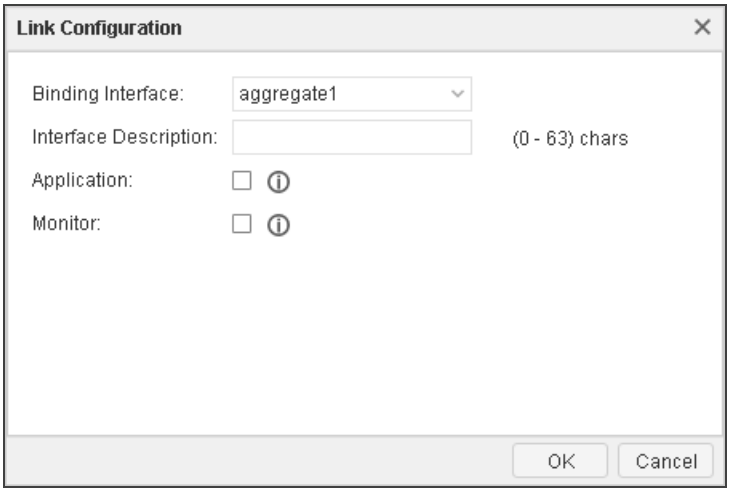
Link Configuration

In the link configuration page, you can configure the binding interface to monitor the link status, and can enable the application switch and link user experience.

To configure the link, take the following steps:

1. Click **Monitor** > **Link Status Monitor** > **Link Configuration**.

2. Click **New**.



In the Link Configuration dialog box, configure these values.

Option	Description
Binding Interface	Select an interface whose traffic needs to be counted from the drop down list.
Interface Description	Specify the description for the interface.
Application	With this check box selected, you can see details of the specific application of the interface, including delay, packet loss rate and jitter.
Monitor	With this check box selected, you can see traffic statistics of the interface in Link User Experience, including delay, packet loss rate and jitter.

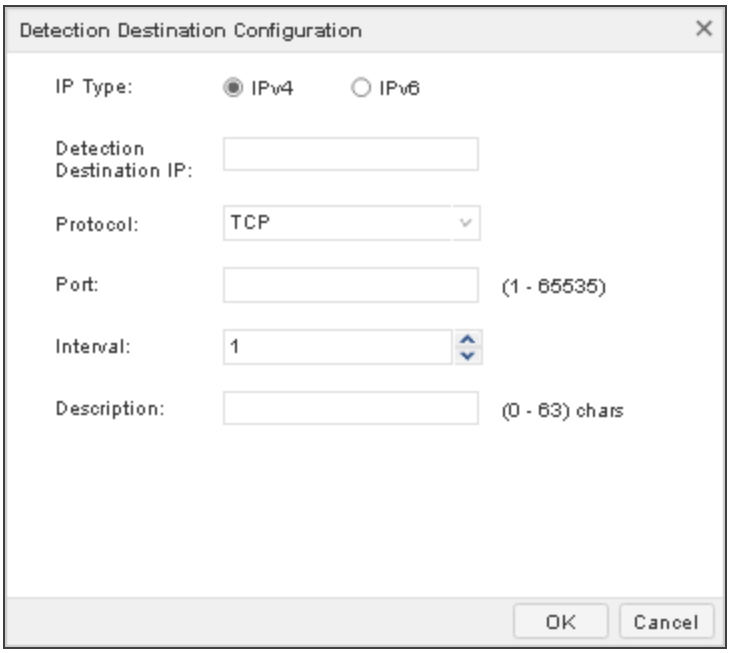
3. Click **OK**.

Detection Destination

In the detection destination page, you can configure the destination IP address to monitor the link status.

To configure the detection destination, take the following steps:

1. Click **Monitor** > **Link Status Monitor** > **Detection Destination**.
2. Click **New**.



In the Detection Destination Configuration dialog box, configure these values

Option	Description
IP Type	Select the IP address type, including IPv4 and IPv6.
Detection Destination IP	Specify the IP address of the detection destination.
Protocol	Specify the protocol of the detection destination, including TCP and ICMP.
Port	Specify the port number of the detection destination.
Interval	Specify the interval time of the detection packet. The value range is 1 to 5 seconds. The default value is 1.
Description	Type the description for the detection destination.

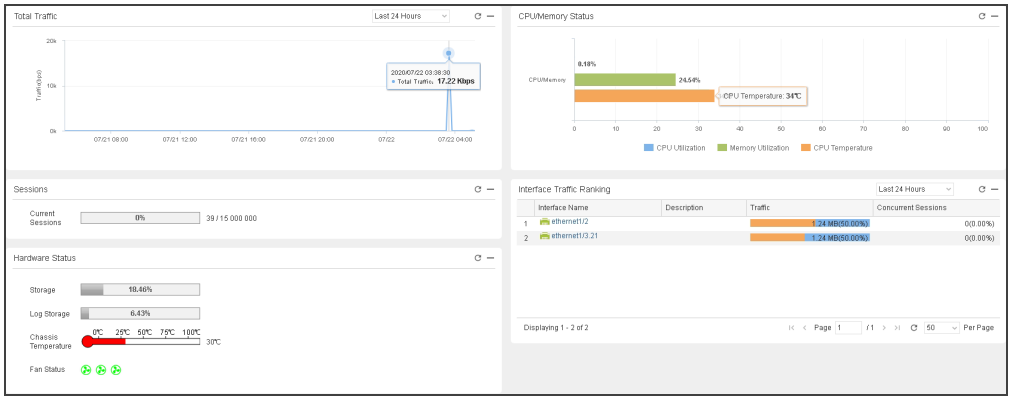
3. Click **OK**.

Device Monitor

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

Summary

The summary displays the device statistics in real time. Click **Monitor** > **Device Monitor** > **Summary**.



- Total traffic: Displays the total traffic within last 30 days/last 24 hours/last 60 minutes/in real time.
- Sessions: Displays the current sessions utilization, the number of current sessions and the total number of sessions.

- Hardware Status: Displays the real-time hardware status, including storage, log storage, chassis temperature and fan status.
    - Storage: Displays the percentage of disk space utilization.
    - Log Storage: Displays the percentage of log storage utilization.
    - Chassis Temperature: Displays the current CPU/chassis temperature.
    - Fan Status: Displays the operation status of the fan. Green indicates normal, and red indicates error or a power supply module is not used.
- CPU/Memory Status: Displays current CPU utilization, memory utilization and CPU temperature statistics.
    - Click legends of **CPU Utilization**, **Memory Utilization** or **CPU Temperature** to specify the histogram statistical objects. By default, it displays statistics of all objects.
    - Hover your mouse over the chart to view CPU utilization, memory utilization or CPU temperature statistics.
- Interface Traffic Ranking: Displays the interface traffic ranking, upstream traffic, downstream traffic, traffic percentage and concurrent sessions of interfaces within last 30 days/last 24 hours/last 60 minutes/in real time.

iQoS Monitor

When the iQoS policy is configured and the function of iQoS is enabled, you can view the real-time traffic details or traffic trends of pipes and sub-pipes in Level-1 Control or Level-2 Control.

Note: The iQoS monitor function is controlled by license. To use the function, install the iQoS license. For more information on license, refer to License.

iQoS Details

Select **Monitor** > **iQoS Monitor** > **iQoS Details** to enter the iQoS page. The pipe name and total traffic will be displayed in the list.

- Click Level-1 Control or Level-2 Control to display the details of the pipes of the selected level.
- In the Real-time drop-down list, select **Last 60 Minutes**, **Last 24 Hours**, **Last 7 Days** or **Last 30 Days** to display the pipe traffic of the selected period.
- Click ◢ to expand sub-pipes.
- Click **Edit** to edit the selected pipe.
- Hover your mouse over the colorful lines of Traffic to view the forward traffic and backward traffic.

The traffic details of the selected pipe will be displayed at the bottom of the page, including traffic, sub-pipe stack (forward) and sub-pipe stack (backward). Only when the monitoring period is not specified as "Real-time", you can view the sub-pipe stack traffic.

- Traffic: Displays the real-time trends of the forward traffic, backward traffic and total traffic of pipes, as well as the historical trends. Hover you mouse over the lines to view the forward traffic, backward traffic and total traffic at a specific point in time. When you click **Forward Traffic**, **Backward Traffic** or **Total Traffic** at the top-right corner of the trend chart, it will turn gray and the corresponding line will be hidden; when you click it again, it will turn black and the line will appear.
- Sub-pipe Stack (Forward): Displays the trends of the forward traffic of all sub-pipes of a pipe. Hover you mouse over the lines to view the top 5 traffic and other forward traffic of sub-pipes at a specific point in time. When you click the

name of the specified sub-pipe at the top-right corner of the trend chart, it will turn gray and the corresponding line will be hidden; when you click it again, it will turn black and the line will appear.

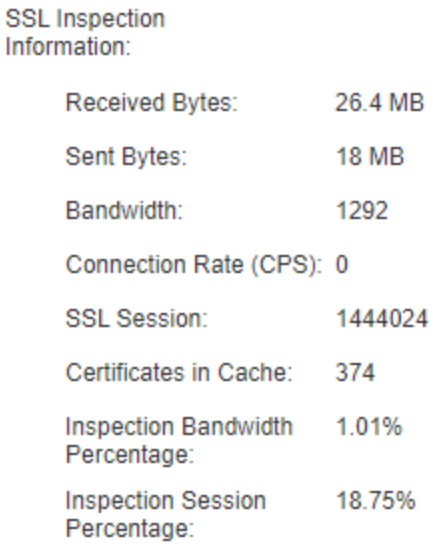
- Sub-pipe Stack (Backward): Displays the trends of the backward traffic of all sub-pipes of a pipe. Hover you mouse over the lines to view the top 5 backward traffic and other backward traffic of sub-pipes at a specific point in time. When you click the name of the specified sub-pipe in the top right corner of trend chart, it will turn gray and the corresponded line will be hidden; when you click it again, it will turn black and the line will appear.

SSL Inspection

You can view the statistics of the SSL inspection traffic.

Click **Monitor** > **SSL Inspection**. Then you can view the statistics, including the total number of received/sent bytes, the number of new connections, the bandwidth, the number of SSL sessions, the number of certificates in the cache, etc.

Click **Clear** to clear the displayed data in the page.



Global Server Load Balance Monitor

After configuring the global server load balance, you can view the statistics of the function in the monitor page.

> **Note:** The global server load balance function is controlled by a license. Only after a global server load balance license is installed, the function can be used.

DNS Server

Click **Monitor** > **Global Server Load Balance** > **DNS Server** to enter the DNS server monitor page. The page will display the following tabs:

- **DNS Server** tab: Displays all statistics of the GSLB DNS server. Click **Clear** to clear the displayed data on the page.
- **View** tab: Displays the view statistics, including the number of resource records, cache hits, etc. To clear a certain view entry, select it and click **Clear**. Click **Clear All** to clear all data.
- **Zone** tab: Displays the zone statistics, including the number of resource records, Smart DNS rule hits, etc. To clear a certain zone entry, select it and click **Clear**. Click **Clear All** to clear all data.

Click **Clear** to clear the selected entries on the page. Click **Clear All** to clear all data.

Smart DNS

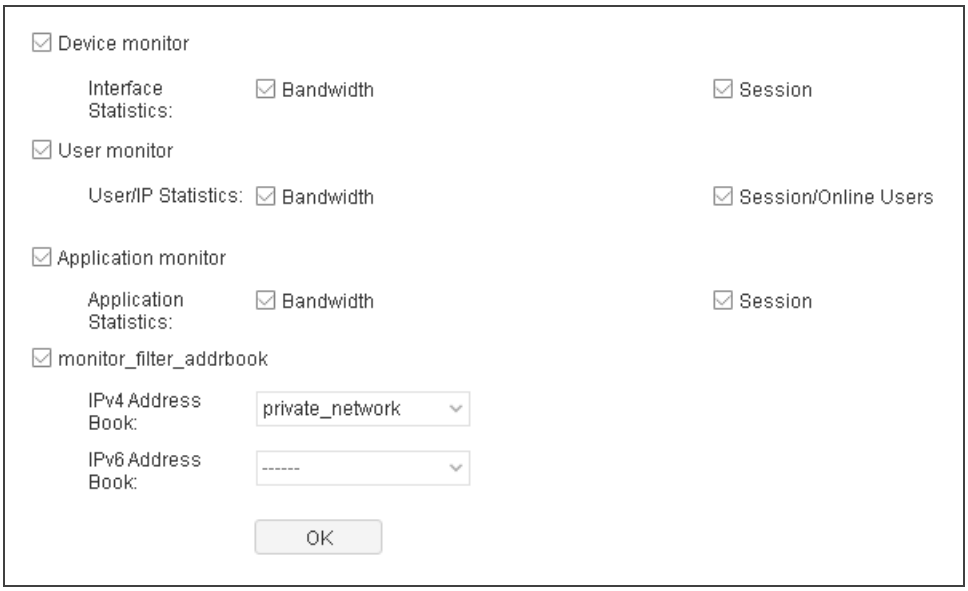
Click **Monitor** > **Global Server Load Balance** > **Smart DNS** to enter the Smart DNS monitor page. This page will display the number of successes and failures of A and AAAA record resolution in the **DNS Host**, **Virtual Server Pool** and **Virtual Server** tabs respectively.

Monitor Configuration

You can enable or disable some monitor items as needed.

To enable/disable a monitor item, take the following steps:

1. Click **Monitor** > **Monitor Configuration**.



2. Select or clear the monitor item(s) you want to enable or disable.

3. Click **OK**.

Logging

Logging is a feature that records various kinds of system logs, including device logs, threat logs, NAT logs, PBR logs, load balance logs and health check logs.

- Device Logs - Include event logs, network logs and configuration logs.
    - Event - Includes 8 severity levels: error, warning, notification, information, debugging, emergency, alert and critical.
    - Network - Logs about network services, like PPPoE and DDNS.
        - Configuration - Logs about configuration on command line interface, e.g. interface IP address setting.
    - NAT Logs - Including NAT type, source and destination IP addresses and ports.
- Session Logs - Including session protocols, source and destination IP addresses and ports.
- PBR Logs - Logs about policy-based route.
- Threat Logs - Logs related to behaviors threatening the protected system.
- L7/L4/GSLB Logs - SLB traffic logs related to load balance, including L7 load balance logs, L4 load balance logs and global server load balance logs.
- SSL Inspection Logs - Logs about SSL inspection.
- Health Check Logs - Logs about health checks of load balance.

The system logs the running status of the device, thus providing information for analysis and evidence.

Log Severity

Event logs are categorized into eight severity levels based on the severity of log messages. For specific information about each severity, refer to the following table:

Severity	Level	Description	Log Definition
Emergencies	0	Identifies illegitimate system events.	LOG_EMERG
Alerts	1	Identifies problems which need immediate attention such as device is being attacked.	LOG_ALERT

Severity	Level	Description	Log Definition
Critical	2	Identifies urgent problems, such as hardware failure.	LOG_CRIT
Errors	3	Generates messages for system errors.	LOG_ERR
Warnings	4	Generates messages for warning.	LOG_WARNING
Notifications	5	Generates messages for notice and special attention.	LOG_NOTICE
Informational	6	Generates informational messages.	LOG_INFO
Debugging	7	Generates all debugging messages, including daily operation messages.	LOG_DEBUG

Destination of Exported Logs

Log messages can be sent to the following eight destinations. You can specify a destination as needed:

- Console - The default output destination. You can close this destination via CLI.
- Remote - Includes Telnet and SSH.
- Buffer - Memory buffer.
- File - By default, the logs are sent to the specified USB destination in form of a file.
- Syslog Server - Sends logs to a UNIX or Windows Syslog Server.
- Email - Sends logs to a specified email account.
- Mobile Phone - Sends logs to a mobile phone via SMS.
- Local database - Sends logs to the local database, i.e., the 1T hard disk that comes with the device.

Log Format

To facilitate the access and analysis of the system logs, ADC logs follow a fixed pattern of information layout, i.e. **date/time, severity level@module: descriptions**. See the example below:

2013-02-05 01:51:21, WARNING@LOGIN: Admin user "admin" logged in through console from localhost.

Event Logs

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

To view event logs, select **Monitor** > **Log** > **Event Log**.

In this page, you can perform the following actions:

- Filter: Click +Filter, and according to your needs, select the time when a log is generated from the **Time** drop-down list; select a log severity level from the **Severity** drop-down list; or type the keyword you want to search into the **Message** text box. Then the logs that match the conditions will be displayed in the log list.
- Configure: Click to jump to the Log Management page.
- Clear: Click to clear all the displayed logs.
- Export: Click to export all or part of the displayed logs as a TXT or CSV file.

Network Logs

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

To view network logs, select **Monitor** > **Log** > **Network Log**.

In this page, you can perform the following actions:

- Filter: Click +Filter to add a filter condition to show logs that match the condition.
- Configure: Click to jump to the Log Management page.
- Clear: Click to clear all the displayed logs.
- Export: Click to export all or part of the displayed logs as a TXT or CSV file.

Configuration Logs

This feature may vary slightly on different platforms. Please see the actual page of the feature that your device delivers.

To view configuration logs, select **Monitor** > **Log** > **Configuration Log**.

In this page, you can perform the following actions:

- Filter: Click +Filter to add a filter condition to show logs that match the condition.
- Configure: Click to jump to the Log Management page.
- Clear: Click to clear all the displayed logs.
- Export: Click to export all or part of the displayed logs as a TXT or CSV file.

PBR Logs

This feature may not be available on all platforms. Please see the actual page of the feature that your device delivers.

PBR logs can be generated under the conditions that:

- PBR logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 493.
- You have enabled logging function in PBR rules. Refer to "Creating a Policy-based Route Rule" on Page 303.

To view PBR logs, select **Monitor** > **Log** > **PBR Log**.

