DS-3WG Access Controller Gateway Series

User Guide

Hangzhou Hikvision Digital Technology Co., Ltd.
https://www.hikvision.com

Document version: 6W102-20250117

COPYRIGHT © 2024-2025 Hangzhou Hikvision Digital Technology Co., Ltd.

ALL RIGHTS RESERVED.

Any and all information, including, among others, wordings, pictures, graphs are the properties of Hangzhou Hikvision Digital Technology Co., Ltd. or its subsidiaries (hereinafter referred to be “Hikvision”). This user manual (hereinafter referred to be “the Manual”) cannot be reproduced, changed, translated, or distributed, partially or wholly, by any means, without the prior written permission of Hikvision. Unless otherwise stipulated, Hikvision does not make any warranties, guarantees or representations, express or implied, regarding to the Manual.

About this Manual

This Manual is applicable to DS-3WG Access Controller Gateway Series.

The Manual includes instructions for using and managing the product. Pictures, charts, images and all other information hereinafter are for description and explanation only. The information contained in the Manual is subject to change, without notice, due to firmware updates or other reasons. Please find the latest version in the company website (https://www.hikvision.com).

Please use this user manual under the guidance of professionals.

Legal Disclaimer

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, THE PRODUCT DESCRIBED, WITH ITS HARDWARE, SOFTWARE AND FIRMWARE, IS PROVIDED “AS IS”, WITH ALL FAULTS AND ERRORS, AND HIKVISION MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION, MERCHANTABILITY, SATISFACTORY QUALITY, FITNESS FOR A PARTICULAR PURPOSE, AND NON-INFRINGEMENT OF THIRD PARTY. IN NO EVENT WILL HIKVISION, ITS DIRECTORS, OFFICERS, EMPLOYEES, OR AGENTS BE LIABLE TO YOU FOR ANY SPECIAL, CONSEQUENTIAL, INCIDENTAL, OR INDIRECT DAMAGES, INCLUDING, AMONG OTHERS, DAMAGES FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, OR LOSS OF DATA OR DOCUMENTATION, IN CONNECTION WITH THE USE OF THIS PRODUCT, EVEN IF HIKVISION HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

REGARDING TO THE PRODUCT WITH INTERNET ACCESS, THE USE OF PRODUCT SHALL BE WHOLLY AT YOUR OWN RISKS. HIKVISION SHALL NOT TAKE ANY RESPONSIBILITES FOR ABNORMAL OPERATION, PRIVACY LEAKAGE OR OTHER DAMAGES RESULTING FROM CYBER ATTACK, HACKER ATTACK, VIRUS INSPECTION, OR OTHER INTERNET SECURITY RISKS; HOWEVER, HIKVISION WILL PROVIDE TIMELY TECHNICAL SUPPORT IF REQUIRED.

SURVEILLANCE LAWS VARY BY JURISDICTION. PLEASE CHECK ALL RELEVANT LAWS IN YOUR JURISDICTION BEFORE USING THIS PRODUCT IN ORDER TO ENSURE THAT YOUR USE CONFORMS THE APPLICABLE LAW. HIKVISION SHALL NOT BE LIABLE IN THE EVENT THAT THIS PRODUCT IS USED WITH ILLEGITIMATE PURPOSES.

IN THE EVENT OF ANY CONFLICTS BETWEEN THIS MANUAL AND THE APPLICABLE LAW, THE LATER PREVAILS.

Environmental protection

This product is environment-friendly by design to minimize its environmental impact. The storage, use, and disposal of this product must be compliant with the applicable national laws and regulations.

Preface

This user guide describes the appearance, LEDs, and installation process of the device in details. In addition, it describes how to locally manage the device through the Web interface.

This preface includes the following topics about the documentation:

- Audience.
- Conventions.

Audience

This documentation is intended for:

- Network planners.
- Field technical support and servicing engineers.
- Network administrators.

Conventions

This section describes the conventions used in the documentation.

Port numbering in examples

The port numbers in the documentation are for illustration only and might be unavailable on your device.

Command conventions

Convention	Description
Boldface	**Bold** text represents commands and keywords that you enter literally as shown.
Italic	*Italic* text represents arguments that you replace with actual values.
[ ]	Square brackets enclose syntax choices (keywords or arguments) that are optional.
{ x | y | ... }	Braces enclose a set of required syntax choices separated by vertical bars, from which you select one.
[x | y | ...]	Square brackets enclose a set of optional syntax choices separated by vertical bars, from which you select one or none.
{ x | y | ... } *	Asterisk marked braces enclose a set of required syntax choices separated by vertical bars, from which you select at least one.
[x | y | ...] *	Asterisk marked square brackets enclose optional syntax choices separated by vertical bars, from which you select one choice, multiple choices, or none.
&<1-n>	The argument or keyword and argument combination before the ampersand (&) sign can be entered 1 to n times.
#	A line that starts with a pound (#) sign is comments.

GUI conventions

Convention	Description
Boldface	Window names, button names, field names, and menu items are in Boldface. For example, the **New User** window opens; click **OK**.

Convention	Description
>	Multi-level menus are separated by angle brackets. For example, **File** > **Create** > **Folder**.

Symbols

Convention	Description
⚠ **WARNING!**	An alert that calls attention to important information that if not understood or followed can result in personal injury.
△ **CAUTION:**	An alert that calls attention to important information that if not understood or followed can result in data loss, data corruption, or damage to hardware or software.
ⓘ **IMPORTANT:**	An alert that calls attention to essential information.
NOTE:	An alert that contains additional or supplementary information.
TIP:	An alert that provides helpful information.

Network topology icons

Convention	Description
	Represents a generic network device, such as a router, switch, or firewall.
	Represents a routing-capable device, such as a router or Layer 3 switch.
	Represents a generic switch, such as a Layer 2 or Layer 3 switch, or a router that supports Layer 2 forwarding and other Layer 2 features.
	Represents an access controller, a unified wired-WLAN module, or the access controller engine on a unified wired-WLAN switch.
	Represents an access point.
	Represents a wireless terminator unit.
	Represents a wireless terminator.
	Represents a mesh access point.
	Represents omnidirectional signals.
	Represents directional signals.
	Represents a security product, such as a firewall, UTM, multiservice security gateway, or load balancing device.
	Represents a security module, such as a firewall, load balancing, NetStream, SSL VPN, IPS, or ACG module.

Contents

Product overview 1
- Chassis views 1
  - DS-3WG105G-SI 1
  - DS-3WG105GP-SI 2
  - DS-3WG210GP-SI 2
  - DS-3WG507G-SI 3
- LEDs 3
- Ports 5
- Technical specifications 5
  - Desktop access controller gateway 5
  - Rack access controller gateway 6

Install the device 7
- Safety precautions 7
- Install the device 7
  - Install the device on a workbench 7
  - Install the device in a rack 8
- Install the device to a wall 9
- Connect cables 10
  - Connect the grounding cable 10
  - Connecting the power cord 11

Log in to the device 13

View system information or access the wizard 14
- About this feature 14
- View CPU usage and memory usage 14
- View connected endpoints 14
- View traffic rate information 14
- View device information 15
- View interface state information 15
- View storage media information 15
- Access a feature through quick access 15

Perform quick configuration 17
- About this feature 17
- Configure WAN settings 17
- Configure LAN settings 19

Configure system monitoring 20
- Configure link monitoring 20
  - About this feature 20
  - Procedure 20
- Configure traffic ranking 20
  - About this feature 20
  - Restrictions and guidelines 20
  - Procedure 21

Manage APs 23
- Configure AP management 23
  - About this feature 23
  - Restrictions and guidelines 23
  - Procedure 23
- Configure Wi-Fi settings 24
  - About this feature 24
  - Restrictions and guidelines 24
  - Procedure 24

Manage online APs ····· 24
About this feature ····· 24
View the AP list ····· 25
View the client list ····· 25
Manage AP versions ····· 25
About this feature ····· 25
Restrictions and guidelines ····· 25
Procedure ····· 25
Configure network settings ····· 27
Configure external network settings ····· 27
About this feature ····· 27
Configure the interface mode ····· 27
Configure WAN settings ····· 27
Edit a multi-WAN policy ····· 31
Configure last hop holding ····· 31
Configure LAN settings ····· 32
About this feature ····· 32
Configure VLANs ····· 32
Configure LAN interface settings ····· 33
Configure static DHCP ····· 35
Reclaim DHCP-assigned IP addresses ····· 36
Configure static bindings for DHCP-assigned IP addresses ····· 36
Manage ports ····· 36
About this feature ····· 36
Procedure ····· 37
Configure NAT ····· 38
About this feature ····· 38
Configure a virtual server ····· 38
Configure one-to-one mappings ····· 39
Configure address pools ····· 40
Configure port triggering ····· 41
Configure NAT hairpin ····· 41
Configure NAT ALG ····· 42
Configure user-defined protocol port numbers ····· 43
Configure network connections ····· 44
Configure address groups ····· 45
About this feature ····· 45
Restrictions and guidelines ····· 45
Procedure ····· 45
Configure PoE ····· 46
About this feature ····· 46
Configure PoE power supply ····· 46
Configure time range groups ····· 47
About this feature ····· 47
Restrictions and guidelines ····· 47
Procedure ····· 47
Configure application groups ····· 48
About this feature ····· 48
Configure user-defined applications ····· 48
Configure application groups ····· 49
Configure network behavior management ····· 51
Configure tasks at a glance ····· 51
Limit the bandwidth of a WAN interface ····· 51
Limit the bandwidth for applications ····· 51
Guarantee the bandwidth for applications ····· 51
Limit the applications that can be used ····· 51
Configure the URLs that can be visited through an allowlist ····· 52
Configure the URLs that cannot be visited through a denylist ····· 52
Limit the types of files that can be downloaded ····· 52
Configure bandwidth management ····· 53

About this feature 53
Restrictions and guidelines 53
Configure rate limiting 53
Configure the restricted channel 55
Configure the green channel 56
Configure network behavior management 57
About this feature 57
Configure application control 58
Configure URL control 61
Configure file control 62
Configure user-defined network applications 63
Configure audit logs 64
About this feature 64
Configure application audit logs 64
Configure URL filter logs 65
Configure an audit server 65
Configure network security 67
Deny inter-VLAN communication 67
Configure tasks at a glance 67
Configure the firewall 67
Configure connection limits 70
About this feature 70
Restrictions and guidelines 70
Configure per-IP connection limits 71
Configure VLAN-based connection limits 72
Configure MAC filter 73
About this feature 73
Configure MAC filter settings 74
Configure MAC denylist and allowlist 74
Configure ARP attack protection 76
About this feature 76
Manage ARP learning 77
Manage dynamic ARP entries 77
Manage static ARP entries 78
Configure ARP attack protection 79
Configure ARP attack detection 80
Configure DDoS attack prevention 81
About this feature 81
Specify attack prevention types 82
View attack prevention statistics 85
Configure packet source authentication 85
Configure abnormal traffic prevention 86
Configure security statistics 87
About this feature 87
Procedure 87
Manage denylist 87
About this feature 87
Procedure 87
Configure access control 88
About this feature 88
Procedure 88
Configure VPNs 89
Configuration tasks at a glance 89
Set up an IPsec VPN 89
Set up an L2TP VPN 89
Set up an IPsec VPN 89
About this feature 89
Configure an IPsec branch node 90
Configure an IPsec HQ node 93
View monitor information 97