In this page, you can perform the following actions:

- Filter: Click the **Filter** button, and then click +Filter to add a filter condition to show logs that match the condition. The filter conditions include:
    - Time - Displays the PBR logs within the specified time range (from start time to end time).
    - PBR Name/Rule ID - Type the PBR name into the first text box and the PBR rule ID into the second text box to display the PBR logs of the rule with the specified ID in the specified PBR.
        - Source IP - Displays the PBR logs of the specified source IP address.
        - Source Port - Displays the PBR logs of the specified source port.
        - Destination IP - Displays the PBR logs of the specified destination IP.
        - Destination Port - Displays the PBR logs of the specified destination port.
        - Protocol - Displays the PBR logs of the specified protocol.
    - Application - Displays the PBR logs of the specified application.
    - Egress Interface - Displays the PBR logs of the specified egress interface.

- Configure: Click to jump to the "Log Configuration" on Page 493 page.
- Clear: Click to clear all the displayed logs.
- Export: Click to export all the displayed logs or search results (search first and then export).

NAT Logs

NAT logs can be generated under the conditions that:

- NAT logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 493.
- You have enabled NAT logging function in NAT rules. Refer to "Configuring SNAT" on Page 373.

To view NAT logs, select **Monitor** > **Log** > **NAT Log**.

In this page, you can perform the following actions:

- Filter: Click +Filter to add a filter condition to show logs that match the condition. The filter conditions include:
  - Time - Displays the NAT logs within the specified time range (from start time to end time).
  - NAT Type - Displays the NAT logs of the specified type (SNAT).
    - ID - Displays the NAT logs of the specified ID.
  - Source IP - Displays the NAT logs of the specified source IP address.
    - Source Port - Displays the NAT logs of the specified source port.
    - Destination IP - Displays the NAT logs of the specified destination IP.
    - Destination Port - Displays the NAT logs of the specified destination port.
    - Translated IP - Displays the NAT logs of the specified translated IP address.
    - Translated Port - Displays the NAT logs of the translated port with specified number.
  - Protocol - Displays the NAT logs of the specified protocol.
- Configure: Click to jump to the "Log Configuration" on Page 493 page.
- Clear: Click to clear all the displayed logs.
- Export: Click to export all the displayed logs or search results (search first and then export).

Health Check Logs

To generate the health check logs, you need to enable the health check logging function. Refer to "Log Configuration" on Page 493.

To view health check logs, select **Monitor** > **Log** > **Health Check Log**.

In this page, you can perform the following actions:

- Filter: Click +Filter to add a filter condition to show logs that match the condition. The filter conditions include:
    - Time - Displays the health check logs within the specified time range (from start time to end time).
    - Severity - Displays the health check logs of the specified severity.
    - Status - Displays the health check logs in the specified status.
    - Service Pool - Displays the health check logs of the specified load balance server pool.
    - Real Server - Displays the health check logs of the specified real server.
        - IP - Displays the health check logs of the specified real server IP address.
        - Port - Displays the health check logs of the real server port.
    - Health Check - Displays the logs of the specified health check.
- Configure: Click to jump to the "Log Configuration" on Page 493 page.
- Clear: Click to clear all the displayed logs.
- Export: Click to export all or part of the displayed logs as a TXT or CSV file.

Threat Logs

Threat logs can be generated under the conditions that:

- Threat logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 493.
- You have enabled the Attack Defense feature. Refer to Attack Defense.

To view threat logs, select **Monitor** > **Log** > **Threat Log**.

In this page, you can perform the following actions:

- Filter: Click +Filter to add a filter condition to show logs that match the condition. The filter conditions include:
    - Detection Period - Displays the threat logs within the specified time range.
    - Type - Displays the threat logs of the specified threat type.
    - Severity - Displays the threat logs of the specified severity.
    - Source - Displays the threat logs of the specified attacking host. IPv4 and IPv6 addresses are supported.
    - Destination - Displays the threat logs of the specified victim host. IPv4 and IPv6 addresses are supported.
    - Detected by - Displays the threat logs of the specified detection engine.
    - Source Interface - Displays the threat logs of the specified source interface.
    - Destination Interface - Displays the threat logs of the specified destination interface.
    - Action - Displays the threat logs of the specified action.
  - Configure: Click to jump to the Log Management page.
- Export: Click to export all the displayed logs or search results (search first and then export).
- Clear: Click to clear all the displayed logs.
- Merge Log: In the drop-down list, select the merge type for the logs displayed in the list, including Do Not Merge, Threat Name, Source IP and Destination IP.

Session Logs

Session logs can be generated under the conditions that:

- Session logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 493.
- You have enabled logging function in policy rules. Refer to "Security Policy" on Page 357.

To view session logs, select **Monitor** > **Log** > **Session Log**.

In this page, you can perform the following actions:

- Filter: Click the **Filter** button, and then click +Filter to add a filter condition to show logs that match the condition. The filter conditions include:
  - Time - Displays the session logs within the specified time range (from start time to end time).
  - Policy ID - Displays the session logs of the policy rule with the specified ID.
  - Source IP - Displays the session logs of the specified source IP address.
  - Source Port - Displays the session logs of the specified source port.
  - Destination IP - Displays the session logs of the specified destination IP.
  - Destination Port - Displays the session logs of the specified destination port.
  - Protocol - Displays the session logs of the specified protocol.
  - Action - Displays the session logs of the specified action.
- Configure: Click to jump to the "Log Configuration" on Page 493 page.
- Clear: Click to clear all the displayed logs.
- Export: Click to export all the displayed logs or search results (search first and then export).

Note:

- For ICMP session logs, system will only record the ICMP type value and its code value. As ICMP 3, 4, 5, 11 and 12 are generated by other communications, not a complete ICMP session, system

will not record such kind of packets.

- For TCP and UDP session logs, system will check the packet length first. If the packet length is 20 bytes (i.e., with IP header, but no loads), it will be defined as a malformed packet and be dropped; if a packet is over 20 bytes, but it has errors, system will drop it either. So, such abnormal TCP and UDP packets will not be recorded.

L7 Load Balance Logs

To generate the Layer 7 load balance logs, you need to enable the load balance logging function. Refer to "Log Configuration" on Page 493.

To view L7 load balance logs, select **Monitor** > **Log** > **L7 Load Balance Log**.

In this page, you can perform the following actions:

- Filter: Click +Filter to add a filter condition to show logs that match the condition.
- Configure: Click to jump to the "Log Configuration" on Page 493 page.

L4 Load Balance Logs

To generate the Layer 4 load balance logs, you need to enable the load balance logging function. Refer to "Log Configuration" on Page 493.

To view L4 load balance logs, select **Monitor** > **Log** > **L4 Load Balance Log**.

In this page, you can perform the following actions:

- Filter: Click +Filter to add a filter condition to show logs that match the condition.
- Configure: Click to jump to the "Log Configuration" on Page 493 page.

Global Server Load Balance Logs

To generate the global server load balance logs, you need to enable the load balance logging function. Refer to "Log Configuration" on Page 493.

To view GSLB logs, select **Monitor** > **Log** > **GSLB Log**.

In this page, you can perform the following actions:

- Filter: Click +Filter to add a filter condition to show logs that match the condition.
- Configure: Click to jump to the "Log Configuration" on Page 493 page.

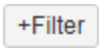
SSL Inspection Logs

SSL inspection logs can be generated under the conditions that:

- SSL inspection logging in the Logging feature is enabled. Refer to "Log Configuration" on Page 493.
- You have enabled the SSL inspection function in policy/zone rules. Refer to "Security Policy" on Page 357 or "Security Zone" on Page 219.

To view SSL inspection logs, select **Monitor** > **Log** > **SSL Inspection Log**.

In this page, you can perform the following actions:

- Filter: Click the **Filter** button, and then click 

to add a filter condition to show logs that match the condition. The filter conditions include: Time, Source IP, Source Port, Destination IP and Destination Port
- Configure: Click to jump to the "Log Configuration" on Page 493 page.
- Clear: Click to clear all the displayed logs.

Managing Logs

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

You can configure various options for different logs in the log management page.

Configuring Logs

To configure parameters of various log types, take the following steps:

1. Select **Monitor** > **Log** > **Log Management**.
2. Click on the tab of the log type you want, and you will enter the corresponding log settings. Configuration options may vary depending on different types of logs. Refer to Option Descriptions of Various Log Types.
3. Click **OK**.

Option Descriptions of Various Log Types

This section describes the options when you set the properties of each log type.

Event Log

Option	Description
Enable	Select the check box to enable the event logging function.
Console	Select the check box to export event logs to the Console. • Lowest Severity - Specify the lowest severity level. Logs below the severity level selected here will not be exported.
Terminal	Select the check box to export event logs to the terminal. • Lowest Severity - Specify the lowest severity level. Logs below the severity level selected here will not be exported.
Cache	Select the check box to export event logs to the cache. • Lowest Severity - Specify the lowest severity level. Logs below the severity level selected here will not be exported. • Max Buffer Size - The maximum size of the cached event logs.
File	Select the check box to export event logs to a file. • Lowest Severity - Specify the lowest severity level. Logs below the severity level selected here will not be exported. • Max File Size - Specify the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the syslog file into the **File Name** text box.
Log Server	Select the check box to export event logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Lowest Severity - Specify the lowest severity level. Logs below the severity level selected here will not be exported.

Option	Description
Email Address	Select the check box to export event logs to the email. • View Email Addresses: Click to see all existing email addresses or add a new address. • Lowest Severity - Specify the lowest severity level. Logs below the severity level selected here will not be exported.
Local Database	Select the check box to export event logs to the local database, i.e., the 1T hard disk that comes with the device.
SMS	Select the check box to send event logs to the SMS. • Lowest Severity - Specify the lowest severity level. Logs below the severity level selected here will not be exported.

Network Log

Option	Description
Enable	Select the check box to enable the network logging function.
Cache	Select the check box to export network logs to the cache. • Max Buffer Size - The maximum size of the cached network logs.
File	Select the check box to export network logs to a file. • Max File Size - Specify the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the syslog file into the **File Name** text box.
Log Server	Select the check box to export network logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server.
Local Database	Select the check box to export network logs to the local database, i.e., the

Option	Description
	1T hard disk that comes with the device.

Configuration Log

Option	Description
Enable	Select the check box to enable the configuration logging function.
Cache	Select the check box to export configuration logs to the cache. • Max Buffer Size - The maximum size of the cached configuration logs.
Log Server	Select the check box to export configuration logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server.
Log Speed Limit	Select the check box to define the maximum speed of generating configuration logs. • Maximum Speed - Specify the maximum speed (messages per second).
Local Database	Select the check box to export configuration logs to the local database, i.e., the 1T hard disk that comes with the device.

Threat Log

Option	Description
Enable	Select the check box to enable the threat logging function.
Terminal	Select the check box to export threat logs to the terminal.
Cache	Select the check box to export threat logs to the cache. • Max Buffer Size - The maximum size of the cached threat logs. • Lowest Severity - Specify the lowest severity level. Logs below the severity level selected here will not be exported.
File	Select the check box to export threat logs to a file.

Option	Description
	• Lowest Severity - Specify the lowest severity level. Logs below the severity level selected here will not be exported. • Max File Size - Specify the maximum size of the syslog file. The value range is 4096 to 1048576 bytes. The default value is 1048576 bytes. • Save logs to USB - Select the check box and select a USB drive (USB0 or USB1) from the drop-down list. Type a name for the syslog file into the **File Name** text box.
Log Server	Select the check box to export threat logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or plain text. • Custom Format Distributed - If you select the check box, log messages will be sent to different log servers, which will relieve the pressure of a single log server. System will select a log server using the specified algorithm, which can be Round Robin or Src IP Hash.
Email Address	Select the check box to export threat logs to the email. • View Email Addresses: Click to see all existing email addresses or add a new address.

PBR Log

Option	Description
Enable	Select the check box to enable the PBR logging function. • Record User Name: Select to show the user's name in the PBR log messages. • Record Host Name: Select to show the host's name in the PBR log mes-

Option	Description
	sages.
Cache	Select the check box to export PBR logs to the cache. • Max Buffer Size - The maximum size of the cached PBR logs.
Log Server	Select the check box to export PBR logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of plain text. • Custom Format Distributed - If you select the check box, PBR log messages will be sent to different log servers, which will relieve the pressure of a single log server. System will select a log server using the specified algorithm, which can be Round Robin or Src IP Hash.

NAT Log

Option	Description
Enable	Select the check box to enable the NAT logging function. • Record Host Name: Select to show the host's name in the NAT log messages.
Cache	Select the check box to export NAT logs to the cache. • Max Buffer Size - The maximum size of the cached NAT logs.
Log Server	Select the check box to export NAT logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or plain text • Custom Format Distributed - If you select the check box, log messages will be sent to different log servers, which will relieve the

Option	Description
	pressure of a single log server. System will select a log server using the specified algorithm, which can be Round Robin or Src IP Hash.

Load Balance Log

Option	Description
Enable	Select the check box to enable the load balance logging function.
Cache	Select the check box to export the load balance logs to the cache. • Max Buffer Size - The maximum size of the cached load balance logs.
Log Server	Select the check box to export load balance logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or plain text. • Custom Format Distributed - If you select the check box, log messages will be sent to different log servers, which will relieve the pressure of a single log server. System will select a log server using the specified algorithm, which can be Round Robin or Src IP Hash.
Local Database	Select the check box to export load balance logs to the local database, i.e., the 1T hard disk that comes with the device.

SSL Inspection Log

Option	Description
Enable	Select the check box to enable the SSL inspection logging function.
Cache	Select the check box to export SSL inspection logs to the cache. • Max Buffer Size - The maximum size of the cached SSL inspection logs.

Option	Description
Log Server	Select the check box to export SSL inspection logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or plain text. • Custom Format Distributed - If you select the check box, log messages will be sent to different log servers, which will relieve the pressure of a single log server. System will select a log server using the specified algorithm, which can be Round Robin or Src IP Hash.

GSLB Log

Option	Description
Enable	Select the check box to enable the global server load balance logging function.
Cache	Select the check box to export the global server load balance logs to the cache. • Max Buffer Size - The maximum size of the cached global server load balance logs.
Log Server	Select the check box to export global server load balance logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server. • Syslog Distribution Methods - The distributed logs can be in the format of binary or plain text. • Custom Format Distributed - If you select the check box, log messages will be sent to different log servers, which will relieve the pressure of a single log server. System will select a log server using

Option	Description
	the specified algorithm, which can be Round Robin or Src IP Hash.
Local Database	Select the check box to export global server load balance logs to the local database, i.e., the 1T hard disk that comes with the device.

Health Check Log

Option	Description
Enable	Select the check box to enable the health check logging function.
Cache	Select the check box to export health check logs to the cache. • Max Buffer Size - The maximum size of the cached health check logs.
Log Server	Select the check box to export health check logs to the syslog server. • View Log Server - Click to see all existing syslog servers or to add a new server.
Local Database	Select the check box to export health check logs to the local database, i.e., the 1T hard disk that comes with the device.

Log Configuration

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

You can create log servers, set up log email addresses, and add UNIX servers.

Log Sever Configuration

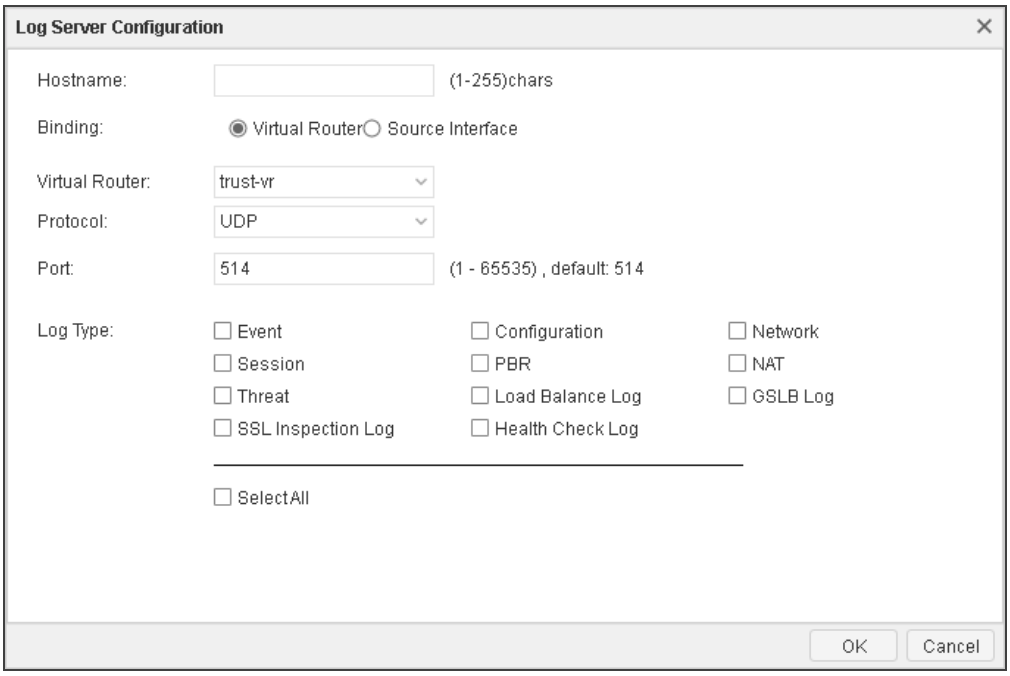
In the Log Server Configuration dialog box, you can create, edit or delete a log server for receiving log messages, as well as configure the log encoding.

Creating a Log Server

To create a log server, take the following steps:

1. Select **Monitor** > **Log** > **Log Configuration**, and click **Log Server Configuration** tab.

2. Click **New**.



In the Log Server Configuration dialog box, configure these values.

Option	Description
Hostname	Enter the name or IP of the log server.
Binding	Specify the source IP address to receive logs, including: • Virtual Router: Select **Virtual Router** and then select a virtual router form the drop-down list. • Source Interface: Select **Source Interface** and then select a source interface from the drop-down list. The device will use the IP address of the interface as the source IP to send logs to the syslog server. If management IP address is configured on the interface, the management IP address will be preferred.
Protocol	Specify the protocol type of the syslog server. If "Secure-TCP" is selected, you can select **Do not validate the server certificate** option, and system can transfer logs normally and do not need any certifications.

Option	Description
Port	Specify the port number of the syslog server.
Log Type	Specify the log types the syslog server will receive.

3. Click **OK** to save the settings.

Note: You can add at most 15 log servers.

Configuring Log Encoding

The default encoding format for the log information that is output to the log server is utf-8, and you can enable GBK encoding as needed. After the GBK encoding format is enabled, the log encoding format that is output to the log server will be GBK encoding. To enable the GBK encoding, take the following steps:

1. Select **Monitor** > **Log** > **Log Configuration**, and click **Log Server Configuration** tab.
2. Click **Log Encoding Configuration** at the top-right corner to open the Log Encoding Configuration dialog box.
3. Select the check box to enable the GBK encoding.
4. Click **OK** to save the settings.

Adding Email Address to Receive Logs

An email in the log management setting is an email address for receiving logs.

To add an email address, take the following steps:

1. Select **Monitor** > **Log** > **Log Configuration**, and click **Web Mail Configuration** tab.
2. Type an email address into the **Email Address** text box, and click **Add**.
3. If you want to delete an existing email, click **Delete** corresponding to the email entry in the Operation column in the list.

Note: You can add at most 3 email addresses.

Specifying a Unix Server

You can specify the name of the UNIX log server. This option can only be used to export logs to a UNIX log server.

To specify a Unix server to receive logs, take the following steps:

1. Select **Monitor** > **Log** > **Log Configuration**, and click **Facility Configuration** tab.
2. Select the device you want and the logs will be exported to that Unix server.
3. Click **OK** to save the settings.

Specifying a Mobile Phone

You can specify the mobile phone number to receive SMS. The option can only be used to send logs to a mobile phone via SMS.

To specify a mobile phone to receive logs, take the following steps:

1. Select **Monitor** > **Log** > **Log Configuration**, and click **SMS Configuration** tab.
2. Type a mobile phone number into the **Mobile Phone** text box, and click **Add**.
3. If you want to delete an existing mobile phone number, click **Delete** corresponding to the mobile phone number in the Operation column in the list.

Note: You can add at most 3 mobile phone numbers.

Chapter 14 System Management

The device's maintenance and management include:

System Information

You can view the general information of system in the System Information page, including Serial Number, Hostname, Platform, System Time, System Uptime, Firmware, Signature Database and so on.

Viewing System Information

To view system information, select **System** > **System Information**.

Option	Description
Serial Number	Show the serial number of the device.
Hostname	Show the name of the device.

Option	Description
Platform	Show the platform model of the device.
System Time	Show the system date and time of the device.
System Uptime	Show the system uptime of the device.
Firmware	Show the current firmware version of the device and the last update time.
Boot File	Show the current boot file of the device.

Device Management

This section introduces how to configure the Administrator, Trust Host, MGT Interface, System Time, NTP Key and system options.

Administrators

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

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

- Administrator: Permission for reading, executing and writing. This role has the authority over all features. You can view the current or historical configuration information.
  - Operator: You have the authority over all features except modifying the Administrator's configuration, but no permission to check the log information.
  - Auditor: You can only operate on the log information, including view, export and clear.
  - Administrator(read-only): Permission for reading and executing. You can view the current or historical configuration information.

Note:

- The device ships with a default administrator named hillstone. You can modify the setting (password and access method only) of hillstone. However, this account cannot be deleted.
- Other administrator roles (except default administrator) cannot configure the admin settings,

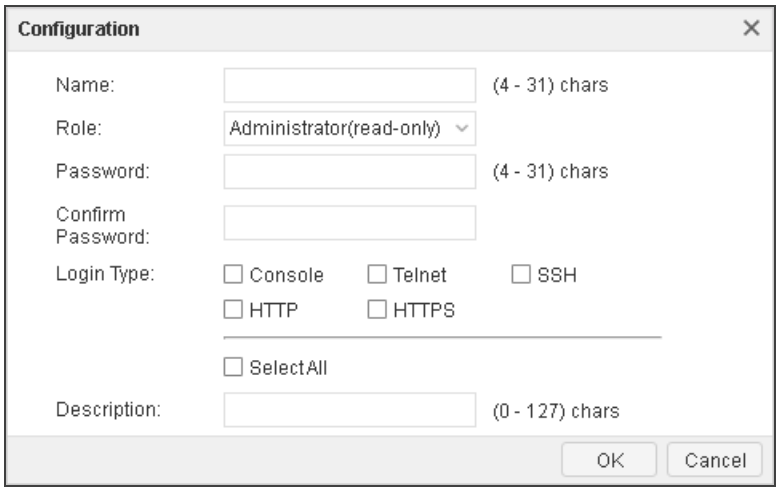
except modifying its own password.

- The system auditor can manage one or more logs, but only the system administrator can manage the log types.

Creating an Administrator Account

To create an administrator account, take the following steps:

1. Select **System** > **Device Management** > **Administrators**.
2. Click **New**.



In the Configuration dialog box, configure the following options.

Option	Description
Name	Type a name for the system administrator account.
Role	From the **Role** drop-down list, select a role for the administrator account. Different roles have different privileges. • Administrator: Permission for reading, executing and writing. This role has the authority over all features. • Operator: This role has the authority over all features except modi-

Option	Description
	fying the Administrator’s configurations, but has no permission to check the log information. • Auditor: You can only operate on the log information, including the view, export and clear. • Administrator(read-only): Permission for reading and executing. You can view the current or historical configuration information.
Password	Type a login password for the admin into the **Password** box. The password should meet the requirements of Password Strategy.
Confirm Password	Re-type the password into the **Confirm Password** box.
Login Type	Select the access method(s) for the admin, including Console, Telnet, SSH, HTTP and HTTPS. If you need all access methods, select **Select All**.
Description	Enter descriptions for the administrator account.

3. Click **OK**. The new administrator account will be displayed in the administrator list.

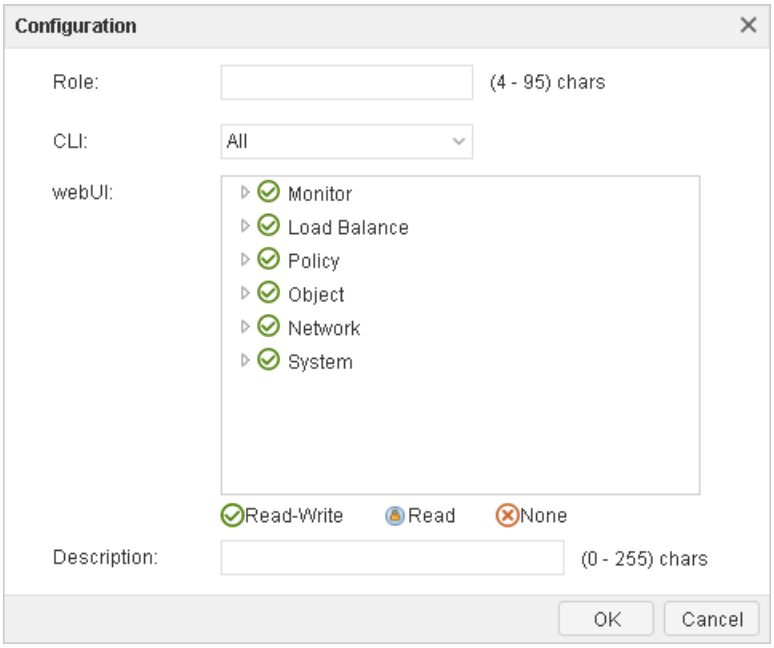
Admin Roles

Device administrators of different roles have different privileges. System supports pre-defined administrator roles and customized administrator roles. The pre-defined administrator role cannot be deleted or edited. You can customize administrator roles according to your requirements.

To create a new administrator role, take the following steps:

1. Select **System** > **Device Management** > **Admin Roles**.

2. Click **New**.



In the Configuration dialog box, configure the following options.

Option	Description
Role	Enter the role name.
CLI	Specify the administrator role's privileges of CLI, including All and None.
WebUI	Click module name to set the administrator role's privilege. represents the administrator role can read and edit the configurations of the specified module. represents the administrator role has the read privilege of the specified module, but cannot edit the configurations. represents the administrator role does not have privilege of the specified module, and cannot read and edit the configurations of the specified module.
Description	Specify the description for this administrator role.

3. Click **OK**. The new administrator role will be displayed in the administrator role list.

Trusted Host

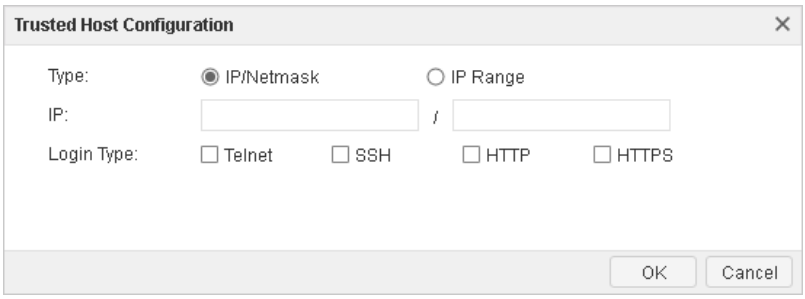
The device only allows the trusted host to manage the system to enhance the security. Administrator can specify an IP range, and hosts in the specified IP range are trusted hosts. Only trusted hosts could access the management interface to manage the device.

Note: If system cannot be managed remotely, check the trusted host configuration.

Creating a Trusted Host

To create a trust host, take the following steps:

1. Select **System** > **Device Management** > **Trusted Host**.
2. Click **New**.



In the Trusted Host Configuration dialog box, configure the following options.

Option	Description
Type	Specify the type of host. You can select **IP/Netmask** or **IP Range**. • IP/Netmask: Type the IP address and netmask into the **IP** box respectively. • IP Range: Type the start IP and end IP into the **IP** box respectively.
Login Type	Select the access methods for the trust host, including Telnet, SSH, HTTP and HTTPS.

3. Click **OK**. The new host will be displayed in the host list.

Management Interface

The device supports the following access methods: Console, Telnet, SSH and WebUI. You can configure the timeout value, port number, PKI trust domain of HTTPS, and PKI trust domain of certificate authentication. When accessing the device through Telnet, SSH, HTTP or HTTPS, if login fails three times in one minute, the IP address that attempts the login will be blocked for 2 minutes during which the IP address cannot connect to the device.

To configure the access methods, take the following steps:

1. Select **System** > **Device Management** > **Management Interface**.

2. **In the Management Interface tab, configure the following options.**

Option	Description
Console	Configure the Console access method parameters. • Timeout: Type the Console timeout value into the **Timeout** box. The value range is 0 to 60 minutes. The default value is 10. The value of 0 indicates never timeout. If there is no activity until the timeout, system will drop the console connection.
Telnet	Configure the Telnet access method parameters. • Timeout: Specify the Telnet timeout value. The value range is 1 to 60 minutes. The default value is 10. • Port: Specify the Telnet port number. The value range is 1 to 65535. The default value is 23.
SSH	Configure the SSH access method parameters. • Timeout: Specify the SSH timeout value. The value range is 1 to 60 minutes. The default value is 10. • Port: Specify the SSH port number. The value range is 1 to 65535. The default value is 22.
Web	Configure the WebUI access method parameters. • Multiple Login with Same Account: Select the check box and users are allowed to log in to devices with the same account simultaneously. By

Option	Description
	default, the function is disabled. In the default situation, when a same account is used to log in again, the previous login account will be kicked out. • Timeout: Specify the WebUI timeout value. The value range is 1 to 1440 minutes. The default value is 10. • HTTP Port: Specify the HTTP port number. The value range is 1 to 65535. The default value is 80. • HTTPS Port: Specify the HTTPS port number. The value range is 1 to 65535. The default value is 443. • HTTPS Trust Domain: Select a PKI trust domain existing in system from the drop-down list. After logging into the device over HTTPS, HTTPS server will use the certificate with the specified PKI trust domain. • Certificate Authentication: Select this check box to enable the certificate authentication. The certificate includes the digital certificate of users and secondary CA certificate signed by the root CA. Certificate authentication is one of two-factor authentication. The two-factor authentication does not only need the user’s name and password authentication, but also other authentication methods, like a certificate or fingerprint. • Certificate Trust Domain: After enabling the certificate authentication and logging into the device over HTTPS, HTTPS server will use the certificate with the specified PKI trust domain. Make sure that root CA certificate is imported into it. • CN Check: After the CN check is enabled, the name of the root CA certificate is checked and verified when the user logs in. Only the certificate and the user can be consistent, and the login succeeds.

3. Click **OK**.

Note: When changing HTTP port, HTTPS port or HTTPS Trust Domain, the web server will restart. You may need to log in again if you are using the Web interface.

System Time

You can configure the current system time manually, or synchronize the system time with the NTP server time via NTP protocol.

Configuring the System Time Manually

To configure the system time manually, take the following steps:

1. Select **System** > **Device Management** > **System Time**.
2. Under System Time Configuration in the System Time tab, configure the following.

Option	Description
Sync with Local PC	Specify the method of synchronizing with local PC. You can select **Sync Time** or **Sync Zone&Time.** • **Sync Time**: Synchronize the system time with local PC. • **Sync Zone&Time**: Synchronize the system zone&time with local PC.
Specified the system time	Configure parameters of system time. • Time Zone: Select the time zone from the drop-down list. • Date: Specify the date. • Time: Specify the time.

3. Click **OK**.

Configuring NTP

The system time may affect the establishment time of the VPN tunnel and schedule, so the accuracy of the system time is very important. To ensure the system is able to maintain an accurate time, the device allows you to synchronize the system

time with a NTP server on the network via NTP protocol.

To configure NTP, take the following steps:

1. Select **System** > **Device Management** > **System Time**.

2. **Under NTP Configuration in the System Time tab, configure the following.**

Option	Description
Enable	Select the **Enable** check box to enable the NTP function. By default, the NTP function is disabled.
Authentication	Select the **Authentication** check box to enable the NTP Authentication function.
Server	Specify the NTP server that the device needs to synchronize with. You can specify at most 3 servers. • IP: Type the IP address of the server into the box. • Key: Select a key from the **Key** drop-down list. If you enable the NTP Authentication function, you must specify a key. • Virtual Router: Select the Virtual Router of interface for NTP communication from the drop-down list. • Source Interface: Select an interface for sending and receiving NTP packets from the drop-down list. • Specify as a preferred server: Click **Specify as a preferred server** to set the server as the first preferred server. System will synchronize with the first preferred server.
Sync Interval	Type the interval value into the box. The device will synchronize the system time with the NTP server at the interval you specified to ensure the system time is accurate.
Time Offset	Type the max adjustment time value into the box. If the time difference between the system time and the NTP server’s time is within the max adjustment value you specified, the synchronization will succeed, otherwise it will fail.

3. Click **OK**.

NTP Key

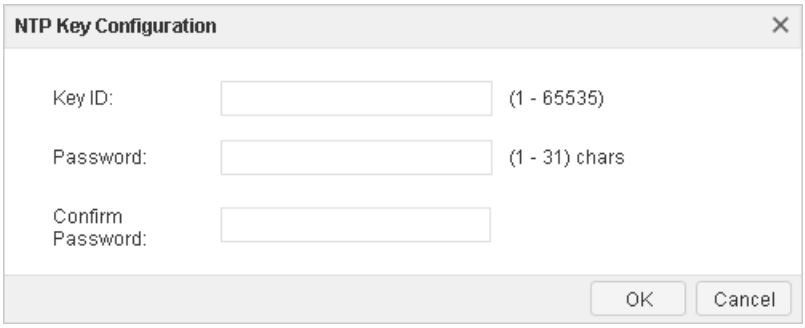
After enabling NTP Authentication function, you need to configure MD5 key ID and keys. The device will only synchronize with the authorized servers.

Creating a NTP Key

To create a NTP Key, take the following steps:

1. Select **System** > **Device Management** > **NTP Key**.

2. Click New. In the NTP Key Configuration dialog box, configure the following options.



Option	Description
Key ID	Type the ID number into the **Key ID** box. The value range is 1 to 65535.
Password	Type a MD5 key into the **Password** box. The value range is 1 to 31.
Confirm Password	Re-type the same MD5 key you have entered into the **Confirm Password** box.

3. Click **OK**. Then this piece of NTP key information will be added to the NTP key list.

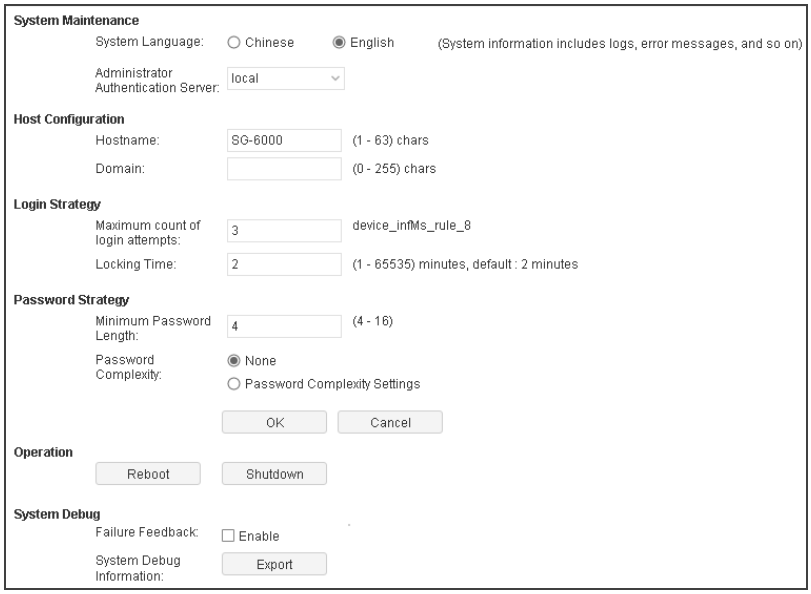
Option

You can specify system options, including system language, administrator authentication server, host name, password strategy, reboot and exporting the system debugging information.