Configure an L2TP server 97
About this feature 97
Configure L2TP settings 97
View tunnel information 99
Configure L2TP users 99
Configure an L2TP client 101
About this feature 101
Restrictions and guidelines 101
Configure L2TP settings 101
View tunnel information 103
Configure advanced settings 104
Configuration tasks at a glance 104
Configure DDNS 104
Specify an output interface for packets with the specified destination IP address 104
Configure PBR 104
Manage application services 104
Configure static DNS 105
Configure DDNS 106
Configure the local DNS service 107
UPnP 108
About this task 108
Restrictions and guidelines 108
Procedure 108
Configure static routing 109
About this task 109
Restrictions and guidelines 109
Procedure 109
Configure PBR 110
About this task 110
Procedure 111
Use system tools 113
Configure system settings 113
About this feature 113
Configure device information 113
Manually set the date and time 113
Configure automatic date and time synchronization 114
Perform network diagnosis 115
About this feature 115
Configure ping 115
Configure tracert 116
Perform a system self-test 117
Collect diagnostic information 117
Configure port mirroring 117
Capture packets 118
Configure remote management 119
About this feature 119
Permit ping on an interface 119
Configure Telnet login 120
Configure HTTP/HTTPS login 121
Use the cloud service 123
Manage configuration 123
About this feature 123
Restore the factory defaults 124
Restore configuration from a backup file 124
Export the running configuration 126
Fast back up the running configuration to a USB drive 126
Fast restore the device configuration from a USB drive 126
Upgrade the system 127
About this feature 127
Restrictions and guidelines 127

Manually upgrade the software 127
Use a USB drive to restore the system software 127
Reboot the device 128
About this feature 128
Reboot the device immediately 128
Configure scheduled reboot 128
Manage system logs 129
About this feature 129
Send system logs to a log server 129
View system logs on the Web page 130
Clear system logs 131
Manage the admin account 132
About this feature 132
Edit the admin account 132

Product overview

NOTE:

The functional introduction involved in this manual is verified through configuration on the DS-3WG105G-SI. If configuration differences exist on the DS-3WG105G-SI, they will be explained separately in the relevant sections.

HIKVISION DS-3WG series access controller gateways include the following models.

- DS-3WG105G-SI (European standard)
- DS-3WG105G-SI (non-European standard)
- DS-3WG105GP-SI
- DS-3WG210GP-SI
- DS-3WG507G-SI

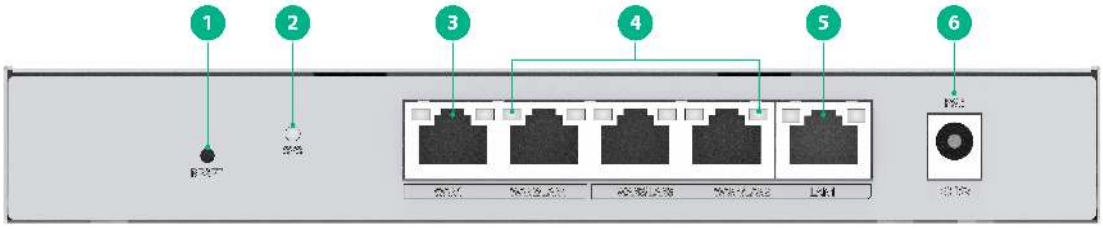
Chassis views

DS-3WG105G-SI

NOTE:

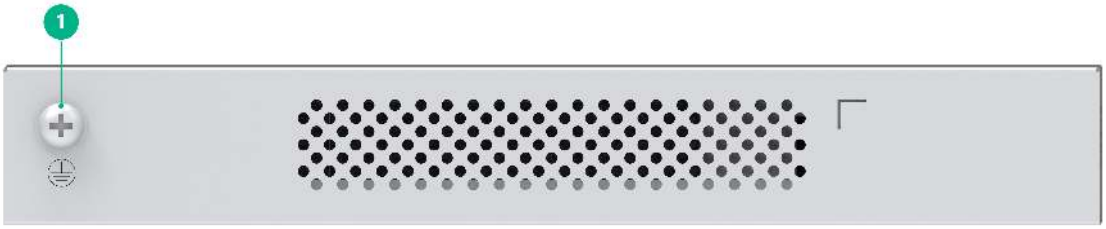
The DS-3WG105G-SI (European standard) and DS-3WG105G-SI (non-European standard) models are only different in the power adapter. All other appearances and specifications are the same.

Figure 1 DS-3WG105G-SI front panel



(1) Reset button (RESET)	(2) System LED (SYS)
(3) WAN port and LED (10/100/1000Base-T copper port)	
(4) WAN/LAN ports and LEDs (10/100/1000Base-T copper port)	
(5) LAN port and LED (10/100/1000Base-T copper port)	(6) Power port

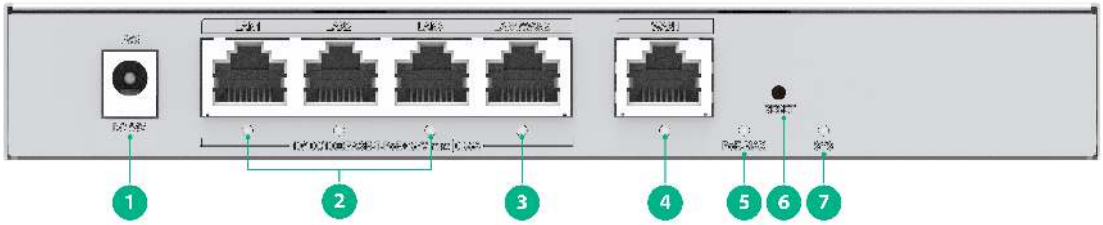
Figure 2 DS-3WG105G-SI rear panel



(1) Grounding screw

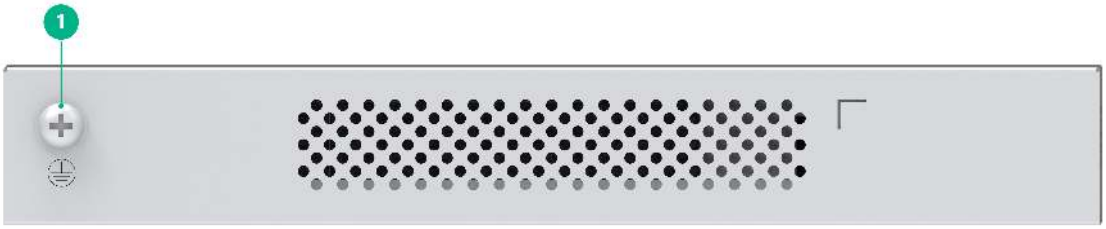
DS-3WG105GP-SI

Figure 3 DS-3WG105GP-SI front panel



(1) Power port	(2) LAN ports and LEDs (10/100/1000Base-T copper port)
(3) LAN/WAN port and LED (10/100/1000Base-T copper port)	
(4) WAN port and LED (10/100/1000Base-T copper port)	
(5) PoE-MAX LED (PoE-MAX)	(6) Reset button (RESET)
(7) System LED (SYS)	

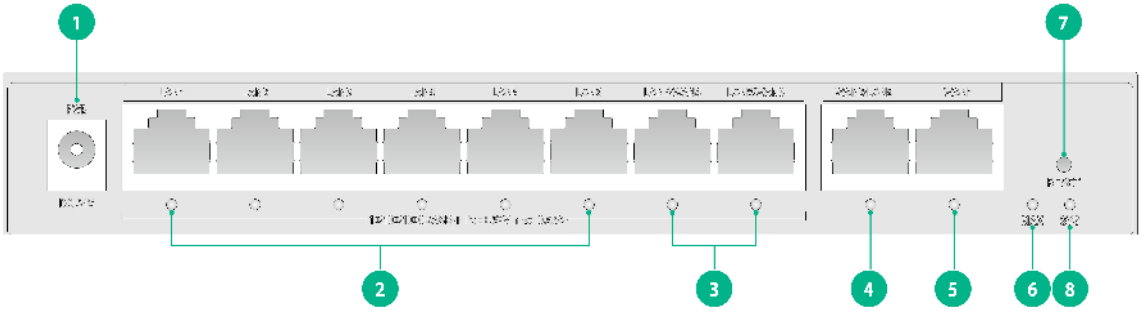
Figure 4 DS-3WG105GP-SI rear panel



(1) Grounding screw

DS-3WG210GP-SI

Figure 5 DS-3WG210GP-SI front panel



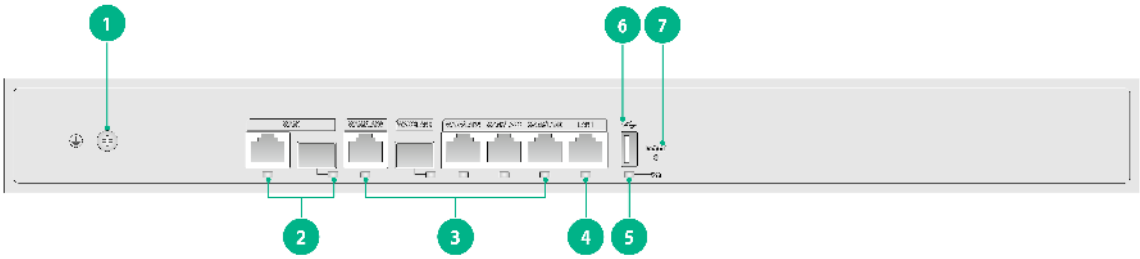
(1) Power port	(2) LAN ports and LEDs (10/100/1000Base-T copper port)
(3) LAN/WAN ports and LEDs (10/100/1000Base-T copper port)	
(4) WAN/LAN port and LED (10/100/1000Base-T copper port)	
(5) WAN port and LED (10/100/1000Base-T copper port)	
(6) PoE-MAX LED (MAX)	(7) Reset button (RESET)
(8) System LED (SYS)	

Figure 6 DS-3WG210GP-SI rear panel

(1) Grounding screw	

DS-3WG507G-SI

Figure 7 Front panel



(1) Grounding screw	(2) WAN ports and LEDs (Combo port)
(3) WAN/LAN ports and LEDs (10/100/1000BASE-T copper port, 1000BASE-X-SFP fiber port)	
(4) LAN port and LED (10/100/1000Base-T copper port)	
(5) System LED (SYS)	(6) USB port
(7) Reset button (RESET)	

Figure 8 DS-3WG507G-SI rear panel

(1) Power port

LEDs

LED	Status	Description
System status LED (SYS)	Steady green	The device is operating correctly.
	Steady amber	An alarm or error is present on the system.
	Slowly flashing amber	The device will restore the default Web login password.
	Fast flashing amber	The device will restore the factory defaults and then reboot.