To change system options, take the following steps:

1. Select **System** > **Device Management** > **Option**.

2. Configure the following.



Option	Description
System Maintenance	Configure the system language and administrator authentication server. • System Language: You can select **Chinese** or **English** according to your own requirements. • Administrator Authentication Server: Select a server to authenticate the administrator from the drop-down list.
Host Configuration	In some situation, more than one devices are installed within a network. To distinguish among these devices, different names should be assigned to different devices. The default host name is assigned according to the model. • Hostname: Type a host name you want to specify into the **Hostname** box. • Domain: Type a domain name you want to specify into the **Domain** box.

Option	Description
Login Strategy	Configure login strategy for administrator , including maximum count of login attempts and locking time. When the number of login attempts is less than or equal to 2, system will remind user "Login Failed, only x attempts left to login", where x represents the actual number of login attempts. • Maximum count of login attempts： Specify the maximum number of login attempts of an IP. The value range is from 1 to 5. The default value is 3. When user log on system through an client IP with a certain access method, and the number of password input exceeds the maximum number, user cannot log on system through the client with the same access method in the locking time. • Locking time： Specify the locking time. When the number of login attempts exceeds the maximum number, system will lock client IP and corresponding login type within the locking time. The value range is from 1 to 65535 minutes. The default value is 2 minutes.

Password Strategy	Configure password complexity for the admin user.
	• Minimum Password Length: Specify the minimum length of the password. The value range is 4 to 16 characters. The default value is 4.
	• Password Complexity: **None** means no restriction on the selection of password characters. You can select **Password Complexity Settings** to enable password complexity checking and configure password complexity:
	  • Capital letters length: The default value is 2 and the range is 0 to 16.
	  • Small letters length: The default value is 2 and the range is 0 to 16.
	  • Number letters length: The default value is 2 and the range is 0 to 16.

Option	Description
	• Special letters Length: The default value is 2 and the range is 0 to 16. • Validity Period: The range is 0 to 365 days. The default value is 0, which indicates that there is no restriction on validity period of the password.

3. Click **OK**.

Rebooting System

Some operations like license installation or image upgrading will require system to reboot before it can take effect.

To reboot system, take the following steps:

1. Select **System** > **Device Management** > **Option**.
2. Click **Reboot**, and select **Yes** in the prompt.
3. System will reboot.

System Debug

System debug is supported for you to check and analyze the problems.

Failure Feedback

To enable the failure feedback function, take the following steps:

1. Select **System** > **Device Management** > **Option**.
2. In the System Debug section, select the **Enable** check box for Failure feedback, and then system will automatically send the technical support file to the manufacturer.

System Debug Information

System debugging helps you to diagnose and identify system errors by the exported file.

To export the system debugging information, take the following steps:

1. Select **System** > **Device Management** > **Option**.

2. Click **Export**, system will pack the file in /etc/local/core and prompt to save tech-support file. After selecting the saved location and click **OK**, you can export the file successfully.

Configuration File Management

This feature may vary slightly on different platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

System configuration information is stored in the configuration file, and it is stored and displayed in the format of command line. The information that is used to initialize the Hillstone device in the configuration file is known as the initial configuration information. If the initial configuration information is not found, the Hillstone device will use the default parameters for the initialization. The information being taking effect is known as the current configuration information.

System initial configuration information includes current initial configuration information (used when system starts) and backup initial configuration information. System records the latest ten pieces of saved configuration information, and the most recently saved configuration information for system will be recorded as the current initial configuration information. The current configuration information is marked as Startup; the previous nine pieces of configuration information is marked with number from 0 to 8, in the order of save time.

You can not only export or delete the saved configuration files, but also export the current system configurations.

Managing Configuration File

To manage the system configuration files, take the following steps:

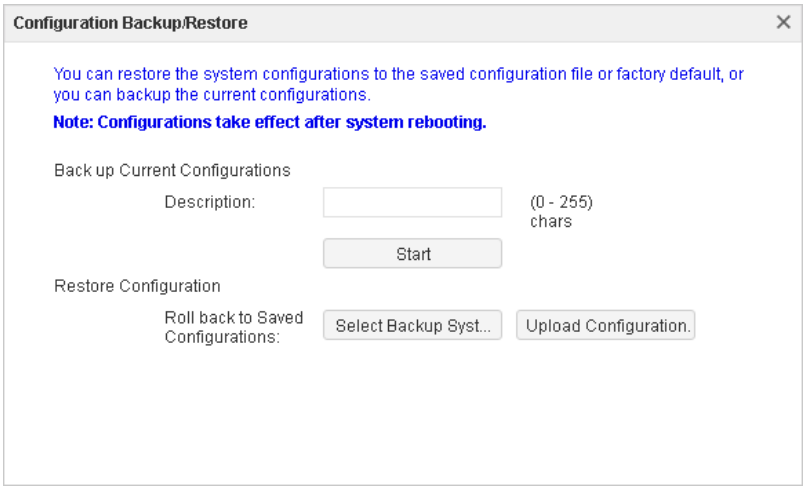
1. Select **System** > **Configuration File Management** > **Configuration File List**.

2. In the Configuration File List page, configure the following:

   - Export: Select the configuration file you want to export, and click **Export**.

   - Delete: Select the configuration file you want to delete, and click **Delete**.

   - Backup Restore: You can restore the system configurations to the saved configuration file or factory default, or you can backup the current configurations.



In the Configuration Backup/Restore dialog box, configure the following.

Option	Description
Back up Current Configurations	Type descriptions for the configuration file into **Description** box. Click **Start** to backup.
Restore Configuration	Roll back to Saved Configurations: • Select Backup System Configuration File: Click this button, then select a configuration file you want from the Backup Configuration File list. Click **OK**. • Upload Configuration File: Click this button. In the Importing Configuration File dialog box, click **Browse** and choose a local configuration file you need in your PC. If you need to make the configuration file take effect, select the check box. Click **OK**. Restore to Factory Defaults: • Click **Restore**. In the Restore to Factory Defaults dialog box, click **OK**.

Note: Device will be restored to factory defaults. Meanwhile, all the system configurations will be cleared, including backup system configuration files.

Viewing the Current Configuration

To view the current configuration file, take the following steps:

1. Select **System** > **Configuration File Management** > **Current Configurations**.
2. Click **Export** to export the current configuration file.

Importing/Exporting the Configuration of All VSYS

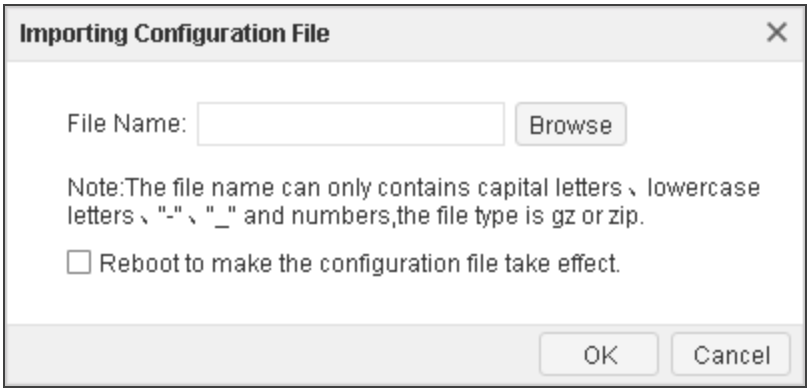
You can export the current configuration file of VSYS, and import the saved configuration file of VSYS.

To export the current configuration file of VSYS, take the following steps:

1. Select **System** > **Configuration File Management** > **Configuration File List**.
2. Click **Export All Vsys Configuration** to export the current configuration file of VSYS.

To import the saved configuration file of VSYS, take the following steps:

1. Select **System** > **Configuration File Management** > **Configuration File List**.
2. Click **Import All Vsys Configuration**.



3. Click **Browse** to select the configuration file needed to be imported. The file type can be GZ and ZIP.
4. The imported configuration file will only take effect after you reboot system. Select the **Reboot to make the configuration file take effect** checkbox to reboot immediately.
5. Click **OK**.

SNMP

The device is designed with a SNMP Agent, which can receive the operation request from the Network Management System and give the corresponding information of the network and the device.

The device supports SNMPv1 protocol, SNMPv2 protocol and SNMPv3 protocol. SNMPv1 protocol and SNMPv2 protocol use community-based authentication to limit the Network Management System to get device information. SNMPv3 protocol introduces a user-based security module for information security and a view-based access control module for access control.

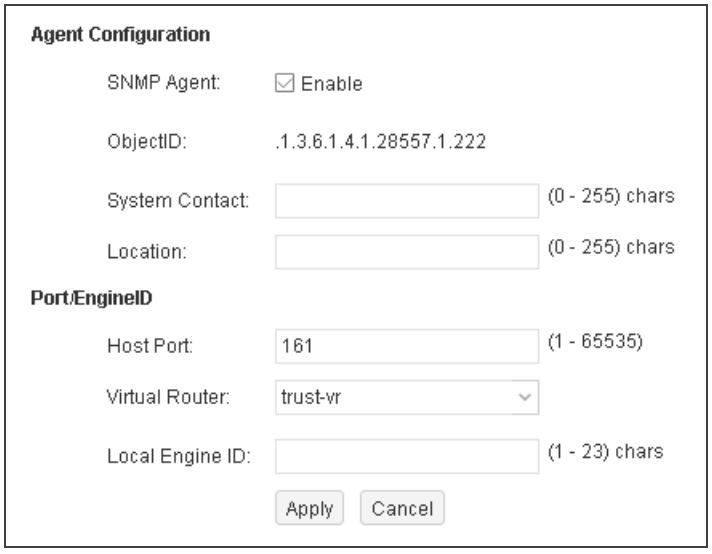
The device supports all relevant Management Information Base II (MIB II) groups defined in RFC-1213 and the Interfaces Group MIB (IF-MIB) using SMIv2 defined in RFC-2233. Besides, system offers a private MIB, which contains the system information, IPSec VPN information and statistics information of the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

SNMP Agent

The device is designed with a SNMP Agent, which provides network management and monitors the running status of the network and devices by viewing statistics and receiving notification of important system events.

To configure an SNMP Agent, take the following steps:

1. Select **System** > **SNMP** > **SNMP Agent**.
2. **In the SNMP Agent page, configure these values.**



Option	Description
SNMP Agent	Select the **Enable** check box for Service to enable the SNMP Agent function.
ObjectID	The Object ID displays the SNMP object ID of system. The object ID is specific to an individual system and cannot be modified.
System Contact	Type the SNMP system contact information of the device into the **System Contact** box. System contact is a management variable of the group system in MIB II and it contains the ID and contact of relevant administrator of the managed device. By configuring this parameter, you can save the important information to the device for the possible use in case of emergency.
Location	Type the location of the device into the **Location** box.
Host Port	Type the port number of the managed device into the **Host Port** box.
Virtual Router	Select a VRouter from the **Virtual Router** drop-down list.
Local EnginelID	Type the SNMP engine ID into the **Local EngineID** box.

3. Click **Apply**.

Note: SNMP Engine ID identifies an engine uniquely. SNMP Engine is an important component of the SNMP entity (Network Management System or managed network device) which implements the

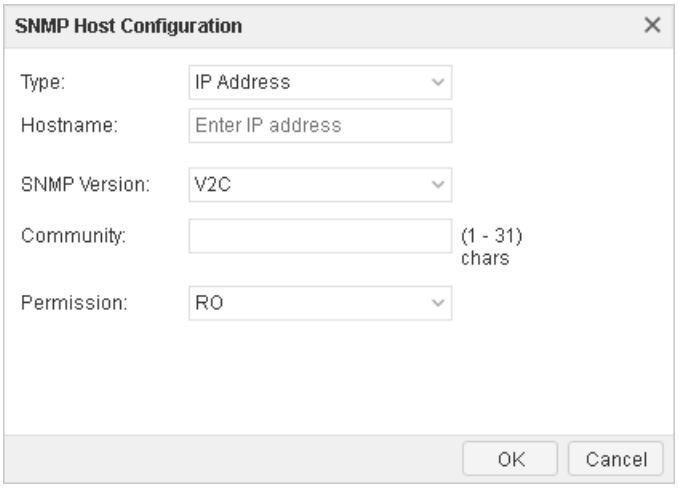
functions like the reception/sending and verification of SNMP messages, PDU abstraction, encapsulation, and communications with SNMP applications.

SNMP Host

To create an SNMP host, take the following steps:

1. Select **System** > **SNMP** > **SNMP Host**.

2. **Click New. In the SNMP Host dialog box, configure these values.**



Option	Description
Type	Select the SNMP host type from the **Type** drop-down list. You can select **IP Address**, **IP Range** or **IP/Netmask**. • IP Address: Type the IP address for the SNMP host into **Hostname** box. • IP Range: Type the start IP and end IP into the **Hostname** box respectively. • IP/Netmask: Type the start IP address and Netmask for the SNMP host into the **Hostname** box respectively.
SNMP Version	Select the SNMP version from the **SNMP Version** drop-down list.
Community	Type the community for the SNMP host into the **Community** box. Community is a password sent in clear text between the manager and the agent. This option is only effective if the SNMP version is V1 or V2C.
Permission	Select the read and write permission for the community from the **Permission** drop-down list. This option is only effective if the SNMP version is V1 or V2C. • RO: Stands for read-only. The read-only community is only allowed to read the MIB information.

3. Click **OK**. The new SNMP host will be displayed in the SNMP host list.

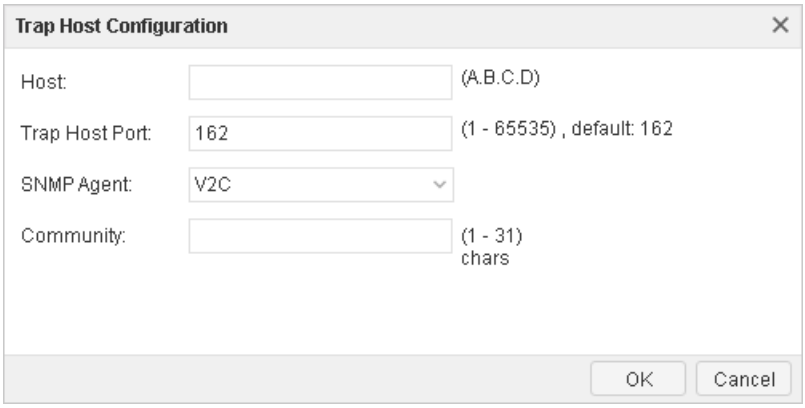
Trap Host

You can configure the SNMP Trap host to receive SNMP Trap packets.

To create a Trap host, take the following steps:

1. Select **System** > **SNMP** > **Trap Host**.

2. **Click New. In the Trap Host Configuration dialog box, configure these values.**



Option	Description
Host	Type the IP address of the Trap host into the **Host** box.
Trap Host Port	Type the port number for the Trap host into the **Trap Host Port** box.
SNMP Agent	Select a SNMP version from the **SNMP Agent** drop-down list. You can select V1, V2C or V3. • V1 or V2C: Type the community for the Trap host into the **Community** box. • V3: Select the V3 user from the **V3 User** drop-down list. Type the Engine ID for the trap host into the **Engine ID** box.

3. Click **OK**. The new Trap host will be displayed in the Trap host list.

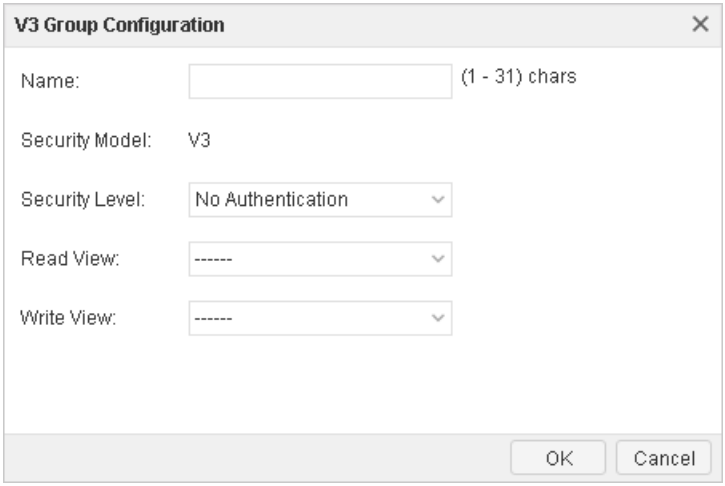
V3 User Group

SNMPv3 protocol introduces a user-based security module. You need to create an SNMP V3 user group for the SNMP host if the SNMP version is V3.

To create a V3 user group, take the following steps:

1. Select **System** > **SNMP** > **V3 User Group**.

2. **Click New. In the V3 Group Configuration dialog box, configure these values.**



Option	Description
Name	Type the SNMP V3 user group name into the **Name** box.
Security Model	Displays the security model for the SNMP V3 user group.
Security Level	Select the security level for the user group from the **Security Level** drop-down list. Security level determines the security mechanism used in processing an SNMP packet. Security levels for V3 user groups include **No Authentication** (no authentication and encryption), **Authentication** (authentication algorithm based on MD5 or SHA) and **Authentication and Encryption** (authentication algorithm based on MD5 or SHA and message encryption based on AES and DES).
Read View	Select the read-only MIB view name for the user group from the **Read**

Option	Description
	View drop-down list. If this parameter is not specified, all MIB views will be none.
Write View	Select the write MIB view name for the user group from the **Write View** drop-down list. If this parameter is not specified, all MIB views will be none.