LED	Status	Description
	Off	• Power shutdown • Power failure • Device hardware failure
WAN/LAN port status LEDs (LINK/ACT) (applicable to the DS-3WG105G-SI)	Green LED: Steady on Amber LED: Steady on	A link is present on the port, and the port is operating at 1000 Mbps.
	Green LED: Steady on Amber LED: Flashing	The port is sending or receiving data at 1000 Mbps.
	Green LED: Off Amber LED: Steady on	A link is present on the port, and the port is operating at 10/100 Mbps.
	Green LED: Off Amber LED: Flashing	The port is sending or receiving data at 10/100 Mbps.
	Off	No link is present on the device.
WAN/LAN port status LED (LINK/ACT) (applicable to the DS-3WG507G-SI)	Steady green	A link is present on the port, and the port is operating at 1000 Mbps.
	Flashing green	The port is sending or receiving data at 1000 Mbps.
	Steady amber	A link is present on the port, and the port is operating at 10/100 Mbps.
	Flashing amber	The port is sending or receiving data at 10/100 Mbps.
	Off	No link is present on the device.
WAN/LAN port status LED (LINK/ACT) (applicable to the DS-3WG105GP-SI and DS-3WG210GP-SI)	Steady green	A link is present on the port, and the port is operating at 10/100/1000 Mbps.
	Flashing green	The port is sending or receiving data at 10/10/100 Mbps.
	Off	No link is present on the device.
SFP fiber port statue LED	Steady green	A link is present on the port, and the port is operating at 1000 Mbps.
	Flashing green	The port is sending or receiving data at 1000 Mbps.
	Steady amber	A link is present on the port, and the port is operating at 10/100 Mbps.
	Flashing amber	The port is sending or receiving data at 10/100 Mbps.
	Off	No link is present on the device.
PoE-MAX LED	Steady green	The power supplied by the PoE device is within its protection power range, which is 60 W to 75 W on a DS-3WG210GP-SI and 47 W to 58 W on a DS-3WG105GP-SI.
	Off	The power supplied by the PoE device has not reached the minimum value of the protection power range.

Ports

Port	Description
Reset button (RESET)	• To reboot the device, press and hold the button less than 5 seconds. • To restore the default Web login password, press and hold the button for 5 to 10 seconds until the system status LED (SYS) slowly flashes amber. • For the device to restore the factory defaults and reboot, press and hold the reset button for 10 to 15 seconds until the system status LED (SYS) fast flashes amber. • If you press and hold the button over 15 seconds, the system status LED (SYS) returns to steady green and the device will not perform any recovery actions.
USB port	Connect to a storage medium (such as a USB flash drive or mobile disk), which allows quick backup or restoration of the device configuration, as well as software version restoration.
Power port	Connect power.
LAN port	Connect to an Ethernet port on a computer or downstream switch.
WAN port	Connect to a network interface provided by the broadband service provider for Internet access.

LAN/WAN port, WAN/LAN port	• Can be used as either a LAN port or a WAN port.
	• Whether the port operates as a LAN port or WAN port by default depends on its shading color.
	  ○ **Yellow**—The port operates as a WAN port by default.
	  ○ **Green**—The port operates as a LAN port by default.

Grounding screw	Connect the grounding cable

Technical specifications

Desktop access controller gateway

Item	DS-3WG105G-SI	DS-3WG105GP-SI	DS-3WG210GP-SI
Dimensions (H × W × D)	44 × 266 × 161 mm (1.73 × 10.47 × 6.34 in)	27 × 190 × 125 mm (1.06 × 7.48 × 4.92 in)	27 × 190 × 125 mm (1.06 × 7.48 × 4.92 in)
Power consumption	< 4.73 W	< 63.18 W	< 80 W
Power adapter rated input voltage	100 to 240 VAC @ 50/60 Hz	100 to 240 VAC @ 50/60 Hz	100 to 240 VAC @ 50/60 Hz
Device power input	12 V ± 5%/1 A	54 V ± 5%/1.17 A	54 V ± 5%/1.48 A
Max output power per port	N/A	30 W	30 W
PoE power output	N/A	58 W	75 W
Weight	0.44 kg (0.97 lb)	0.45 kg (0.99 lb)	0.5 kg (1.10 lb)
Console port	N/A	N/A	N/A
USB port	N/A	N/A	N/A
LAN port	3 × Gigabit copper ports (two of them are	4 × Gigabit copper ports (one of them is	8 × Gigabit copper ports (two of them are switchable

Item	DS-3WG105G-SI	DS-3WG105GP-SI	DS-3WG210GP-SI
	switchable to WAN ports)	switchable to a WAN port)	to WAN ports)
WAN port	2 × Gigabit copper ports (only one is switchable to a LAN port)	1 × Gigabit copper port (WAN mode only)	2 × Gigabit copper ports (only one is switchable to a LAN port)
Operating temperature	0°C to 45°C (32°F to 113°F)	0°C to 40°C (32°F to 104°F)	0°C to 40°C (32°F to 104°F)
Operating humidity	5% RH to 95% RH, noncondensing	5% RH to 95% RH, noncondensing	5% RH to 95% RH, noncondensing
Heat dissipation method	Passive cooling	Passive cooling	Passive cooling

Rack access controller gateway

Item	DS-3WG507G-SI
Dimensions (H × W × D)	44 × 440 × 227.4 mm (1.73 × 17.32 × 8.95 in)
Power consumption	< 36 W
Power adapter rated input voltage	N/A
Device power input	100 to 240 VAC @ 50/60 Hz
Max output power per port	N/A
PoE power output	N/A
Weight	2.4 kg (5.29 lb)
Console port	N/A
USB port	1 × USB 2.0 port
LAN port	4 × Gigabit copper ports (three of them are switchable to LAN ports)
WAN port	• 1 × combo interface (WAN mode only) • 1 × Gigabit copper port (switchable to a LAN port) • 1 × Gigabit fiber port (switchable to a LAN port)
Operating temperature	0°C to 40°C (32°F to 104°F)
Operating humidity	5% RH to 95% RH, noncondensing
Heat dissipation method	Passive cooling

Install the device

You can install the device in a rack or on a workbench. This section uses an DS-3WG507G-SI as an example.

Safety precautions

To ensure correct operation and long service life of the device, follow these restrictions and guidelines:

- Use the device indoors only and place it in a dry and well-ventilated location.
- To prevent potential damage from a fall, do not place the device on an unstable support platform, such as an unstable table.
- Keep the device clean and dust-free. Do not place it in damp areas or let liquids enter the interior.
- Do not place open flame sources, such as lit candles, on the device.
- Reserve a minimum clearance of 10 cm (3.94 in) around the device for heat dissipation.
- Do not cover the ventilation holes with items such as newspapers, tablecloths, or curtains, as this could obstruct airflow. Avoid placing the device on sofas, carpets, or similar surfaces that could block the cooling vents.
- The device's interface cables must be routed indoors, not outdoors, to prevent signal port damage from overvoltage or overcurrent caused by lightning.
- Make sure the device's plug or socket, which is used to disconnect power, is accessible for easy insertion and removal.
- Before wiring, installing, or dismantling the device, make sure the power is off.
- After powering off the device, avoid touching any exposed parts on the external incoming side (such as the metal parts of the plug) for 5 minutes as they may still carry voltage.
- The device's protective grounding must be reliably connected to the building's grounding system.
- Set up the grounding facility for the device separately and away from that of power distribution equipment and lightning protection system.
- Position the device far away from high-power radio transmitters, radar transmitters, and high-frequency, high-current equipment.
- Use only the power cord supplied with the device. Do not use any non-matching products. The power voltage must be in the input voltage range of the dedicated power cord.
- If the device exhibits signs of smoke, unusual odors, or strange noises, immediately disconnect the device's power source and contact the dealer or service center promptly.

Install the device

The device supports installing on a workbench or in a rack. This section uses the DS-3WG507G-SI as an example.

Install the device on a workbench

△ **CAUTION:**

Make sure the workbench is stable and reliably grounded. Do not place heavy objects on the device.

NOTE:

The DS-3WG105G-SI, DS-3WG105GP-SI, and DS-3WG210GP-SI can be installed on a workbench directly without the rubber feet.

Attach the rubber feet to the bottom of the device. Then place the device on the workbench with the top side facing upwards.

Figure 9 Installing the device on a workbench

Install the device in a rack

NOTE:

Only the DS-3WG507G-SI supports installing in a rack.

Install cage nuts

Attach mounting brackets to the device

Rack-mount the device

Install the device to a wall

NOTE:

Only the DS-3WG105G-SI and DS-3WG105GP-SI supports installing to a wall.

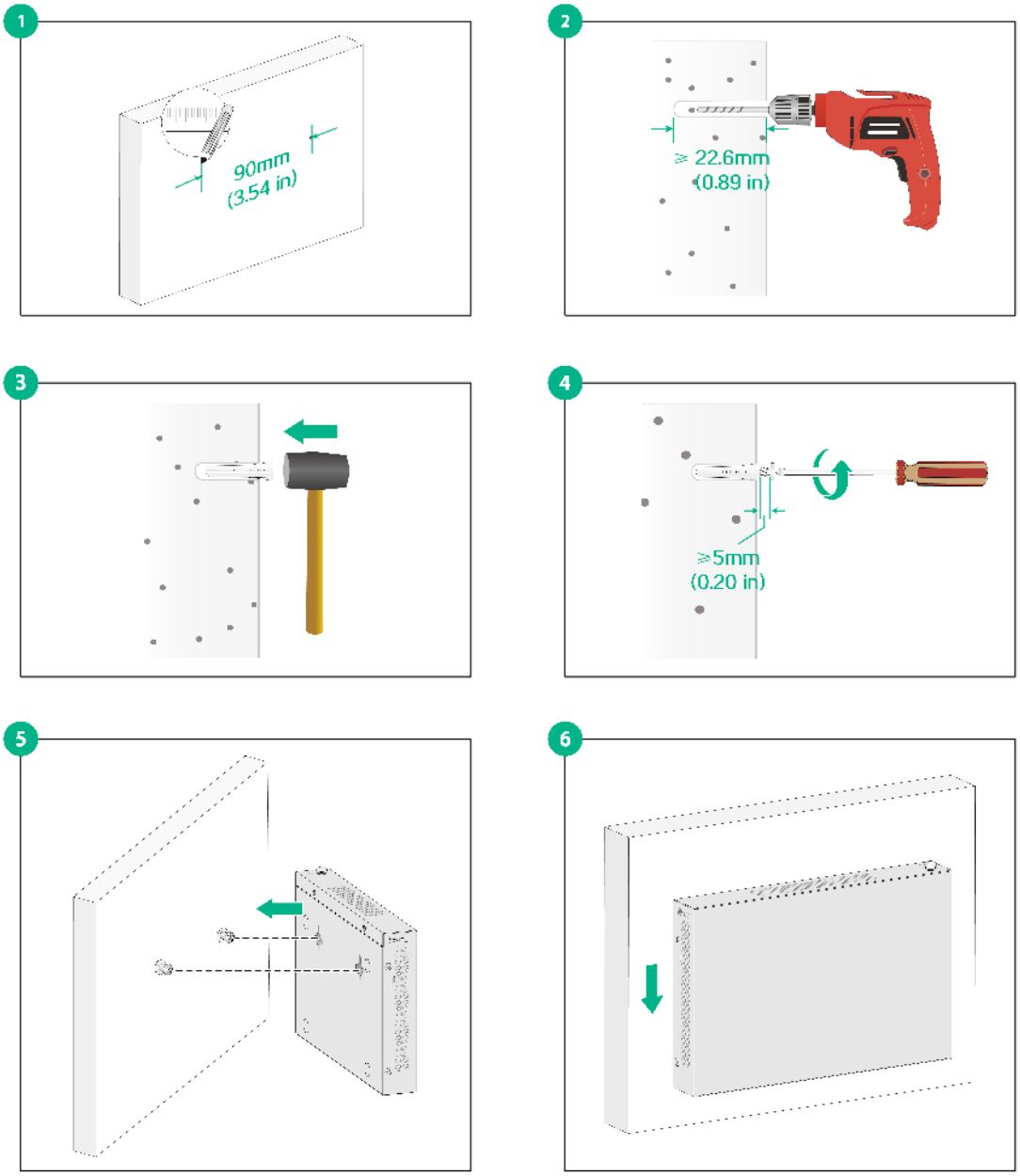
1. Drill two holes for the wall-mount screws on the vertical surface. Make sure the holes are at least 22.6 mm (0.89 in) deep.