3. Click **OK**. The new V3 user group will be displayed in the V3 user group list.

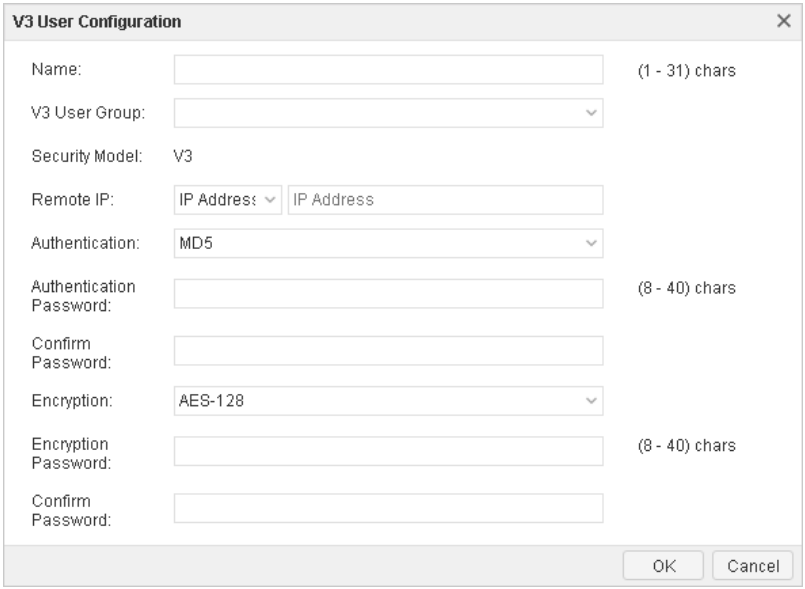
V3 User

If the selected SNMP version is V3, you need to create an SNMP V3 user group for the SNMP host and then add users to the user group.

To create a user for an existing V3 user group, take the following steps:

1. Select **System** > **SNMP** > **V3 User**.

2. **Click New. In the V3 User Configuration dialog box, configure these values.**



Option	Description
Name	Type the SNMP V3 user name into the **Name** box.
V3 User Group	Select an existing user group for the user from the **V3 User Group** drop-

Option	Description
	down list.
Security Model	Displays the security model for the SNMP V3 user.
Remote IP	Type the IP address of the remote management host into the **Remote IP** box.
Authentication	Select the authentication protocol from the **Authentication** drop-down list. By default, this parameter is None, i.e., no authentication.
Authentication Password	Type the authentication password into the **Authentication Password** box.
Confirm Password	Re-type the authentication password into the **Confirm Password** box to confirm.
Encryption	Select the encryption protocol from the **Encryption** drop-down list.
Encryption Password	Type the encryption password into the **Encryption Password** box.
Confirm Password	Re-type the encryption password into the **Confirm Password** box to confirm.

3. Click **OK**. The new V3 user will be displayed in the V3 user list.

Upgrading System

The firmware upgrade wizard helps you:

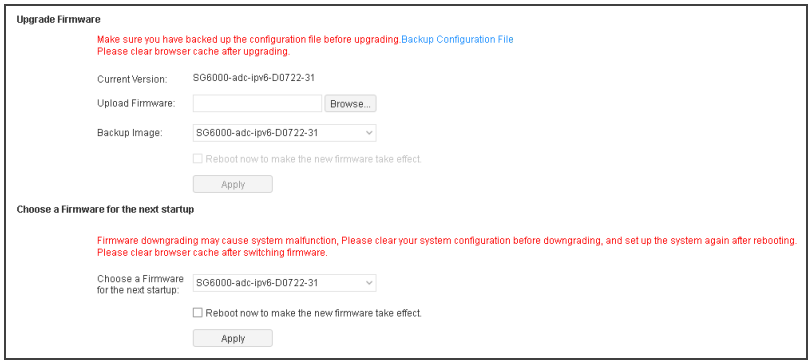
- Upgrade Firmware
- Update Signature Database
- Update Information Database

Upgrading Firmware

To upgrade firmware, take the following steps:

1. Select **System** > **Upgrade Management** > **Upgrade Firmware**.

2. In the Upgrade Firmware page, configure the following.



Upgrade Firmware	
Backup Configuration File	Make sure you have backed up the configuration file before upgrading. Click **Backup Configuration File** to backup the current firmware file. After the backup, system will automatically redirect to the Configuration File Management page, and the backed up files will be displayed in the configuration file list.
Current Version	Shows the current firmware version.
Upload Firmware	Click **Browse** to select a firmware file from your local disk.
Backup Version	Shows the backup firmware version.
Reboot	Select the **Reboot now to make the new firmware take effect** check box and click **Apply** to reboot system and make the firmware take effect. If you click **Apply** without selecting the check box, the firmware will take effect after the next startup.
Choose a Firmware for the next startup	
Choose a Firmware for the next startup	Select the firmware that will take effect for the next startup.
Reboot	Select the **Reboot now to make the new firmware take effect** check box and click **Apply** to reboot system and make the firmware take effect. If you

Upgrade Firmware	
	click **Apply** without selecting the check box, the firmware will take effect after the next startup.

Updating Signature Database

You can only view the signature databases installed with licenses.

To update signature database, take the following steps

1. Select **System** > **Upgrade Management** > **Signature Database Update**.

2. In the Signature Database Update page, configure the following.

Option	Description
Current Version	Shows the current version number.
Remote Update	Configure parameters for remotely updating the signature database. • Update Now: Click **Update** to update the signature database right now. • Auto Update: Select **Enable Auto Update** and specify the auto update time. Click **Save**, and system will automatically update the signature database according to the specified time. • Configure Update Server: Hillstone devices provide two default update servers: https://update1.hillstonenet.com and https://update2.hillstonenet.com. You can customize the servers as needed: Click **Configure Update Server**, and in the pop-up Auto Update Settings dialog box, specify the server IP or domain name. • Configure Proxy Server: When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various signature databases can update normally. Click **Configure Proxy Server**, then enter the IP addresses and ports of the main proxy server and the backup proxy server.

Option	Description
Local Update	To upload a local file for updating, click **Browse** and select the signature file in your local PC, and then click **Upload**.

Updating Information Database

The IP geography database, domain geography database and ISP database share the same update method. To update one of them, take the following steps:

1. Select **System** > **Upgrade Management** > **Information Database Update**.

2. In the Information Database Update page, configure the following.

Option	Description
Current Version	Shows the current version number.
Remote Update	Configure parameters for remotely updating the information database. • Update Now: Click **Update** to update the information database right now. • Auto Update: Select **Enable Auto Update** and specify the auto update time. Click **Save**, and system will automatically update the information database according to the specified time. • Configure Update Server: Hillstone devices provide two default update servers: https://update1.hillstonenet.com and https://update2.hillstonenet.com. You can customize the servers as needed: Click **Configure Update Server**, and in the pop-up Auto Update Settings dialog box, specify the server IP or domain name. • Configure Proxy Server: When the device accesses the Internet through a HTTP proxy server, you need to specify the IP address and the port number of the HTTP proxy server. With the HTTP proxy server specified, various information databases can update normally. Click **Configure Proxy Server**, then enter the IP addresses and ports of the main proxy server and the backup proxy server.

Option	Description
Local Update	To upload a local file for updating, click **Browse** and select the information database file in your local PC, and then click **Upload**.

License

Licenses are used to authorize users to use certain features or services, or extend the performance.

License classes and rules are as follows:

Platform License	Description	Valid Time
Platform Trial	Platform license is the basis of the other licenses operation. If the platform license is invalid, the other licenses are not effective. The device has been pre-installed with platform trial license valid for 15 days in the factory, which supports the same functions as platform base license.	You cannot modify the existing configuration when the license expires. System will restore to factory defaults when the device reboots.
Platform Base	You can install the platform base license after the device formal sale.	System cannot upgrade the OS version when the license expires, but could still work normally.
Function License	**Description**	**Valid Time**
Feature Trial License	Providing the trial of GSLB, QoS, LLB and other functions.	-
GSLB License	Providing the global server load balance function.	Permanent.
QoS License	Providing the QoS function.	System cannot upgrade the QoS function and cannot provide the maintenance service when the license expires.
VSYS License	Authorizing the available number of VSYS.	Permanent.

Service License	Description	Valid Time
APP signature	Allowing the APP signature database to be upgraded. APP signature license is issued with platform license, you do not need to apply for it. Its validity is the same as that of the platform license.	System cannot upgrade the APP signature database when the license expires.

vADC Licenses

vADC licenses are categorized to platform licenses, sub licenses, and function licenses. A platform license is the base to install all other types of licenses.

After the installation of the new platform license, the SN number of the device will be changed to a virtual SN (vSN for short). If you want to continue to obtain function or sub licenses, they can be applied through the vSN number. For the new license does not depend on the SN number of the original system after the re-installation of system, the new license that was originally applied for can still be effective. At the same time, Hillstone provides the public network license server and the internal network LMS (License Management System) to verify and manage licenses, which can ensure the security of licenses.

Note: If your vADC is a full license product, you do not need to purchase or install any license. It is already a full feature device when you purchase it.

Platform Licenses

vADC is pre-installed with a free default license without application. You can apply for the platform sub license and platform base license as needed.

- **Default License**

  vADC has a built-in free default license. All features are available in system with default license. However, performance is limited, e.g., only 500 concurrent HTTP sessions are supported. The license is valid for 30 days. After expiration, all functions of system cannot be used, the OS version and all the signature databases cannot be upgraded.

- **Platform Sub License**

  After the installation of Platform Sub License, you will get the same features as system with Platform Base License. But

the duration will be shorter. The duration is determined by the agreement you signed, which is an absolute period, for example, March 1 to March 31. After expiration, the existing configuration cannot be modified. After the reboot, only the platform functions are available while the performance is limited.

- **Platform Base License**

  When a vADC is officially purchased, you can buy a Platform Base License. Platform Base License provides fundamental application delivery features, and can ensure the vADC reach the nominal performance. When it expires, system can be normally functioning, but cannot be upgraded to higher version.

Note:

When the platform license expires, the installed sub license and function license can still be effective, but the OS version cannot be upgraded.

Sub Licenses

Sub licenses control whether corresponding functions are enabled or not and the time limit as well.

- **CPU Sub License**

  CPU Sub License authorizes the maximum number of vCPUs available to the vADC. The CPU license has both base and trial types, and the base CPU license does not expire. After the trial license expires, system will restart and the number of available vCPUs will revert to 2vCPU, which is the configuration of the minimum model SG-6000-AX02.

- **iQoS Sub License**

  iQoS sub license enables iQoS function. When the iQoS sub license expires, all the configurations of iQoS will not be lost until the device is restarted.

Function Licenses

Some functions can be enabled and signature databases can be upgraded only after corresponding licenses are installed.

- **Feature Trial License**

  Feature Trial License provides the trial of LLB, GSLB, QoS and other functions. Its validity is permanent.

- **APP Signature License**

  APP signature License allows the APP signature database to be upgraded. APP signature license is issued with platform

license, you do not need to apply for it. Its validity is the same as that of the platform license. When the license expires, the APP signature database cannot be upgraded.

- VSYS License

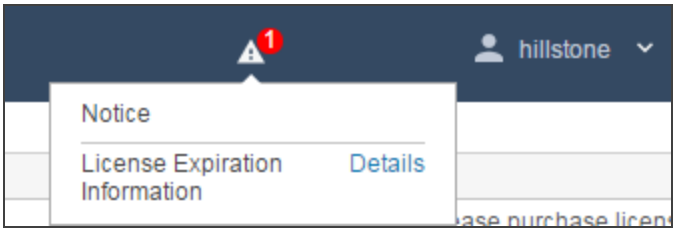
  Authorizing the available number of VSYS. Its validity is permanent.

Viewing License List

Select **System** > **License** to enter the License List page. All licenses the system supports will be displayed in this page, including the authorized licenses and unauthorized licenses.

If there is license that is about to expire (the remaining valid period is within 30 days) or has expired:

- When you log into the device, the License Expiration Information dialog box will pop up, which prompts for licenses that are about to expire or have expired. Check the **Don't remind me again** check box so that the dialog box will never prompt again when you login. Click **Update Now** to jump to the License List page.
- The notification icon with the number of notifications is displayed in the upper-right corner. Hover your mouse over the icon, and click **Details** behind the License Expiration Information, the License Expiration Information dialog box will pop up.



Applying for a License

Before applying for a license, you have to generate a license request first. Take the following steps:

1. Select **System** > **License** > **License**.

2. Under License Request, input user information. All fields are required.

3. Click **Generate**, and then appears a bunch of code.

4. Send the code to your sales contact. The sales person will issue the license and send the code back to you.

Installing a License

After obtaining the license, you should install it to the device to make it take effect. To install a license, take the following steps:

1. Select **System** > **License** > **License**.

2. Under License Request, select the method you desire:

   - Upload License File: Select **Upload License File**. Click **Browse** to select the license file, using the TXT format, and then click **OK** to upload it.

   - Manual Input: Select **Manual Input**. Type the license string into the box.

3. Click **OK**.

4. Select **System** > **Device Management** > **Option**.

5. Click **Reboot**, and select **Yes** in the prompt.

6. System will reboot. When it starts again, installed license(s) will take effect.

Verifying License

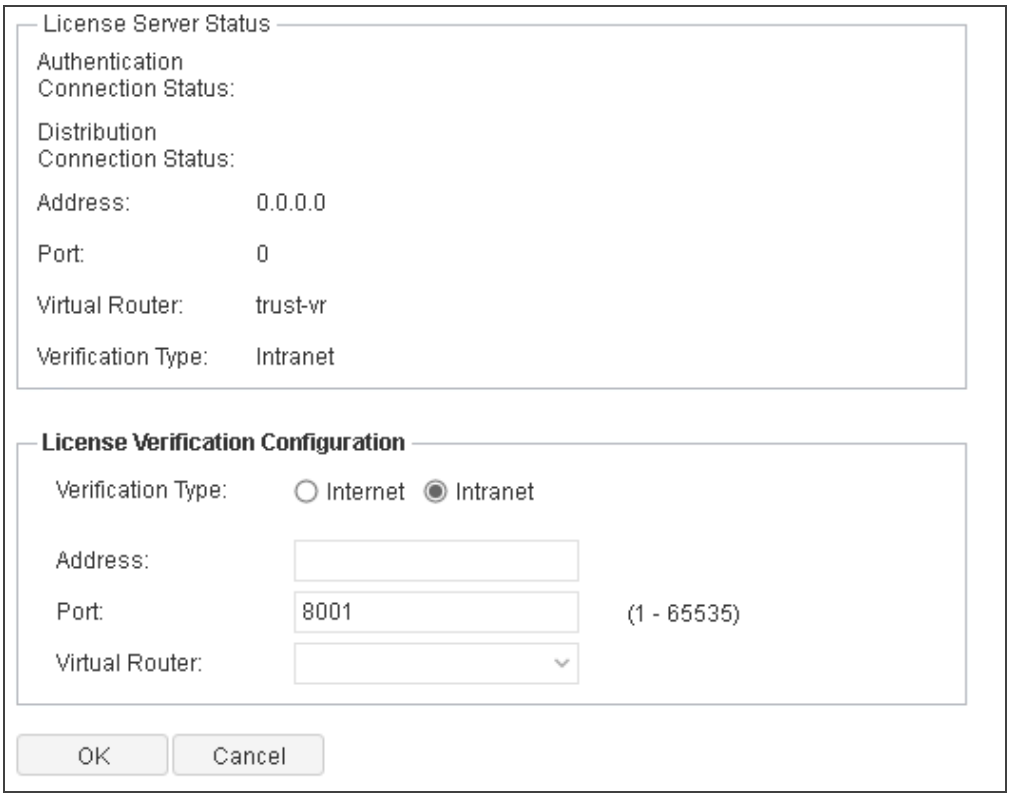
For vADC, after the installation of the new platform license, the SN number of the device will be changed to a virtual SN (vSN for short). If you want to continue to obtain function or sub licenses, they can be applied through the vSN number. For the new license does not depend on the SN number of the original system after the re-installation of system, the new license that was originally applied for can still be effective. At the same time, Hillstone provides the public network license server and the internal network LMS (License Management System) to verify and manage licenses, which can ensure the security of licenses. You need to connect vADC to the license server to verify the validity of a license to prevent the license from being cloned.

System supports two verfication ways, one is connecting vADC to the public network license server via Internet, and the other is connecting vADC to the internal network LMS via LAN. You can choose one of them as needed.

- The way to verify validity through the public network license server is suitable for some small-scale private or public cloud scenarios. After the vADC connects to the public network server, the server will verify validity of the license (currently the public network server does not support the distribution and management of licenses). If the cloned license is found or the vADC is not checked by the server, the vADC will be restarted in 30 days.
- The way to verify validity through LAN LMS is suitable for large-scale private or industry cloud scenarios. After the vADC connects to the LMS, the LMS not only verifies validity of the license, but also supports automatic distribution and management licenses. If the cloned license is found, the server will recover all licenses of either the cloning or cloned vADC, and restart the vADC; if the vADC does not connect to the server to verify the license, the vADC will be restarted in 30 days.

To verify licenses, take the following steps:

1. Select **System** > **License** > **License Verification**.



2. In the **License Server Status** section, the server's authentication and distribution connection status, IP address, port, virtual router and verification type will be displayed.

   In the License Verification Configuration section, you can choose one of the following two ways as needed:

   - **Internet**: Select **Internet** and specify a virtual router, and then click **OK**. The vADC will verify the license through the public server.
   - **Intranet**: Select **Intranet**, and specify the server's address, port and virtual router, and click **OK**. The vADC's license will be verified, distributed and managed through the LMS.