   Make sure the two holes align horizontally with the following spacing.

Spacing	Device model
90 mm (3.54 in)	DS-3WG105G-SI
80 mm (3.15 in)	DS-3WG105GP-SI

2. Insert a screw anchor into each wall hole until its end is flush with the wall surface.
3. Screw the screws into the anchors, ensuring a gap of no less than 5 mm (0.20 in) between each screw end and the wall surface.
4. Hang the device on the screws.

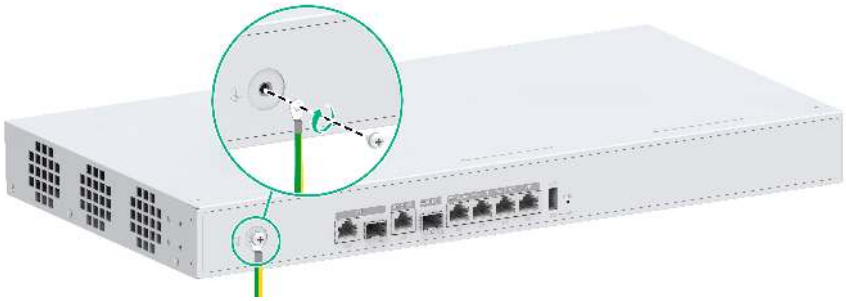
Figure 10 Install the device to a wall (DS-3WG105G-SI)



Connect cables

Connect the grounding cable

1. Connect one end of the grounding cable to the grounding hole of the device.
2. Wind the other end of the grounding cable to the grounding strip.



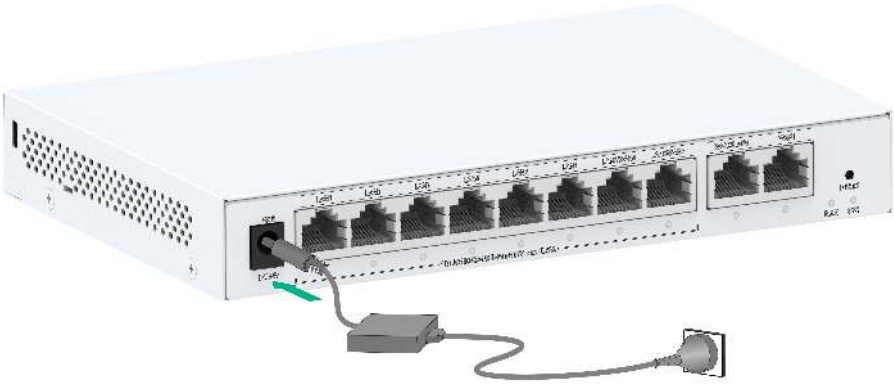
Connecting the power cord

CAUTION:

- Only the DS-3WG507G-SI supports direct power connection by using an AC power cord. For other device models, a power adapter is required for power supply.
- To prevent adapter damage because of insufficient power, use the power adapter that came with the device for power supply.
- Before connecting the power cord, make sure the device is reliably grounded.

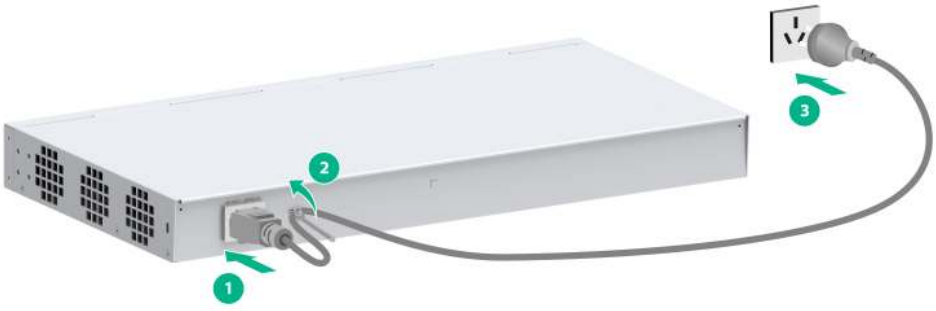
Connect a power adapter

1. Connect one end of the power adapter into the power port on the device.
2. Connect the other end of the power adapter to an external AC power source.



Connect an AC power cord

1. Connect one end of the AC power cord to the AC power receptacle on the device and then use the cable tie to secure the power cord.
2. Connect the other end of the power cord to an external AC power source.


1
2
3

Log in to the device

NOTE:

As a best practice for optimal performance, access the Web management page using Internet Explorer 10 or higher, Chrome 57 or higher, or Firefox 35 or higher.

1. Connect a PC to the LAN port of the device.
2. Configure your PC to automatically obtain an IP address (recommended) or manually set the PC's IP address to be in the same subnet as 192.168.9.0/24.
3. Check the proxy server settings on your PC. If your PC accesses the internet through a proxy, you must first disable this service.
4. Open a web browser. Enter http://192.168.9.1 (the device's default management IP address, modifiable after login) in the address bar and press **Enter**.
5. As shown below, enter the administrator username (default is **admin**) in the pop-up window and click to log in to the device. Upon first login, the system will automatically display the activation page. Enter and confirm your new password, then click **Apply** to complete activation.

View system information or access the wizard

About this feature

You can view device operation information, use the wizard for basic settings, and obtain technical support.

View CPU usage and memory usage

About this task

Perform this task to view information about CPU usage and memory usage, including:

- Current CPU usage and average CPU usage.
- Current memory usage and average memory usage.
- System time and system uptime.
- Device model, serial number, and software version.
- Storage space usage on the storage media.
- Current status of WAN interfaces and LAN interfaces.

Procedure

1. From the left navigation pane, select **System Info**.
2. Click the **CPU Usage** or **Memory Usage** section to view the current CPU usage and average CPU usage or the current memory usage and average memory usage.

View connected endpoints

About this task

Perform this task to view information about connected endpoints, including:

- Real-time traffic Top 5.
- Number of online endpoints and number of network connections on online endpoints.
- Online endpoint information table, including endpoint IPs, endpoint names, number of network connections, access methods, interfaces, and MAC addresses of endpoints.

Procedure

1. From the left navigation pane, select **System Info**.
2. Click the **Connected Endpoints** section to view information about connected endpoints.

View traffic rate information

About this task

Perform this task to view network traffic information on the device, including average uplink speed in last 5 minutes, average downlink speed in last 5 minutes, WAN interface status, and network access parameters.

Procedure

1. From the left navigation pane, select **System Info**.
2. Click the **Traffic Rate-WAN Interface** section to view network traffic information.

View device information

About this task

Perform this task to view device information, including system time and device model.

Procedure

1. From the left navigation pane, select **System Info**.
2. You can view system time, uptime, device model, serial number, Boot ROM version, and hardware version, and software version.

View interface state information

About this task

Perform this tack to view usage information of WAN interfaces and LAN interfaces.

Procedure

1. From the left navigation pane, select **System Info**.
2. In the **Interface State** section, click an interface icon to enter the WAN settings page or LAN settings page.

View storage media information

About this task

Perform this task to view storage space usage of the storage media on the device.

Procedure

1. From the left navigation pane, select **System Info**.
2. You can view the storage space usage of the storage media on the device in the lower right corner of the page.

Access a feature through quick access

To access a feature through quick access and quickly configure network settings for the device:

1. From the left navigation pane, select **System Info**.
2. Click **Quick Access**.
3. To configure a feature, click the corresponding feature link as follows:
   - **Network Settings**
     - **Connect to the Internet**—Click **Connect to the Internet** to go to the **External Networks** page.
     - **LAN Settings**—Click **LAN Settings** to go to the **LANs** page.
     - **NAT**—Click **NAT** to go to the **NAT** page.
   - **Network Behaviors**

- **Application Control**—Click **Application Control** to go to the **Application Control** tab on the **Network Behaviors** page.
- **URL Control**—Click **URL Control** to go to the **URL Control** tab on the **Network Behaviors** page.
- **File Control**—Click **File Control** to go to the **File Control** tab on the **Network Behaviors** page.
- **Rate Limiting**—Click **Rate Limiting** to go to the **Rate Limiting** tab on the **Bandwidth Mgmt** page.
- **Connection Limits**—Click **Connection Limits** to go to the **Per-IP Connection Limits** tab on the **Connection Limits** page.
- **Traffic Ranking**—Click **Traffic Ranking** to go to the **Traffic Ranking** page.

o **Access Security**

- **ARP Attack Protection**—Click **ARP Attack Protection** to go to the **ARP Attack Protection** page.
- **Firewall**—Click **Firewall** to go to the **Firewall** page.
- **VPN Settings**—Click **VPN Settings** to go to the **IPsec VPN** page.
- **MAC Address Filtering**—Click **MAC Address Filtering** to go to the **MAC Filter** page.

o **Device Maintenance**

- **Backup & Restore**—Click **Backup & Restore** to go to the **Configuration** page.
- **System Upgrade**—Click **System Upgrade** to go to the **System Upgrade** page.
- **Reboot**—Click **Reboot** to go to the **Reboot** page.
- **Remote Management**—Click **Remote Management** to go to the **Remote Management** page.
- **Network Diagnostics**—Click **Network Diagnostics** to go to the **Info Collector** page.
- **FAQ**—Click **FAQ** to go to the **FAQ** page.

Perform quick configuration

About this feature

After you complete the basic configuration of WAN and LAN through quick configuration, users in the LAN can access the Internet.

Configure WAN settings

Restrictions and guidelines

The device supports two WAN access scenarios: single WAN and dual WAN. For models that support only dual WAN, the single WAN option is not displayed on the **Quick Settings** page. If the user only rents services of one ISP, select the single WAN scenario. If the user rents services of two ISPs, select the dual WAN scenario. The configuration methods are the same for the single WAN and dual WAN scenarios.

NOTE:

- Support for the single WAN scenario and dual WAN scenario depends on the device model.
- You can configure single WAN or dual WAN through quick configuration. To configure a multi-WAN scenario, navigate to the **Network Settings** > **External Networks** page.

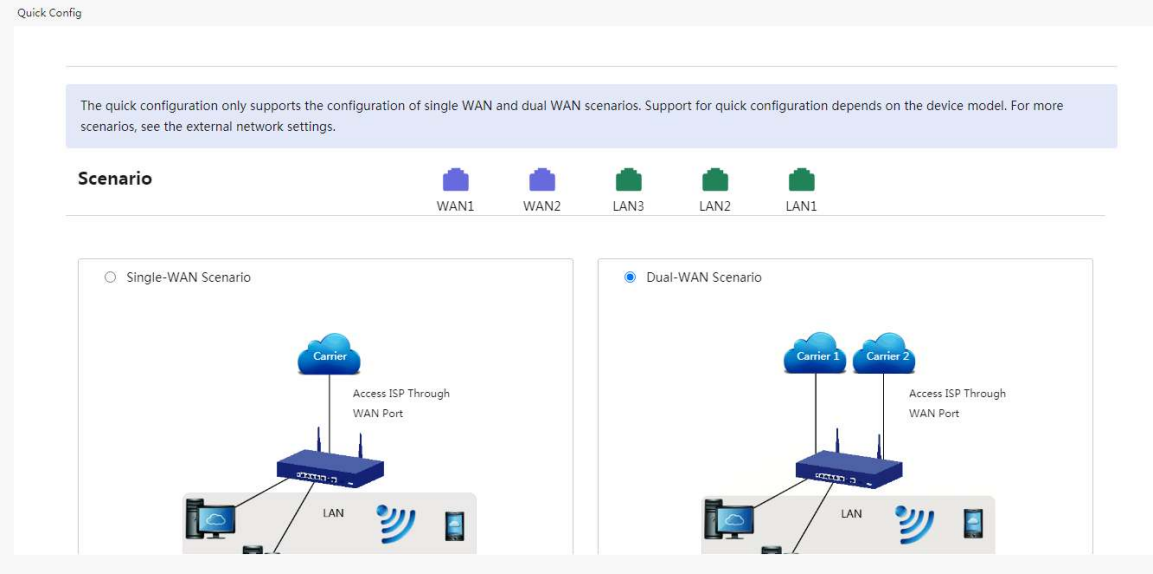
Procedure

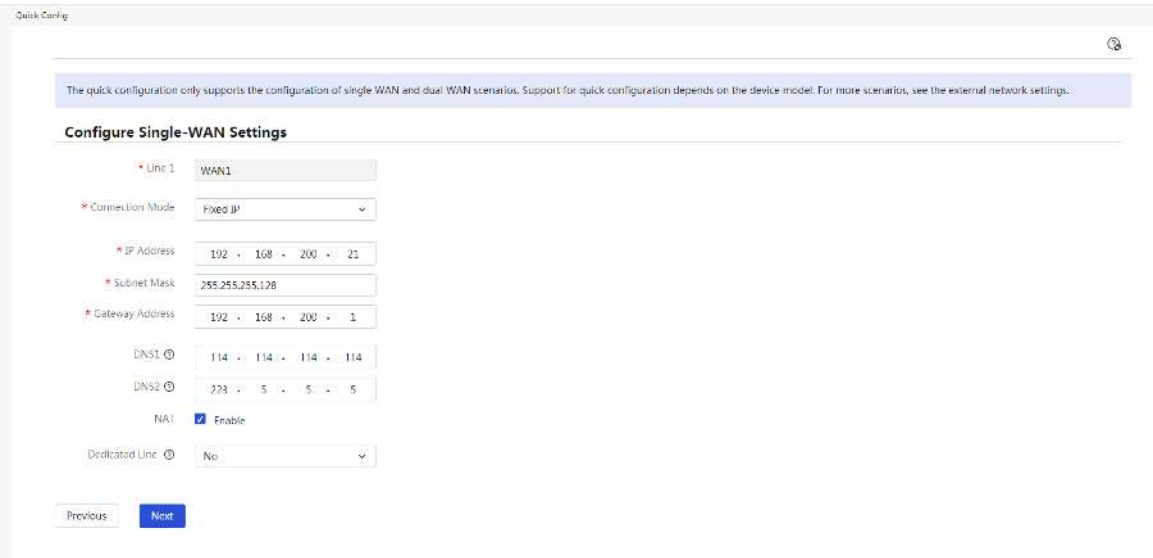
1. From the left navigation pane, select **Quick Config**.
2. Select the single WAN scenario or dual WAN scenario as needed, and configure WAN access setting.
3. Select a connection mode.
   - If you select **PPPoE**, configure the following:
     - In the **User ID** field, enter the username provided by the ISP.
     - In the **User Password** field, enter the password provided by the ISP.
     - In the **DNS1**/**DNS2** field, enter the DNS server address used by the device to access the WAN. The device first uses DNS 1 to translate domain names. If the translation fails, the device tries again with DNS 2.
   - If you select **DHCP**, configure the following:

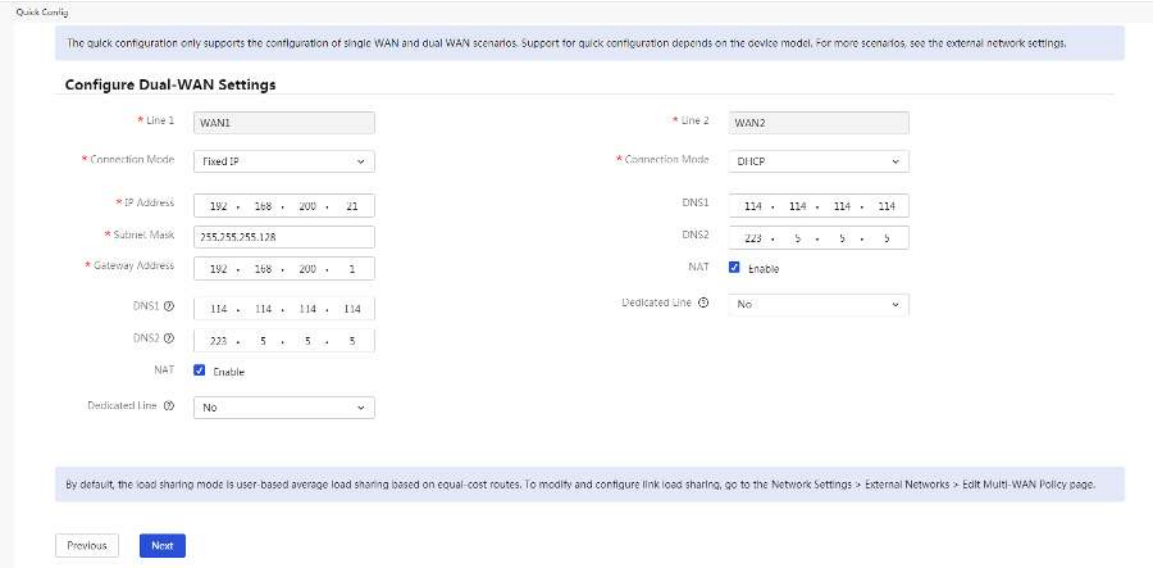
     In the **DNS1**/**DNS2** field, enter the DNS server address used by the device to access the WAN. The device first uses DNS 1 to translate domain names. If the translation fails, the device tries again with DNS 2.
   - If you select **Fixed IP**, configure the following:
     - In the **IP Address** field, enter the fixed IP address used by the device to access the WAN. Only class-A, class-B, and class-C IP addresses are supported.
     - In the **Subnet Mask** field, enter the IP address mask or mask length, for example, 255.255.255.0 or 24.
     - In the **Gateway Address** field, enter the gateway IP address used by the device to access the WAN. Only class-A, class-B, and class-C IP addresses are supported.
     - In the **DNS1**/**DNS2** field, enter the DNS server address used by the device to access the WAN. The default DNS1 address is 114.114.114.114 and the default DNS2 address is 223.5.5.5. The device first uses DNS 1 to translate domain names. If the translation fails, the device tries again with DNS 2. .

4. Enable NAT as needed. If multiple devices in the LAN use the same public network IP address, enable this feature.
5. Select whether to specify the current line as a dedicated line.
   - **Yes**: Specify the current line as the dedicated line. Then, you need to configure static route settings.
   - **No**: Not specify the current line as the dedicated line.

   Dedicated lines such as medical and public security lines are typically designed for specific purposes and are not connected to external networks.
6. Click **Next**.

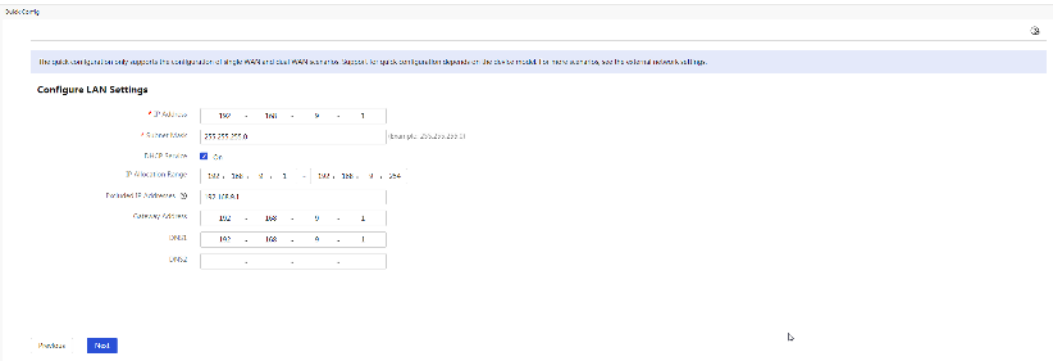






Configure LAN settings

1. In the **IP Address** field, enter the IP address used by the device in the LAN.
2. In the **Subnet Mask** field, enter the IP address mask or mask length, for example, 255.255.255.0 or 24. The input subnet mask length will be automatically converted to the decimal dotted format of the subnet mask.
3. In the **DHCP Service** field, select whether to enable DHCP service. To enable the device to act as the DHCP server to assign IP addresses to hosts in the LAN, select **On** for this field.
   - If you select **On**, configure the following settings:
     - **IP Allocation Range**: Enter the start address and end address of an address range for IP address allocation.
     - **Excluded IP Addresses**: Enter IP addresses in the IP allocation range that cannot be assigned to hosts, such as the IP address of the gateway.
     - **Gateway Address**: Enter the gateway address for hosts in the LAN.
     - **DNS1**/**DNS2**: Enter the DNS server address used by the device to access the WAN. The device first uses DNS 1 to translate domain names. If the translation fails, the device tries again with DNS 2.
   - If you do not select **On**, the DHCP service is disabled.
4. Click **Next**. Verify the configuration and click **Apply** to compete quick configuration.



Configure system monitoring

Configure link monitoring

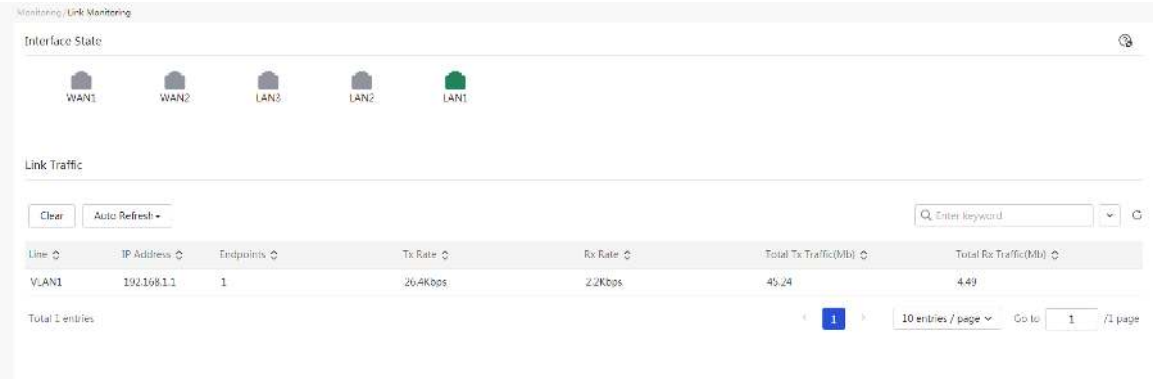
About this feature

Link monitoring presents interface states and link traffic statistics for traffic analysis and auditing.