3. Select **System** > **Device Management** > **Option**.

4. Click **Reboot**, and select **Yes** in the prompt.

5. System will reboot. When it starts again, installed license(s) will take effect.

Note: When you verify your license through a public network server, make sure that the VRouter used to connect to the server is bound to a zone, and the interface bound to the zone can access Internet. For more information about LMS, refer to LMS User Guide.

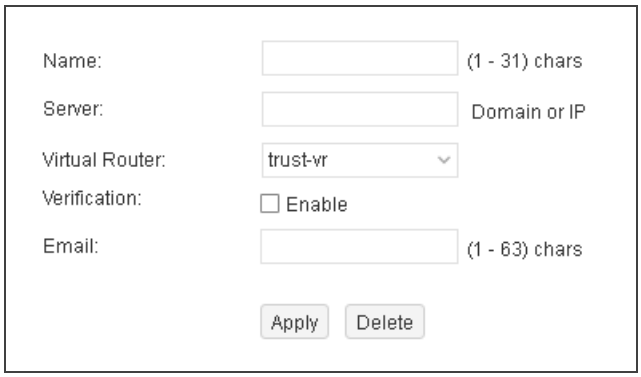
Mail Server

By configuring the SMTP server in the Mail Server page, system can send the log messages to the specified email address.

Creating a Mail Server

To create a mail server, take the following steps:

1. Select System > Mail Server. In the Mail Server Configuration page, configure these values.



Option	Description
Name	Type a name for the SMTP server into the box.
Server	Type a domain name or an IP address for the SMTP server into the box.
VR	From the **Virtual Router** drop-down list, select a virtual router for the SMTP server.
Verification	Select the **Enable** check box for SMTP verification to enable it if needed. Type the username and its password into the corresponding boxes.
Email	Type the email address that sends log messages.

2. Click **Apply**.

Connecting to Hillstone CloudView

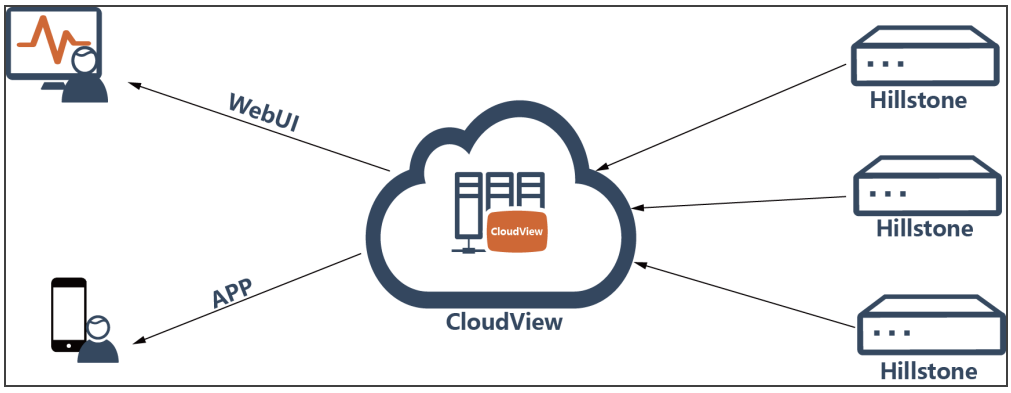
CloudView is a SaaS products of security area and a cloud security services platform in the mobile Internet era. CloudView is deployed in the public cloud to provide users with online on-demand services. You can get convenient, high quality and low cost value-added security services through the Internet and APP, and get a better security experience.

After the Hillstone device is properly configured to connect the CloudView, you can register the Hillstone device to the public cloud and connect the device with the CloudView, thereby remotely monitoring the device through CloudView.

CloudView Deployment Scenarios

The main deployment scenarios of CloudView are described as follows:

When Hillstone devices register to the public cloud, the threat event, system logs, etc., are uploaded to the cloud, which provides a visual display. You can monitor the device status information, reports, threat analysis, etc., through the Web or mobile phone APP.

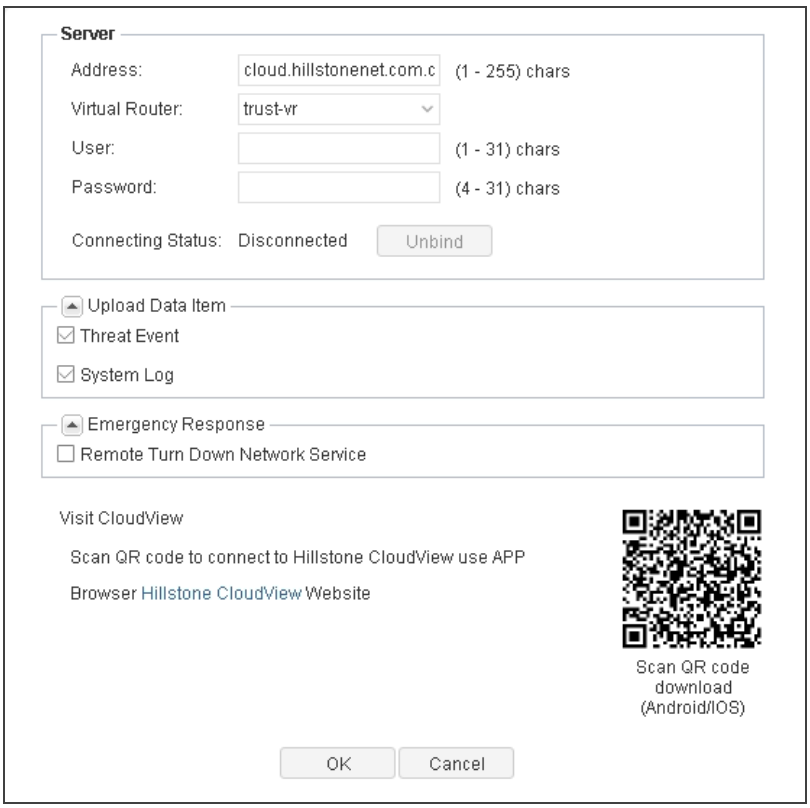


Note: For more information about CloudView, see CloudView FAQ and CloudView Getting Started Guide.

Connecting to Hillstone CloudView

To connect the device to the CloudView server, take the following steps:

1. Select **System** > **Hillstone Cloud**.



2. Type the URL of the CloudView server into the **Address** text box. The default configuration is cloud.hillstonenet.com.cn.

3. Select a virtual router from the **Virtual Router** drop-down list. The default option is trust-vr.

4. Type the registered username into the **User** text box, and register the device under this username. For example: Typing the username: abc@example.com means that the AX device will be registered under "abc@example.com".

5. Type the password of the user into the **Password** text box.

6. **Server Status** displays the CloudView status.

7. Select **Threat Event** to upload the threat events detected by the device to CloudView.

8. Select **System Log** to upload the event logs to CloudView.

9. Click **OK**. Log in to CloudView with your username and password to view the information of the AX device.

One-click Disconnection

When users' websites or businesses are under attack, they can disconnect their businesses from the Internet temporarily with this function in the CloudView APP to minimize the losses.

After registered to the CloudView, the AX device will periodically report the virtual server information to the cloud, and display some of configurations (such as protocol type, IP port and number of connections), running status, statistics, etc., of virtual servers in the APP.

To configure one-click disconnection, take the following the steps:

1. Select **System** > **Hillstone Cloud**.
2. Select the **One-click Disconnection** check box, and click **OK**.
3. Open **CloudView** on your mobile phone. You can scan the QR code on the page to download the CloudView APP.
4. Enter the username (for example: abc@example.com) and password of your CloudView account.
5. Click the **Monitor** module, and the registered AX device will be displayed on the Monitor page.
6. Click the device, and select the **One-click Disconnection** tab to display all virtual servers under the device and their status.
7. Click **Enable** to disconnect the selected virtual server with one click, or disconnect virtual servers in batch.
8. If necessary, click **Disable** to resume traffic forwarding for the down virtual server.

Connecting to HSM

Hillstone Security Management (HSM) is a centralized management platform to manage and control multiple Hillstone devices. Using WEB2.0 and RIA (Rich Internet Application) technology, HSM supports a visualized interface to centrally manage policies, monitor devices, upgrade system online, display reports, as well as import and export configuration files.

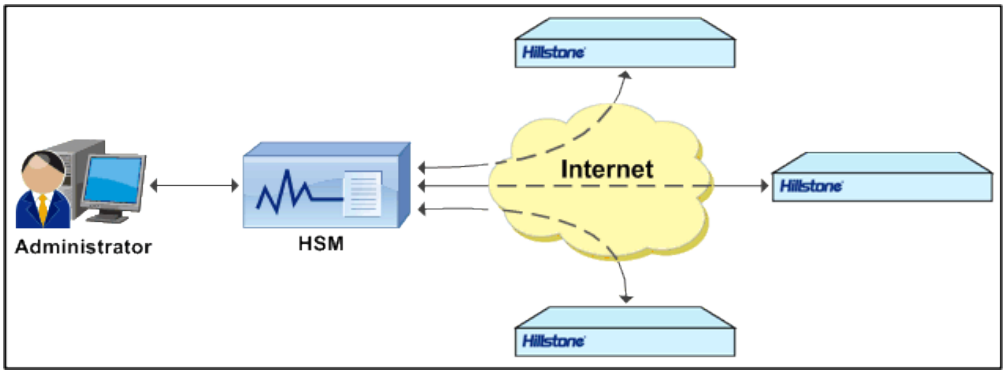
Each ADC system has an HSM module inside it. When the ADC is configured with HSM parameters, it can connect to HSM and be managed by HSM.

Note: For more information about HSM, refer to HSM User Guide. You can visit https://-docs.hillstonenet.com to download guides.

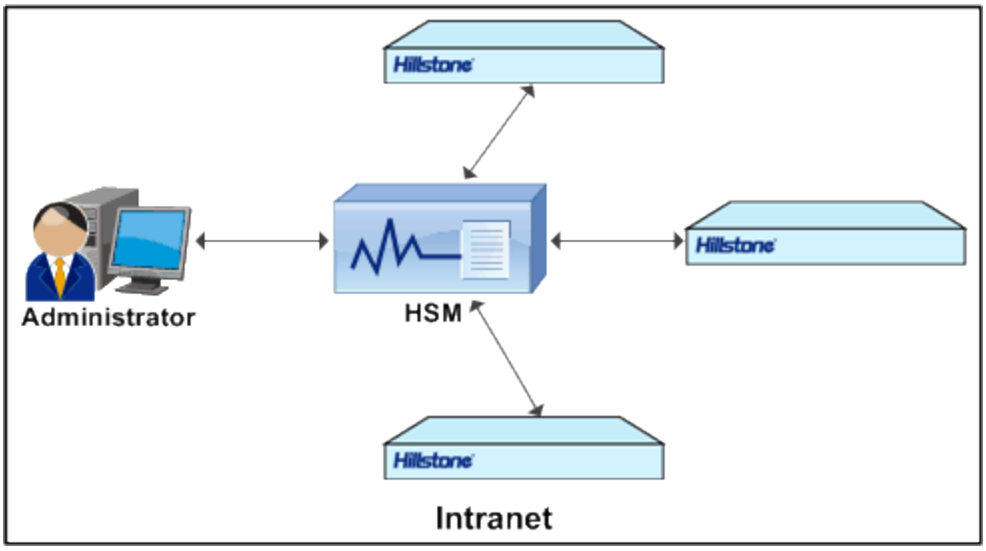
HSM Deployment Scenarios

HSM normally is deployed in one of the two scenarios: installed in public network or in private network:

- Installed in public network: HSM is remotely deployed and connected to managed devices via Internet. When the HSM and managed devices have an accessible route, the HSM can control the devices.



- Installed in private network: In this scenario, HSM and the managed devices are in the same subnet. HSM can manage devices in the private network.

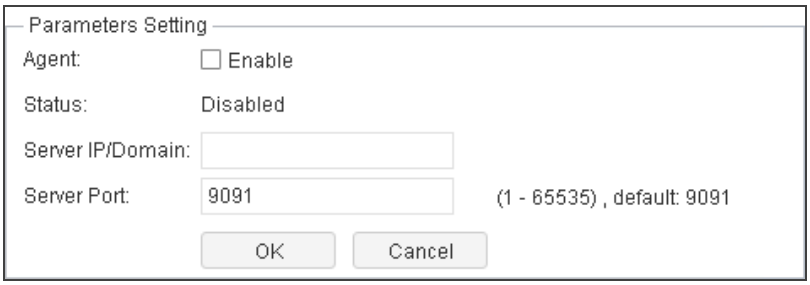


Connecting to HSM

To configure HSM parameters for the ADC, take the following steps:

1. Select **System** > **HSM Agent**.

2. Select **Enable** of HSM Agent field to enable this function.



3. Type the HSM server's IP address into the Sever IP/Domain text box. The address cannot be 0.0.0.0 or 255.255.255.255, or a mutlicast address.

4. Type the port number of the HSM server into the Server Port text box.

5. Click **OK**.

Note: The Syslog Server part shows the HSM server's syslog server and its port.

PKI

PKI (Public Key Infrastructure) is a system that provides public key encryption and digital signature service. PKI is designed to automate secret key and certificate management, and assure the confidentiality, integrity and non-repudiation of data transmitted over the Internet. The certificate of PKI is managed by a public key by binding the public key with a respective user identity by a trusted third-party, thus authenticating the user over the Internet. A PKI system consists of Public Key Cryptography, CA (Certificate Authority), RA (Certificate Authority), Digital Certificate and related PKI storage library.

PKI terminology:

- Public Key Cryptography: A technology used to generate a key pair that consists of a public key and a private key. The public key is widely distributed, while the private key is only known to the recipient. The two keys in the key pair complement each other, and the data encrypted by one key can only be decrypted by the other key of the key pair.
- CA: A trusted entity that issues digital certificates to individuals, computers or any other entities. CA accepts requests for certificates and verifies the information provided by the applicants based on certificate management policy. If the information is legal, CA will sign the certificates with its private key and issue them to the applicants.

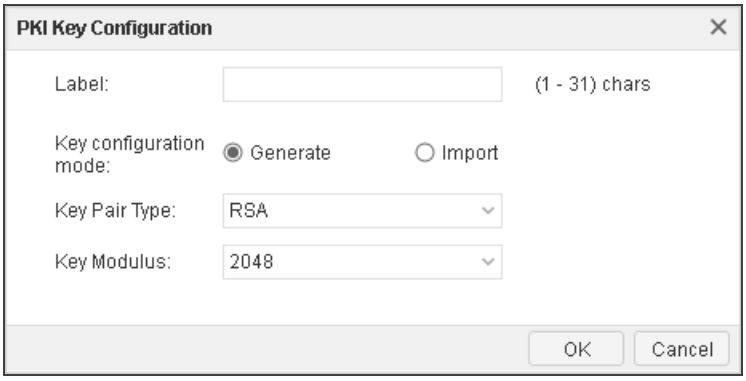
- RA: The extension to CA. RA forwards requests for a certificate to CA, and also forwards the digital certificate and CRL issued by CA to directory servers in order to provide directory browsing and query services.
- CRL: Each certificate is designed with expiration. However, CA might revoke a certificate before the date of expiration due to key leakage, business termination or other reasons. Once a certificate is revoked, CA will issue a CRL to announce the certificate is invalid, and list the series number of the invalid certificate.

PKI is used in the following two situations:

- HTTPS/SSH: PKI applies to the situation where a user accesses a Hillstone device over HTTPS or SSH.

Creating a PKI Key

1. Select **System** > **PKI** > **Key**.
2. Click **New**.



In the PKI Key Configuration dialog box, configure the following options.

Option	Description
Label	Specify the name of the PKI key. The name must be unique.
Key configuration mode	Specify the generation mode of keys, which includes Generate and Import.
Key Pair Type	Specify the type of key pair, either RSA, or DSA or SM2.
pki_key_win_config	If you select ECC, you need to select an elliptic curve group from the drop-down list, including P-256, P-384 and P-521.
Type	Specify the type of key, including Encryption Key and Key Pair. This option takes effect only after the GM IPSec VPN license is installed.

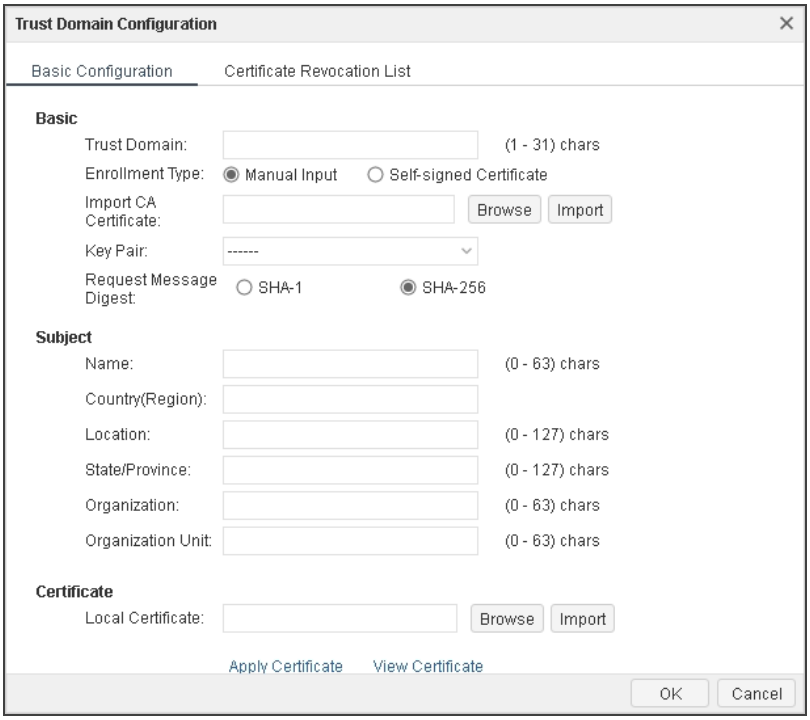
Option	Description
Key Modulus	Specify the modulus of the key pair. You can select 1024 (the default value), 2048, 512 or 768 bits.
Import Key	If you select the **Import** as the key configuration mode, click **Browse** to select a key file in your local file system and import it.