The page displaying varies by device model.

Procedure

1. From the left navigation pane, select **Monitoring** > **Link Monitoring**.
2. In the **Interface State** section, click an interface icon to access the WAN or LAN configuration page.
3. In the **Link Traffic** section, view information about link traffic in the list.



Configure traffic ranking

About this feature

Traffic ranking displays the traffic information of endpoints for network behavior analysis and auditing. The displayed information includes the endpoint IP address, total amount of traffic on the current day, and online duration.

Restrictions and guidelines

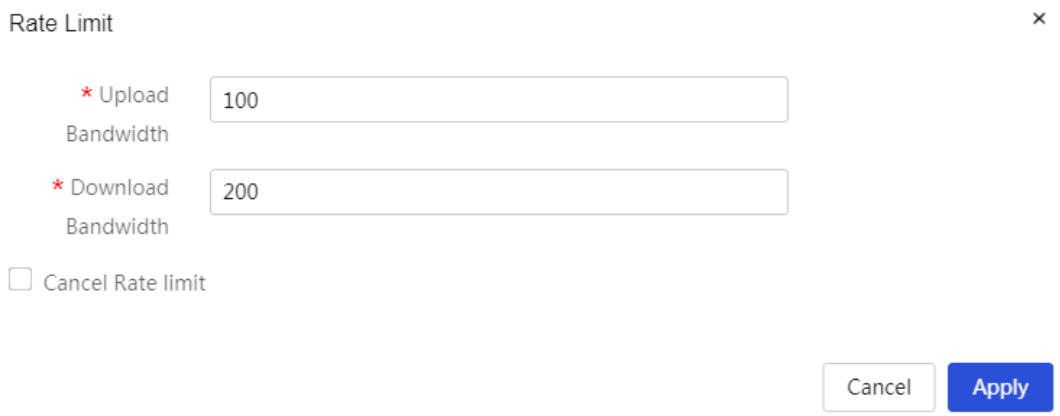
- The traffic ranking list displays only the online IP traffic information of the current users who are accessing the Internet.
- The traffic ranking list displays the traffic statistics during the most recent 5 minutes for endpoints connected to the device.
- The connection count is the number of connections that an internal IP address initiates to the Internet. The following connections are not counted: connections to the device and to other internal IP addresses, and connections from the Internet to the internal IP address.

- The counted connections in the traffic ranking list contain TCP connections, UDP connections, and other connections (connections other than TCP connections and UDP connections, for example, ICMP connections).
- The total amount of traffic indicates the traffic sent from an IP address continuously. If no traffic from an IP address is present for a period of time, the total amount of traffic is re-counted.
- The traffic units can be converted as follows: 1 Gbit=1000 Mbit=1000000 Kbit=1000000000 bit

Procedure

1. From the left navigation pane, select **Monitoring** > **Traffic Ranking**.
2. Select **Enable Traffic Ranking**.

3. Configure rate limit.
   a. In the traffic ranking list, click the rate limit icon in the **Actions** column for an endpoint IP address. The rate limit dialog box opens,
   b. Specify the upload bandwidth.
   c. Specify the download bandwidth.
   d. Select **Cancel Rate Limit** to cancel rate limit for the endpoint.
   e. Click **Apply**.



4. Add an endpoint to the denylist.
   a. In the traffic ranking list, click the denylist icon in the **Actions** column for an endpoint IP address. The denylist dialog box opens.
      – To deny the endpoint for a period, specify the period in the **Denylisted for** field.
      – To deny the endpoint permanently, select **Permanently Denylisted**.
   b. Click **Apply**.

Denylist

This operation will add the endpoint to the denylist, and disable it from accessing the Internet.

- (●) Denylisted for 10 (10-71582 min)
- ( ) Permanently Denylisted

Cancel Apply

Manage APs

Configure AP management

About this feature

You can centrally manage the connected APs by enabling the AP management function.

Restrictions and guidelines

Some clients may not be able to access the wireless service after being kicked offline multiple times. Please be cautious when you enable the weak-signal client optimization feature.

Procedure

1. From the left navigation pane, select **APs** > **AP Mgmt**.
2. Click **View the list of supported AP models** to view AP models supported by the device.
3. Select whether to enable AP management. If AP management is enabled, the device can manage the associated APs.
4. Select whether to enable smart optimization.
5. Select whether to turn on the AP LED. With this feature enabled, the LED is green when the AP is online and is blue when the AP is offline.
6. Select whether to enable optimization for weak-signal clients (2.4GHz)/(5GHz):
   - Select whether to enable weak-signal client optimization for the 2.4 GHz network. If you enable this feature, configure the parameters as needed:
     - **Weak Signal RSSI Threshold**: Clients with a signal strength lower than the threshold cannot connect to the network. The value range is 1 to 30 dB. A higher threshold may cause difficulties in client access. Configure this parameter according to the actual situation.
     - **Client Reconnection Threshold**: For an online client, when the signal strength drops below the threshold, the client is kicked offline and attempts to reconnect. The value range is 0 to 29 dB. Note that the client reconnection threshold must be lower than the weak-signal RSSI threshold.
   - Select whether to enable weak-signal client optimization for the 5GHz network. If you enable this feature, configure the parameters as needed:
     - **Weak Signal RSSI Threshold**: Clients with a signal strength lower than the threshold cannot connect to the network. The value range is 1 to 30 dB. A higher threshold may cause difficulties in client access. Configure this parameter according to the actual situation.
     - **Client Reconnection Threshold**: For an online client, when the signal strength drops below the threshold, the client is kicked offline and attempts to reconnect. The value range is 0 to 29 dB. Note that the client reconnection threshold must be lower than the weak-signal RSSI threshold.
7. Select whether to enable the WiFi6 2.4GHz or 5GHz radio and click **Apply**.
8. Set the signal strength thresholds for a client to initiate roaming, and click **Apply**. Increase the roaming sensitivity in dense deployment scenarios, and decrease the roaming sensitivity in other scenarios.
9. Click **Apply**.

Configure Wi-Fi settings

About this feature

This feature displays the Wi-Fi configuration of the device. An AP can provide wireless services only after a wireless service is bound to it.

Restrictions and guidelines

AP binding or unbinding operations might cause a brief disconnection for some clients connected to the AP. As a best practice, perform the binding or unbinding operation when the AP usage is low.

Procedure

1. From the left navigation tree, select **APs** > **Wi-Fi Settings**.
2. Click **Bind** for the corresponding the SSID in the list.
3. Select the APs to be bound in the AP list.
4. Click **Apply** to bind the SSID and the selected APs.
5. To edit a Wi-Fi configuration, click the **Edit** icon in the **Actions** column for the target SSID in the SSID list.
6. Edit the SSID.
7. Select whether to enable the wireless service.
8. Select the encryption algorithm. Options include:
   - **No Encryption**: Do not encrypt wireless signals.
   - **Encrypted**: Encrypt wireless signals.
9. Enter the shared key. The key is required when wireless users access the network. The shared key is required if you select to encrypt the wireless signals. The key is a case-sensitive string of 8 to 63 characters. Only letters, digits, and special characters ~!@#$%^&*()_+-={}|[]:<>,./ are supported.
10. Enter the AP management VLAN. By default, the AP management VLAN ID is 1.
11. Select the bands for the SSID.

    You can configure the AP to use this SSID to provide only 2.4G services, 5G services, or both.
12. Select whether to enable user rate limit. With this feature enabled, you can set the maximum uplink traffic and maximum downlink traffic.
    - **Uplink**—Rate limit traffic from clients to the device.
    - **Downlink**—Rate limit traffic from the device to clients.
13. Select whether to hide the SSID.
14. Click **Apply**.

Manage online APs

About this feature

You can view the online AP devices and clients through the online AP management function. This function displays detailed information about APs.

View the AP list

1. From the left navigation pane, select **APs** > **Online APs**.
2. To edit an AP, click the **Edit** icon for the target AP in the **Actions** column. You can modify the following settings as needed.
   - AP name.
   - AP service VLAN.
   - Wireless service enabling state.
   - Working channel.
   - Transmit power.
   - Bandwidth in MHz.
   - Roaming sensitivity.
   - Click **Apply**.
3. To delete APs, select the target APs and then click **Delete**.
4. To collect logs and configuration of APs, select the target APs and then click **Collect Logs&Config**.
5. To restart APs, select the target online APs and then click **Restart**.
6. To reset APs, select the target online APs and then click **Reset**. The APs will come online with the factory default settings and use the default wireless service template.

   If you only click **Reset** without deleting the AP records, you cannot restore the AP to factory settings.
7. You can set the number of AP entries displayed per page as needed.

View the client list

1. From the left navigation pane, select **APs** > **Online APs**.
2. Click the **Client List** tab to view the client list.

Manage AP versions

About this feature

The AP version management feature can help you upgrade the software version of APs.

Restrictions and guidelines

Before using the AP version upgrade function, upload the software version required for AP upgrade to the device.

Procedure

1. From the left navigation pane, select **APs** > **Version**.
2. Click **Upload Version**.
   - Click **Upload File**, browse to the AP image file, and select the file.
   - The version number is automatically detected and displayed on the page. Manual input is not required.

- Enter the description information of the version.
- Select the corresponding AP models.
- Click **Apply**.

3. Select the target AP models, and then click **Update Version** to deploy the images and upgrade the APs.

Configure network settings

Configure external network settings

About this feature

Typically, an external network refers to a wide area network (WAN). A WAN is a data communication network covering a large physical range. The Internet is an extremely large WAN.

Typically, a device has multiple WAN interfaces. You can configure the WAN interfaces to enable the device to access the external network.

Configure the interface mode

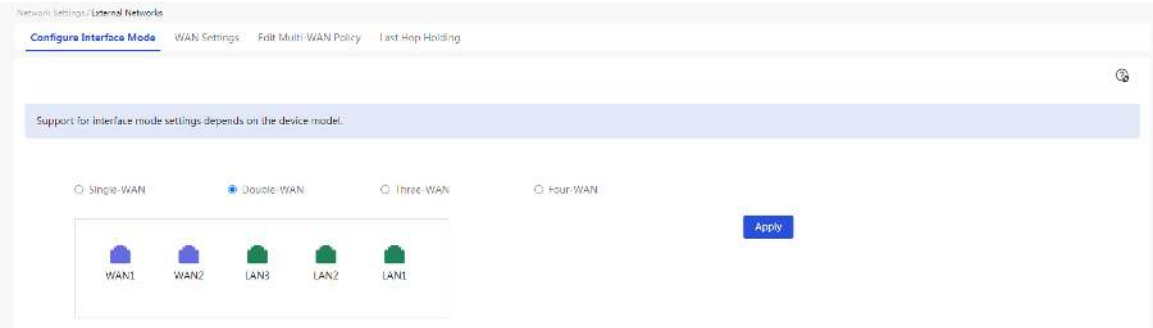
About this task

Perform this task to configure the number of access WAN interfaces on the device.