3. Click **OK**.

Creating a Trust Domain

1. Select **System** > **PKI** > **Trust Domain**.

2. Click **New**, and the Trust Domain Configuration dialog box will appear.



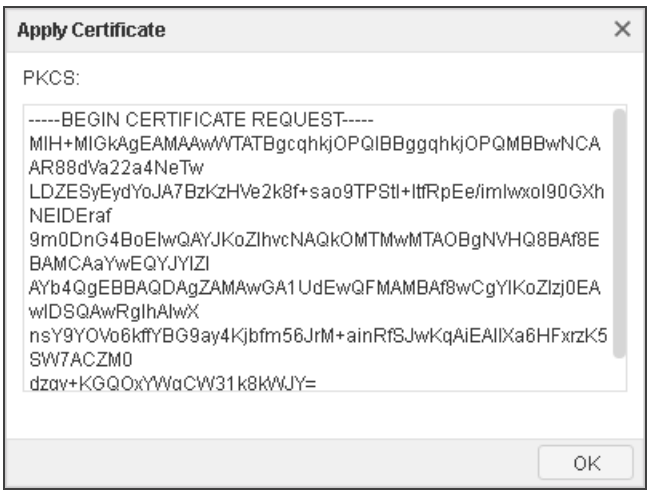
In the Basic Configuration tab, configure values for basic properties.

Basic Configuration	
Trust Domain	Enter the name of the new trust domain.
Enrollment Type	Select one of the two following methods depending on different CAs:

Basic Configuration	
	• For external CAs, select **Manual Input**. Click **Browse** behind Import CA Certificate to find the certificate, and click **Import** to import it into system. • Select **Self-signed Certificate**, and the certificate will be generated by the device itself.
Key Pair	Select a key pair.
Request Message Digest	Specify the message digest algorithm for certificate requests, including SHA-1 and SHA-256. The default option is SHA-256.
Subject	
Name	Optional. Enter a name of the subject.
Country (Region)	Optional. Enter the name of applicant's country or region. Only an abbreviation of two letters are allowed, like CN.
Location	Optional. The location of the applicant.
State/Province	Optional. State or province name.
Organization	Optional. Organization name.
Organization Unit	Optional. Department name within applicant's organization.

3. Click **Apply Certificate**, and a string of code will appear.

4. Copy this code and send it to CA via email.



5. When you receive the certificate sent from CA. Click **Browse** behind Local Certificate to find the certificate, and click **Import** to import it into system.

6. (Optional) In the Certificate Revocation List tab, configure the following options.

Certification Revocation List	
Check	• No Check - System does not check CRL. This is the default option. • Optional - System accepts certificating from peer, no matter if CRL is available or not. • Force - System only accepts certificating from peer when CRL is available.
URL 1 URL 2 URL 3	Specify the URL address for receiving CRL. At most 3 URLs are allowed, and their priority is from 1 to 3. • Select http:// if you want to get CRL via HTTP. • Select ldap:// if you want to get CRL via LDAP. If you use LDAP to receive CRL, you need to enter the login-DN

Certification Revocation List	
	(usually a user account with query permission preset for the LDAP server) of the LDAP server and password. If no login-DN or password is added, the transmission will be anonymous.
Auto Update	Specify the update frequency for the CRL list.
Manually Update	Get the CRL immediately by clicking **Obtain CRL**.

7. Click **OK**.

Importing/Exporting Trust Domain

To simplify configurations, you can export certificates (CA or local) and private key (in the format of PKSC12) to a computer and import them to another device.

To export a PKI trust domain, take the following steps:

1. Select **System** > **PKI** > **Trust Domain Certificate**.
2. Select a domain from the **Trust Domain** drop-down list.
3. Select the radio button of the item you want to export, and click **Export**.

If you choose PKCS, you need to set up a password.

4. Click **OK**, and select a storage path to save the item.

To import the saved trust domain to another device, take the following steps:

1. Select **System** > **PKI** > **Trust Domain Certificate**
2. Select a domain from the **Trust Domain** drop-down list.

3. Select the radio button of the item you want to import, and click **Import**.

If you choose PKCS, you need to enter the password when it was exported.

4. Click **Browse** and find the file you want to import.

5. Click **OK**. The domain file is imported.

Certificate Chain

For PKCS # 7 or PKCS # 12 files containing multi-level certificates, you can import them into system, and then use them together with key pair files to create a certificate chain. The created certificate chain can be directly referenced by other functions, such as SSL profiles. You can also export the certificate chain in PKCS#7 or PKCS#12 format, which can be imported into and used by another device.

Creating a Certificate Chain

To create a certificate chain, take the following steps:

1. Select **System** > **PKI** > **Cert-chain**.

2. Click **New**.

In the Cert-chain Configuration dialog box, configure the following options.

Option	Description
Name	Specify the name of the certificate chain.

Option	Description
Import Certificate Type	Specify the type of the certificate. You can select PKCS#7 or PKCS#12 according to the format of the certificate file you want to import.
Certificate	Click **Browse** and find the certificate you want to import.
Key Pair	If you choose PKCS#7, you need to import the key pair file of the terminal entity. Click **Browse** and find the key pair you want to import.
Password	If you choose PKCS#12, you need to enter the password of the PKCS#12 file.

Exporting a Certificate Chain

To exporting a certificate chain, take the following steps:

1. Select **System** > **PKI** > **Cert-chain**.
2. Select a certificate chain from the list.
3. Click **Export Cert-chain**, and select **Export PKCS#7** to export the certificate file in PKCS#7 format; enter the password, and click **Export PKCS#12** to export the certificate file in PKCS#12 format.

VSYS (Virtual System)

VSYS (Virtual System) logically divides the physical firewall into several virtual firewalls. Each virtual firewall can work independently as a physical device with its own system resources, and it provides most firewall features. A VSYS is separated from other VSYS, and by default, they cannot directly communicate with each other.

VSYS has the following characteristics:

- Each VSYS has its own administrator;
- Each VSYS has an its own virtual router, zone, address book and service book;
- Each VSYS can have its own physical or logical interfaces;
- Each VSYS has its own security policies.

Note: The maximum VSYS number is determined by the platform capacity and license. You can expand VSYS maximum number by purchasing additional licenses.

VSYS Objects

This section describes VSYS objects, including root VSYS, non-root VSYS, administrator, VRouter, VSwitch, zone, and interface.

Root VSYS and Non-root VSYS

System contains only one root VSYS which cannot be deleted. You can create or delete non-root VSYSs after installing a VSYS license and rebooting the device.

When creating or deleting non-root VSYSs, you should follow the rules listed below:

- When creating or deleting non-root VSYSs through CLI, you should be under the root VSYS configuration mode.
- Only the root VSYS administrators and root VSYS operators can create or delete non-root VSYS. For more information about administrator permissions, see "Device Management" on Page 498.

- When creating a non-root VSYS, the following corresponding objects will be created simultaneously:
  - A non-root VSYS administrator named admin. The password is vsys_name-admin.
  - A VRouter named vsys_name-vr.
  - A L3 zone named vsys_name-trust.

  For example, when creating the non-root VSYS named vsys1, the following objects will be created: A non-root VSYS administrator named admin with the password vsys1-admin; a default VRouter named vsys1-vr; and a L3 zone named vsys1-trust, which will be bound to vsys1-vr automatically.
- When deleting a non-root VSYS, all the objects and logs in the VSYS will be deleted simultaneously.
- The root VSYS contains a default VSwitch named VSwitch1, but there is no default VSwitch in a newly created non-root VSYS. Therefore, before creating L2 zones in a non-root VSYS, a VSwitch must be created. The first VSwitch created in a non-root VSYS will be considered as the default VSwitch, and the L2 zone created in the non-root VSYS will be bound to the default VSwitch automatically.

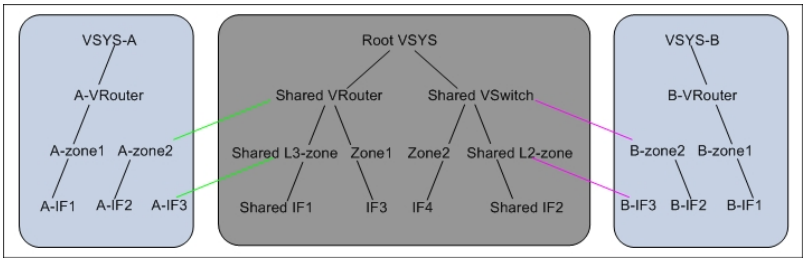
VRouter, VSwitch, Zone and Interface

VRouter, VSwitch, zone, and interface in VSYS have two properties which are shared and dedicated. Objects with dedicated property are dedicated objects, while doing specific operations to the object with the shared property will make it a shared object.

The dedicated object and shared object have the following characters:

- Dedicated object: A dedicated object belongs to a certain VSYS, and cannot be referenced by other VSYSs. Both root VSYS and non-root VSYS can contain dedicated objects.
- Shared object: A shared object can be shared by multiple VSYSs, but only belongs to and can only be configured in the root VSYS. A non-root VSYS can reference a shared object, but cannot configure it. The name of the shared object must be unique in the whole system.

The figure below shows the reference relationship among dedicated and shared VRouter, VSwitch, zone, and interface.



As shown in the figure above, there are three VSYSs in ADC: Root VSYS, VSYS-A, and VSYS-B. Root VSYS contains shared objects (including Shared VRouter, Shared VSwitch, Shared L3-zone, Shared L2-zone, Shared IF1, and Shared IF2) and dedicated objects.

VSYS-A and VSYS-B only contain dedicated objects, which can reference the shared objects in Root VSYS. For example, A-zone2 in VSYS-A is bound to the shared object Shared VRouter in Root VSYS, and B-IF3 in VSYS-B is bound to the shared object Shared L2-zone in Root VSYS.

- **Shared VRouter**: A shared VRouter contains the shared and dedicated L3 zones of the root VSYS. After binding a L3 zone with the shared property to a shared VRouter, this zone becomes a shared zone.
- **Shared VSwitch**: A shared VSwitch contains the shared and dedicated L2 zones of the root VSYS. After binding a L2 zone with the shared property to a shared VSwitch, this zone becomes a shared zone.
- **Shared Zone**: The shared zones consist of L2 shared zones and L3 shared zones. After binding a L2 zone with the shared property to a shared VSwitch, this zone becomes a shared L2 zone; after binding the L3 zone with shared property to a shared VRouter, this zone becomes a shared L3 zone. A shared zone can contain interfaces in both root VSYS and non-root VSYS. All functional zones (such as HA functional zone) cannot be shared.
- **Shared Interface**: After binding an interface in the root VSYS to a shared zone, the interface becomes a shared interface automatically.

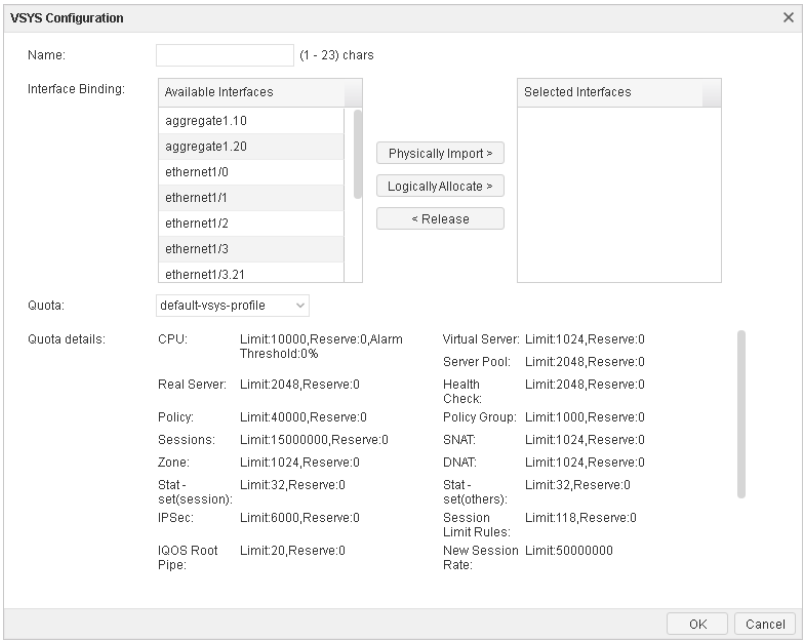
Note: Only the administrator or operator has the authority to delete or create interfaces. If you want to create or delete an interface and its sub-interfaces, you have to do it under the same VSYS.

Creating Non-root VSYS

To create a new non-root VSYS, take the following steps:

1. Select **System** > **VSYS** > **VSYS**.

2. Click New. In the VSYS Configuration dialog box, configure these values.



Option	Description
Name	Enter a name for the non-root VSYS.
Description	Enter the description information for the non-root VSYS.
Interface Binding	Select a physical or a logical interface. In VSYS, a physical interface can have its sub-interfaces, but logical interfaces cannot. • Physically Import: Select the interface you want from the **Available Interfaces** list, and click **Physically Import** to add it to the **Selected Interfaces** list. • Logically Allocate: Select the interface you want from the **Available Interfaces** list, and click **Logically Allocate** to add it to the **Selected Interfaces** list. • Release: Select the added interface(s) from the **Selected Interfaces** list, and click **Release** to delete it.

Option	Description
Quota	Select an existing quota from the drop-down list.
Quota Details	Displays the detailed information of the quota.。

3. Click **OK**. The new VSYS will be displayed in the VSYS list.

Entering/Exiting from the Non-root VSYS

To enter a non-root VSYS, you can use the management IP of the non-root VSYS directly or enter from the root VSYS (only root VSYS admin has the privilege).

After typing the management IP of the non-root VSYS in a browser, you should type the username and password in the login page. For example, type the management IP (10.90.89.1) of the root VSYS, and type the username (hillstone) and password (hillstone), then you can enter the root VSYS. After creating the non-root VSYS (vsys1), you should type the management IP 10.90.89.1, and type the non-root administrator username (vsys1\admin) and password (vsys1-admin) in the login page, then you can enter the non-root VSYS directly. For the detailed information of administrator configuration, see "Device Management" on Page 498.

Note: If using the above method to enter the non-root VSYS, you cannot return to the root VSYS. You need exit from the non-root VSYS, and then type the management IP in the browser for the root VSYS.

The root VSYS administrator can enter the non-root VSYS from the root VSYS. After entering, the administrator in the root VSYS can configure the functions of the non-root VSYS. To enter or exit from a non-root VSYS, take the following steps:

1. Select **System** > **VSYS** > **VSYS** to enter the VSYS page.
2. In the VSYS list, click the name of a non-root VSYS, and enter the non-root VSYS.
3. To return to the root VSYS, click at the top-right corner of the page, and click **Return root Vsys** in the pop-up dialog box.

Configuring Dedicated and Shared Objects for Non-root VSYS

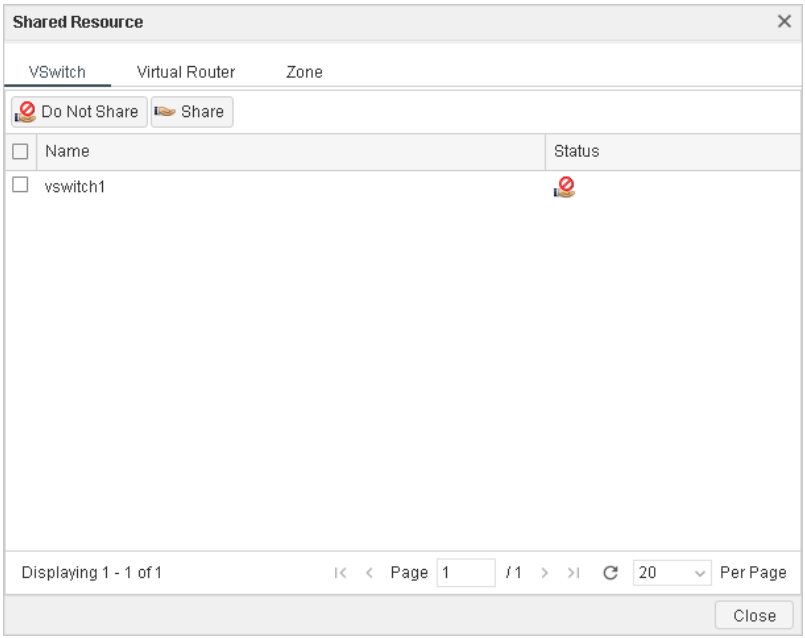
VRouter, VSwitch, zone, and interface in VSYS have two properties which are shared and dedicated. Objects with dedicated property are dedicated objects, while doing specific operations to the object with the shared property will make it a shared

object. The dedicated object and shared object have the following characters:

- **Dedicated object**: A dedicated object belongs to a certain VSYS, and cannot be referenced by other VSYSs. Both root VSYS and non-root VSYS can contain dedicated objects.
- **Shared object**: A shared object can be shared by multiple VSYSs, but only belongs to and can only be configured in the root VSYS. A non-root VSYS can reference a shared object, but cannot configure it. The name of the shared object must be unique in the whole system.

To configure VSYS shared object, take the following steps:

1. Select **System** > **VSYS** > **VSYS**
2. Click **Shared Resource**. In the Shared Resource dialog box, configure values for VSwitch, VRouter and Zone.