- Typically, after a LAN interface is changed to a WAN interface, the connection mode of the interface is DHCP. The VLAN configuration of a LAN interface is lost after the interface is changed to a WAN interface.
- Typically, the mirroring configuration of a LAN interface is cleared after the interface is changed to a WAN interface. To use the port mirroring feature after the change, configure port mirroring again.

Procedure

1. From the left navigation pane, select **Network Settings** > **External Networks**.
2. Click the **Configure Interface Mode** tab, and then select an option as required to configure the number of WAN interfaces supported by the device. Support for the number of WAN interfaces (or interface mode) varies by device model.
3. Click **Apply**.



Configure WAN settings

1. From the left navigation pane, select **Network Settings** > **External Networks**.
2. Click the **WAN Settings** tab.
3. In the line list, click the **Edit** icon in the **Actions** column for a line.
4. From the **Connection mode** list, select a connection mode as required.
   - If you select the PPPoE connection mode, perform the following tasks:

- In the **User ID** field, enter the PPPoE access username provided by the service provider.
- In the **User Password** field, enter the PPPoE access password provided by the service provider.
- In the **LCP active detection** field, select whether to detect the PPPoE link state anomalies. To enable this feature, select **Yes**. The link state is detected every 20 seconds. To disable this feature, select **No**. The link state is detected every 2 minutes.
- Select **Always Online** for the **Online Mode** field.

- If you select the DHCP connection mode, the DHCP server automatically assigns the public IP addresses for accessing the external network.
- If you select the fixed IP connection mode, perform the following tasks:
  - In the **IP Address** field, enter the fixed IP address for accessing the WAN. You can enter only a class A, B, or C IP address.
  - In the **Subnet Mask** field, enter the mask or mask length for the IP address, for example, 255.255.255.0 or 24.
  - In the **Gateway Address** field, enter the gateway address for accessing the WAN. You can enter only a class A, B, or C IP address.
  - In the **DNS1** and **DNS2** fields, enter the IP addresses of DNS servers for accessing the WAN. The device preferentially uses DNS server **DNS1** for domain name resolution. If DNS server **DNS1** fails to resolve a domain name, DNS server **DNS2** is used.

5. In the **MAC Address** field, select **Factory Default MAC address (F0-10-90-25-CD-5D)** or **Static MAC** as required. If you access the external network through a public IP address allocated by the service provider, you must configure a static MAC address.
6. In the **Uplink Network Bandwidth** and **Downlink Network Bandwidth** fields, enter the bandwidths provided by the service provider.
7. In the **Dial Mode** field, select a dial mode of the PPPoE connection. Options include:
   - **Auto**—In this mode, automatic dialup will be performed after you complete the configuration and click **Apply**.
   - **Manual**—In this mode, you must click **Dial** in the lower part of the dialog box to perform dialup after you complete the configuration.

   This field is available only when you select the PPPoE connection mode.
8. In the **Host-Uniq** field, select whether to carry the **Host-Uniq** field in the discovery packets of a PPPoE client.
   - **Carry Host-Uniq Field**—Configure the discovery packets of a PPPoE client to carry the **Host-Uniq** field.
   - **Not Carry Host-Uniq Field**—Configure the discovery packets of a PPPoE client not to carry the **Host-Uniq** field.

   When the connection mode is PPPoE, the device acts as a PPPoE client to send discovery packets to the PPPoE server. You can configure the discovery packets to carry the **Host-Uniq** field to uniquely identify the PPPoE client of discovery packets. When the PPPoE server receives a discovery packet with the **Host-Uniq** field, it must include this field unmodified in the response packet.

   This field is available only when you select the PPPoE connection mode. In some scenarios, the PPPoE server will require the **Host-Uniq** field in the discovery packets of PPPoE clients. Therefore, select the **Carry Host-Uniq Field** option as a best practice.
9. In the **Server Name** field, enter the name of the PPPoE server. This field is available only when you select the PPPoE connection mode.
10. In the **Service Name** field, enter the service name of the PPPoE server. This field is available only when you select the PPPoE connection mode.

11. In the **Host name** field, enter the host name that will be advertised to the DHCP server. This field is available only when you select the DHCP connection mode.
12. In the **NAT** field, select whether to enable NAT. Enable NAT when multiple devices in the LAN share one public IP address. If you select **On**, select **Address Pool Translation** as required. If you select **Address Pool Translation**, select an existing NAT address pool or add one. The existing NAT address pools are added on the **Network Settings** > **NAT** > **Address Pool** page.
13. In the **TCP MSS** field, configure the maximum segment size (MSS) of TCP packets for the interface. The default MSS is 1280 bytes.
14. In the **MTU** field, enter the (maximum transmission unit) MTU for the interface.
15. Options for the **Link Detection** field include **Off**, **ICMP Detection**, **DNS Detection**, and **NTP Detection**. When you select **ICMP Detection**, **DNS Detection**, or **NTP Detection**, perform the following tasks:
    - In the **Detected Address** field, enter an IP address for link detection. If you select **DNS Detection**, you can also enter a domain name.
    - In the **Detection Interval** field, enter the interval for link detection.
    - In the **Detection Times** field, enter the number of link detections.

    After you enable link detection, you can judge the state of the link to the specified IP address to improve the link availability.
16. In the **Dedicated Line** field, select whether to set the current line as a dedicated line. Typically, a dedicated line (such as a medical or public security dedicated line) cannot access the external network.
    - **Yes**—Set the current line as a dedicated line. If you select this option, you must configure static routes for the line.
    - **No**—Do not set the current line as a dedicated line.
17. Click **Apply**.

Edit WAN Settings

WAN Interface	WAN1
Connection Mode	PPPoE
User ID	test
User Password	••••••
LCP active detection	Yes
Online Mode	Always Online
DNS1	114 . 114 . 114 . 114
DNS2	223 . 5 . 5 . 5
MAC Address	Factory Default MAC (00-19-10-28-00-80)
	Static MAC
	HH - HH - HH - HH - HH - HH
Uplink Network Bandwidth	(Mbps)
Downlink Network Bandwidth	(Mbps)
Dial Mode	Auto
Host-Uniq	Carry Host-Uniq Field
Server Name	(1-31 characters)
Service Name	(1-31 characters)
NAT	On
	Address Pool Translation — Select...
TCP MSS	1280
MTU	1492 (576-1492 bytes)
Link Detection	Off
Detected Address	
Detection Interval	(1-10 sec)
Detection Times	(1-30,The default value is 3.)
Dedicated Line	No

Cancel Apply

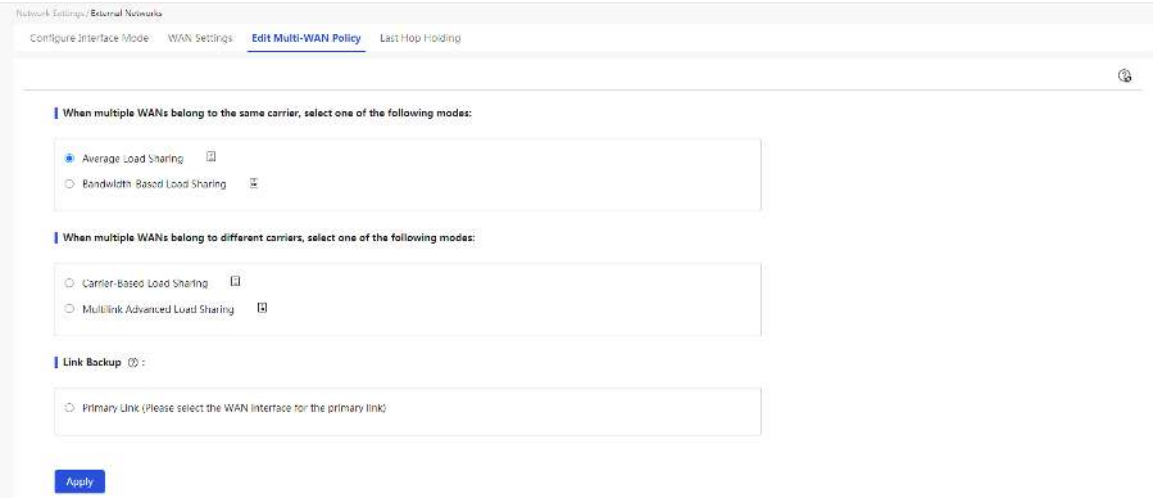
Edit a multi-WAN policy

Restrictions and guidelines

You can configure settings on this page only in the multi-WAN scenario.

Procedure

1. From the left navigation pane, select **Network Settings** > **External Networks**.
2. Click the **Edit Multi-WAN Policy** tab.
3. According to actual applications, edit the multi-WAN policy as follows:
   - If multiple WANs belong to the same service provider, as a best practice, select **Average Load Sharing** or **Bandwidth-Based Load Sharing**. If multiple WAN links have the same bandwidth, as a best practice, select **Average load sharing**. In other situations, select **Bandwidth-Based Load Sharing** and set the link bandwidth ratio. If you configure the double-WAN interface mode for the device and set the bandwidth ratio for WAN1 and WAN2 to 0:1, traffic is only forwarded by WAN2.
   - If multiple WANs belong to different service providers, as a best practice, select **Carrier-based load sharing** or **Multilink advanced load sharing**. If links provided by each service provider have the same bandwidth, as a best practice, select **Carrier-Based Load Sharing**. In other situations, select **Multilink Advanced Load Sharing** and set the link bandwidth ratio.
   - To ensure network stability, you can perform link backup. Select **Primary Link (Please select the WAN interface for the primary link)** and the corresponding link *n*, and then select link *m* for the secondary link. To implement link backup, make sure *n* and *m* are different. If the selected primary link has link detection enabled on the **External Networks** > **WAN Settings** page, the system will change the actual primary link that takes effect according to the link detection result. If the selected primary link does not have link detection enabled, the system will change the actual primary link that takes effect according to the physical state of the corresponding interface.
4. Click **Apply**.



Configure last hop holding

1. From the left navigation pane, select **Network Settings** > **External Networks**.
2. Click the **Last Hop Holding** tab.

3. Select **Enable Last Hop Holding** or **Disable Last Hop Holding** as required. In the multi-WAN scenario, to make sure packets entering the LAN and packets leaving the LAN are forwarded through the same WAN interface, enable the last hop holding feature.

Configure LAN settings

About this feature

Use this feature to assign LAN interfaces of the device to VLANs, configure VLAN interface parameters, enable Dynamic Host Configuration Protocol (DHCP), and configure DHCP parameters.

DHCP is a LAN protocol mainly used for assigning IP addresses to hosts on a LAN. DHCP supports the following allocation mechanisms:

- **Dynamic allocation**—Configure this feature on an interface. This feature dynamically assigns IP addresses to hosts. When the lease of an IP address expires or an IP address is explicitly rejected by a host, the IP address can be used by another host. This allocation mechanism applies to a network scenario where you need to assign an IP address to a host for a limited period of time.
- **Static allocation**—Statically assigned IP addresses are not bound to clients' interfaces, and they are bound to the host NIC MAC addresses. A static IP address can be used permanently. This allocation mechanism applies to a network scenario where you need to assign an IP address to a host permanently.

Configure VLANs

About this task

Assign the LAN interfaces on the device to the specified VLAN, so that hosts in the same VLAN can communicate and hosts in different VLANs cannot directly communicate.

Restrictions and guidelines

When you configure a VLAN as the PVID for an interface on the detailed port settings page, make sure the VLAN has already been created.