Option	Description
VSwitch	In the VSwtich tab, select a VSwitch and click **Share** to set it as a shared object; to make a VSwitch as a dedicated object, click **Do Not Share**.
Virtual Router	In the Virtual Router tab, select a VSwitch and click **Share** to set it as a shared object; to make a Virtual Router as a dedicated object, click **Do Not Share**.

Option	Description
	Note: proxy-vr is a shared object by default and cannot be modified.
Zone	In the Zone tab, select a Zone and click **Share** to set it as a shared object; to make a Zone as a dedicated object, click **Do Not Share**.

3. Click **Close** to exit.

Configuring VSYS Quota

VSYSs work independently in functions but share system resources including the virtual server number, server pool number, health check number, real server number, session number, zone number, policy rule number, SNAT rule number, DNAT rule number, etc. The root RXW administrator can specify the reserved quota and maximum quota for each type of system resource in a VSYS by creating a VSYS profile. Reserved quota refers to the resource number reserved for the VSYS; while maximum quota refers to the maximum resource number available to the VSYS. The total for each resource of all VSYSs cannot exceed the system capacity.

To define a quota for VSYS, take the following steps:

1. Select **System** > **VSYS** > **Quota**.

2. Click **New**. In the Quota Configuration dialog box, configure these values.

Option	Description
Basic Configuration	
Name	Enter a name for the new quota.
CPU	Specify quotas for CPU in the VSYS. • Limit: Type the maximum CPU quota into the text box. The value range is 1 to 10000 in the unit of 1/10000, and 10000 means 100%. • Reserve: Type the reserved CPU quota into the text box. The value range is 0 to 20000. • Alarm Threshold: Type a percentage value for alarms into the text box. When the CPU usage reaches this value, system will generate alarm logs. The value range is 50 to 99.

Option	Description
Basic Configuration	
	For example, if the maximum CPU quota is specified as 5000 (i.e., 50%) and the alarm threshold as 70 (i.e., 70%), then when the CPU usage exceeds (5000/10000)*70%, system will generate alarm logs for CPU.
System Resources	
System Resources	Specify the maximum quota and reserved quota of system resources. • Virtual Servers: Specify the maximum and reserved quota for virtual servers in the VSYS. • Server Pools: Specify the maximum and reserved quota for server pools in the VSYS. • Real Servers: Specify the maximum and reserved quota for real servers in the VSYS. • Health Check: Specify the maximum and reserved quota for health check in the VSYS. • Sessions: Specify the maximum and reserved quota for sessions in the VSYS. • Zone: Specify the maximum and reserved quota for zones in the VSYS. • Policy rules: Specify the maximum and reserved quota for policy rules in the VSYS. • Policy Groups: Specify the maximum and reserved quota for policy groups in the VSYS. • SNAT rules: Specify the maximum and reserved quota for SNAT rules in the VSYS. • DNAT rules: Specify the maximum and reserved quota for SNAT

Option	Description
Basic Configuration	
	rules in the VSYS. • Stat-set (session): Specify the maximum and reserved quota for sessions of a statistic set in the VSYS. • Stat-set (others): Specify the maximum and reserved quota for other items than sessions of a statistic set in the VSYS. • IPsec: Specify the maximum and reserved quota for IPSec tunnels in the VSYS. • Session Limit Rules: Specify the maximum and reserved quota for session limit rules in the VSYS. • IQoS: Select the **Enable** check box to enable the QoS function and specify the maximum and reserved quota for root-pipe in the VSYS.
Log Configuration	
Log Configuration	Specify the maximum quota and reserved quota of memory buffer for each type of log in a VSYS. The reserved quota should not exceed the maximum quota. If the logs' capacity in a VSYS exceeds its maximum quota, the new logs will override the earliest logs in the buffer.

3. Click **OK**. The new VSYS quota will be displayed in the VSYS quota list.

Note:

- Up to 128 VSYS quotas are supported.
- The default VSYS profile of the root VSYS named root-vsys-profile and the default VSYS profile of the non-root VSYS named default-vsys-profile cannot be edited or deleted.
- Before deleting a VSYS profile, you should delete all the VSYSs referencing the VSYS profile.
- The reserved quota should not exceed the maximum quota.

Chapter 15 Diagnostic Tool

This feature may not be available on all platforms. If there is a conflict between this guide and the actual page, the latter shall prevail.

System supports the following diagnostic methods:

- Test Tools: DNS Query, Ping, Traceroute and Curl can be used when troubleshooting the network.

Test Tools

DNS Query, Ping, Traceroute and Curl can be used when troubleshooting the network.

DNS Query

To check the DNS working status of the device, take the following steps:

1. Select **System** > **Diagnostic Tool** > **Test Tools**.
2. Type a domain name into the **DNS Query** box.
3. Click **Test**, and the testing result will be displayed in the list below.

Ping

To check the network connecting status by using Ping, take the following steps:

1. Select **System** > **Diagnostic Tool** > **Test Tools**.
2. Type an IP address into the **Ping** box.
3. Click **Test**, and the testing result will be displayed in the list below.
4. The testing result contains two parts:
    - The Ping packet response. If there is no response from the target after timeout, it will print Destination Host Not Response, etc. Otherwise, the sequence number, TTL and response time of the received response will be displayed.

- Overall statistics, including the number of sent packets, the number of received packets, the percentage of no response, and the minimum, average and maximum response time.

Traceroute

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

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

1. Select **System** > **Diagnostic Tool** > **Test Tools**.
2. Type an IP address into the **Traceroute** box.
3. Click **Test**, and the testing result will be displayed in the list below.

Curl

To test the HTTP/HTTPS service of the server by using Curl, take the following steps:

1. Select **System** > **Diagnostic Tool** > **Test Tools**.
2. Type an IP address or a domain name of the HTTP/HTTPS service to be queried into the **Traceroute** box.
3. Click **Test**, and the testing result will be displayed in the list below.

Diagnostic Files

This page displays the diagnostic files stored in system, which are generated after a diagnostic tool with the storage function is used.

- View the diagnostic file: In the list of diagnostic files, you can view the name, size and creation time of a diagnostic file.
- Delete the diagnostic file: To delete a diagnostic file, select the file you want to delete, and click **Delete**.

Chapter 16 High Availability

High Availability (HA) provides a fail-over solution for communications lines or device failure to ensure the smooth communication and effectively improve the reliability of the network. To implement the HA function, you need to configure two AX devices as HA clusters, using the identical hardware platform and firmware version, . When one device is not available 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.

System supports the 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 takes over its work to forward packets. This A/P mode is highly redundant, and features a simple network structure for you to maintain and manage.

Basic Concepts

HA Cluster

An HA cluster combines devices to realize the HA function. For the external network devices, the 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 devices with the same HA group ID in an HA cluster according to the HCMP protocol and the HA configuration. The master device is in the 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.

Virtual Forward Interface and MAC

In the HA environment, each HA group has an interface to forward traffic, which is known as the Virtual Forward Interface. The master device of each HA group manages a virtual MAC (VMAC) address which is corresponding with its inter-

face, 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 to the backup device. There are three types of information that can be synchronized: configuration information, files and RDO (Runtime Dynamic Object). The specific content of RDO includes:

- Health status
- Session information
- Session persistence table (IPv6 is supported)
- DNS cache mappings
- ARP table
- PKI information
- DHCP information
- MAC table

System 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.

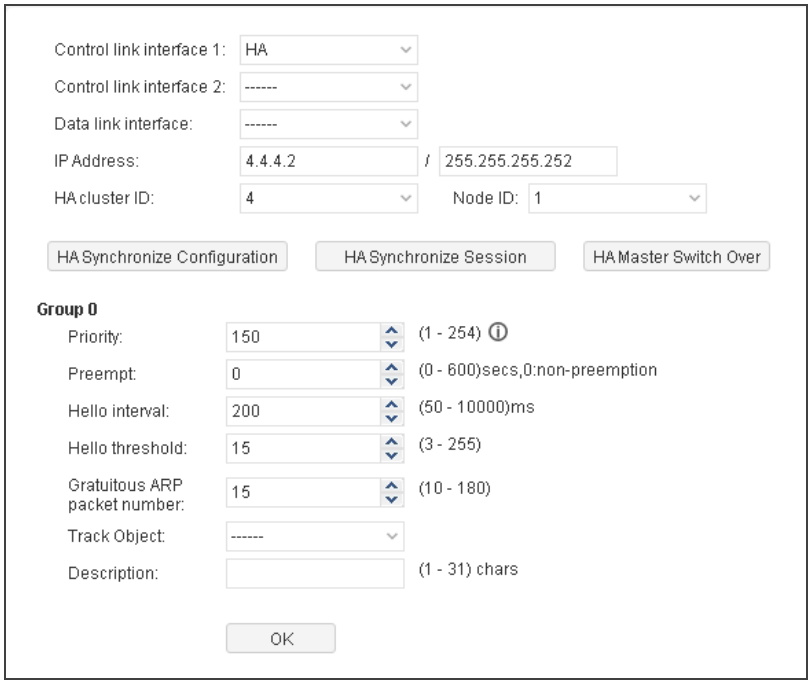
Configuring HA

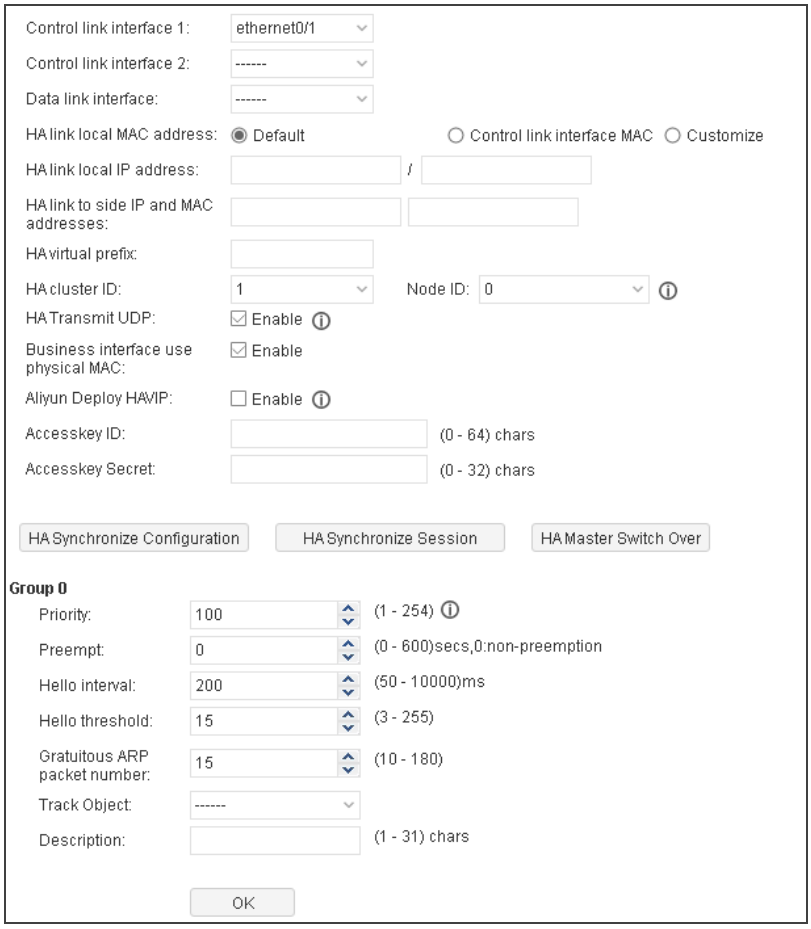
To configure the HA function, take the following steps:

1. Configure an HA Virtual Forward Interface.
2. Configure an HA link interface and its IP, which will be used for the device synchronization and HA packets transmission.
3. Configure an HA cluster. Specify the HA cluster ID and enable the HA function.
4. Configure an HA group. Specify the priority for devices (for selection) and HA messages parameters.

To configure HA, take the following steps:

1. Go to **System** > **HA**.





Configure the HA as follows.

Option	Description
Control link interface 1	Specify the name of the HA control link interface. The control link interface is used to synchronize all data between two devices.
Control link interface 2	Specify the name of the HA control link interface (Backup device).
Data link interface	Specify the name of the HA data link interface. The data link interface is only used to synchronize the data packet information. 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.

Option	Description
IP Address	Specify the IP address and netmask of the HA link interface.
HA link local MAC address	This function is only supported by vADC. Specify the local MAC address of the HA link. The MAC address refers to the source MAC address used by the HA device for sending heartbeats (Hello packets) to other devices in the HA group. By default, system will use the default MAC address as the local MAC address of the HA link to send heartbeats. Besides, you can use the MAC address of the control link interface or a customized MAC as the local MAC address of the HA link. • If Default is selected, system will send heartbeat packets using the default MAC address. • If Control link interface MAC is selected, system will send heartbeat packets using the MAC address of the control link interface as the local MAC address of the HA link. • If Customize is selected, you need to type a MAC address into the **Mac** text box. Then, system will send heartbeat packets using the MAC address as the local MAC address of the HA link.
HA link local IP address	This function is only supported by vADC. Specify the IP address and netmask of the HA link interface.
HA link to side IP and MAC addresses	This function is only supported by vADC. Specify the IP and MAC addresses of the HA peer. By default, the two devices in the HA environment will negotiate through multicast mode. However, in a virtualized environment, some cloud platforms may require the devices to communicate with the assigned MAC address, otherwise packets will be dropped. System supports HA negotiation through Layer 2 unicast mode. When deploying HA, you can configure the HA peer IP address or configure both the peer IP and mac (i.e., the MAC address of the heartbeat interface) addresses on each device. Then, the two devices will negotiate through Layer 2 unicast mode.

Option	Description
HA virtual prefix	This function is only supported by vADC. Specify the prefix of the HA virtual MAC in hexadecimal format. Its length can only be configured as seven or eight. 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 the prefix is set to 7 hexadecimal, you can deploy up to 128 HA clusters on the same network segment. When the length of the 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, system will prompt the HA virtual MAC range to be generated and the configuration will take effect after reboot. By default, the prefix of the HA virtual MAC is 0x001C54FF. It should be noted that 0x00000000, 0x0000000, 0xFFFFFFFF, 0xFFFFFFF or multicast addresses (i.e., the second hexadecimal number is odd) are invalid.
HA cluster ID	Specify an ID for HA cluster. The ID ranges from 1 to 8 (When the length of the virtual prefix is set to 7 hexadecimal, the ID ranges from 1~128.). None indicates to disable the HA function.
HA Transmit UDP	This function is only supported by vADC. With this function enabled, HA Hello packets will be transmitted over the UDP protocol. By default, HA Hello packets are transmitted over the VRRP protocol. In a virtualized environment, the core switch limits the transmission rate and size of VRRP packets, affecting the synchronization between the HA master and backup devices. However, transmission over the UDP protocol can prevent the packets from being restricted by the core switch.
Business interface use physical MAC	This function is only supported by vADC. With this function enabled, the business interface of the device will forward traffic using the physical MAC address assigned by a cloud platform. If the function is disabled, the interface will forward traffic using the virtual MAC address assigned by system. The function is disabled by default.
Aliyun Deploy	This function is only supported by vADC. Only the vADC deployed on

Option	Description
HAVIP	Alibaba Cloud supports this function. With this function enabled, vADC will use the HAVIP function that Alibaba Cloud provides to deploy HA. If you use the secondary IP of the interface for HA deployment or do not want to deploy HA, you need to disable this function.
Accesskey ID	This function is only supported by vADC. Only the vADC deployed on Alibaba Cloud supports this function. Specify the AccessKey ID of your Alibaba Cloud account.
Accesskey Secret	This function is only supported by vADC. Only the vADC deployed on Alibaba Cloud supports this function. Specify the AccessKey ID of your Alibaba Cloud account.
Node ID	After enabling the HA function, specify the Node ID (HA Node) for the device. The IDs 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 by automatic negotiation.
HA Synchronize Configuration	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 devices. Click **HA Synchronize Configuration** to synchronize the configuration information of the master and backup devices.
HA Synchronize Session	By default, 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 automatic HA session synchronization according to the device workload to assure stability. Click **HA Synchronize Session** to enable automatic HA session synchronization.
HA Master Switch Over	Click **HA Master Switch Over** to manually switch between the master and backup devices. **Note**: You can only perform this operation on the HA master device.

Option	Description
Priority	Specify the priority for the device. The device with higher priority (smaller number) will be selected as the master device.
Preempt	Configure the preempt mode. When the preempt mode is enabled, once the backup device finds that its own priority is higher than the master device, it will upgrade itself to become the master device and the original master device will become the backup device. The value of 0 indicates to disable the preempt mode. 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.
Hello interval	Specify the Hello interval value. The 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.
Hello threshold	Specify the threshold value of the Hello message. If the device does not receive the specified number of Hello messages from the other device, it will suppose the other device's heartbeat stops.
Gratuitous ARP packet number	Specify the number of gratuitous ARP packets. 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.
Track object	Specify the track object you have configured. The track object is used to monitor the working status of the device. Once finding the device stop working normally, system will take the corresponding action.
Description	Type the descriptions of the HA group into the box.

2. Click **OK**.

Note:

- If the HA cluster ID is selected, it means that the HA function is enabled. In this case, if you want to modify the HA configuration, disable the HA function first.

- For vADC deployed on Alibaba Cloud, make sure that system can access Alibaba Cloud services, that is, vpc.aliyuncs.com can be pinged.
- For vADC deployed on Alibaba Cloud, make sure the time error between the system time and the time on the Alibaba Cloud platform is less than 15 minutes. For more information about the time configuration, see **Device Management** > "Device Management" on Page 498.

Chapter 17 aRule

ADC provides various load balance parameters that can be configured via WebUI and CLI, which can meet most user needs. Besides, for users with complex requirements, ADC provides a more convenient and flexible script interface for users to write scripts to control request.

Only HTTP and HTTPS virtual servers (VS) support using aRule scripts. If needed, contact Service Line: 1-800-889-9860 for help.