NOTE:

The PVID identifies the default VLAN of a port. Untagged packets received on a port are considered as the packets from the port PVID.

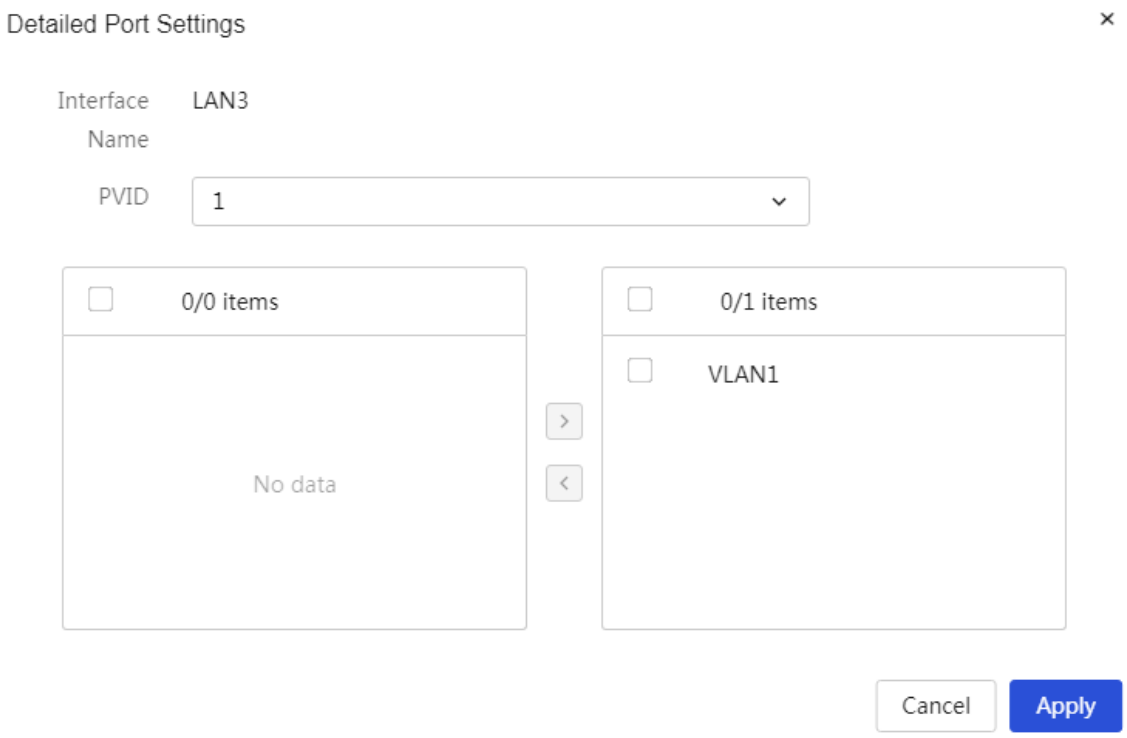
Prerequisites

Plan the VLANs to which each LAN interface belongs on the device, and create the corresponding VLAN interface on the LAN settings page.

Procedure

1. From the left navigation pane, select **Network Settings** > **LANs**.

2. Click the **VLAN Division** tab.
3. In the port list, click the **Edit** icon in the **Actions** column for a port. The **Detailed Port Settings** page opens.
4. From the **PVID** list, select a PVID as required.
5. To assign a port to or remove a port from VLANs:
   - Select VLAN IDs from the available VLAN list or click the available VLAN list checkbox to select all VLANs. Then, click the right arrow button to add the port to the selected VLANs.
   - Select VLAN IDs from the selected VLAN list or click the selected VLAN list checkbox to select all VLANs. Then, click the left arrow button to remove the port from the selected VLANs.
6. Click **Apply**.



Configure LAN interface settings

About this task

Create a VLAN interface for the device to connect to the intranet, and use the VLAN interface as the gateway for the intranet device to provide DHCP service.

Restrictions and guidelines

If you enable DHCP service for a VLAN interface and then disable it, the system will delete the static DHCP bindings of this VLAN interface on the **Static DHCP** page at the same time.

Procedure

1. From the left navigation pane, select **Network Settings** > **LANs**.
2. Click the **VLAN Settings** tab.
3. The interface list displays all created VLAN interfaces.

   To edit a VLAN interface, click the **Edit** icon in the **Actions** column for that VLAN interface.

   To delete a single VLAN interface, click the **Delete** icon in the **Actions** column for that VLAN interface. To delete one or multiple VLAN interfaces in bulk, select the VLAN interfaces and then click **Delete**.
4. To add a VLAN interface, click **Add**.
5. In the **VLAN ID** field, enter the ID of the VLAN interface.
6. In the **Interface IP Address** field, enter the IP address of the VLAN interface.
7. In the **Subnet Mask** field, enter the mask or mask length for the IP address, for example, 255.255.255.0 or 24.
8. In the **TCP MSS** field, configure the MSS of TCP packets for the interface. The default MSS is 1280 bytes.
9. In the **MTU** field, enter the MTU for the interface.
10. To enable DHCP, select **Enable DHCP**. Then, the device dynamically assigns IP addresses to clients (such as PCs) connected to the device. Configure the following parameters as required:
    - Select **ARP Protection (Dynamic ARP Binding) for DHCP-Assigned Addresses** to bind each client's MAC address to the dynamically assigned IP address.
    - In the **Start IP Address** and **End IP Address** fields, specify a range of IP addresses that can be assigned to clients.
    - In the **Excluded IP Addresses** field, specify the IP addresses that cannot be assigned to clients. If some IP addresses in the address range (for example, the gateway address) cannot be assigned to clients, specify these addresses as excluded IP addresses.
    - In the **Client Domain Name** field, enter the domain name suffix assigned to a client by the device.
    - In the **Gateway Address**, **DNS1**, and **DNS2** fields, enter the IP addresses of the gateway, primary DNS server, and secondary DNS server, respectively.
    - In the **Address Lease** field, enter the lease (in minutes) of IP addresses to be assigned. For example, to specify the lease of IP addresses as five days, enter 7200.
11. Click **Apply**.

Configure static DHCP

About this task

To assign fixed IP addresses to some clients, configure static DHCP to bind client MAC addresses to IP addresses.

Restrictions and guidelines

- Make sure statically bound client IP addresses are not contained in the WAN interface IP address range specified on the device.
- If the IP address assigned to a client is already in use by another endpoint on the network, the endpoint providing the MAC address of the client will be assigned a different IP address when it connects to the network. Once the previously assigned IP address is released, the DHCP server will allocate that IP address to the endpoint providing the MAC address of the client.

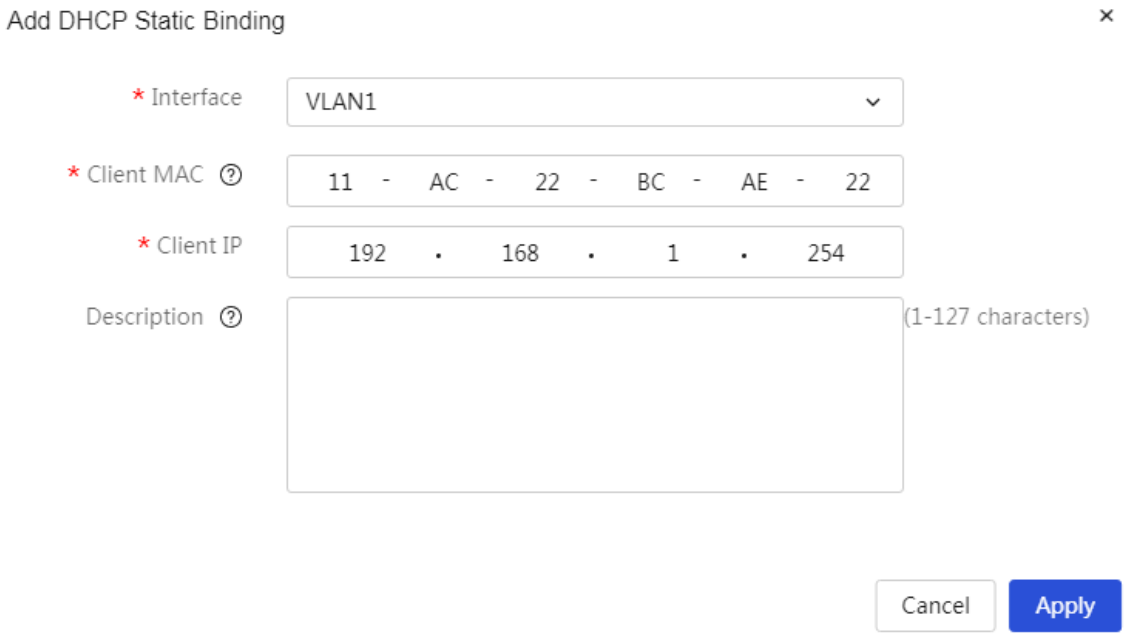
Prerequisites

Before configuring static DHCP, first enable the DHCP service on the target VLAN interface.

Procedure

1. From the left navigation pane, select **Network Settings** > **LANs**.
2. Click the **Static DHCP** tab.
3. Click **Add**. The **Add DHCP Static Binding** dialog box opens.
4. From the **Interface** list, select a DHCP-enabled interface.

5. In the **Client MAC** field, enter a client MAC address. For example, you can obtain the MAC address of a PC from its NIC.
6. In the **Client IP** field, enter the IP address assigned to the client.
7. Click **Apply**.



Reclaim DHCP-assigned IP addresses

1. From the left navigation pane, select **Network Settings** > **LANs**.
2. Click the **DHCP Allocation List** tab.
3. Select the IP addresses to be reclaimed in the list.
4. Click **One-Key Reclamation** and click **Yes** in the dialog box that opens.

Configure static bindings for DHCP-assigned IP addresses

1. From the left navigation pane, select **Network Settings** > **LANs**.
2. Click the **DHCP Allocation List** tab.
3. Select the IP addresses to be configured with static bindings.
4. Click **Static Allocation** and click **Yes** in the dialog box that opens.

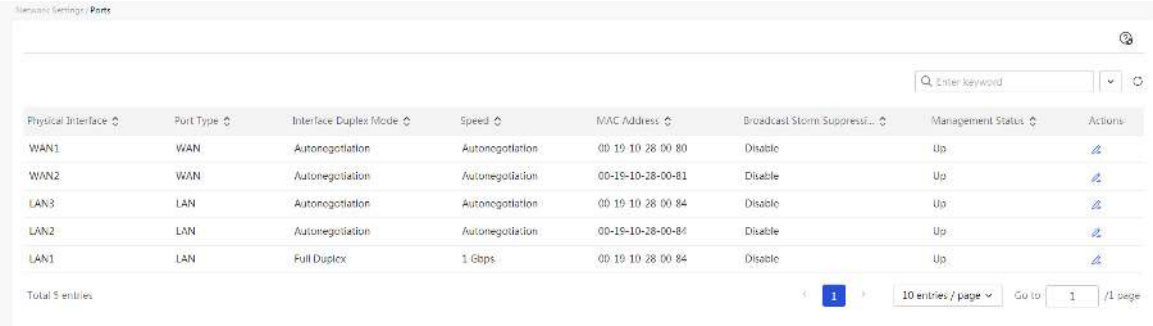
Manage ports

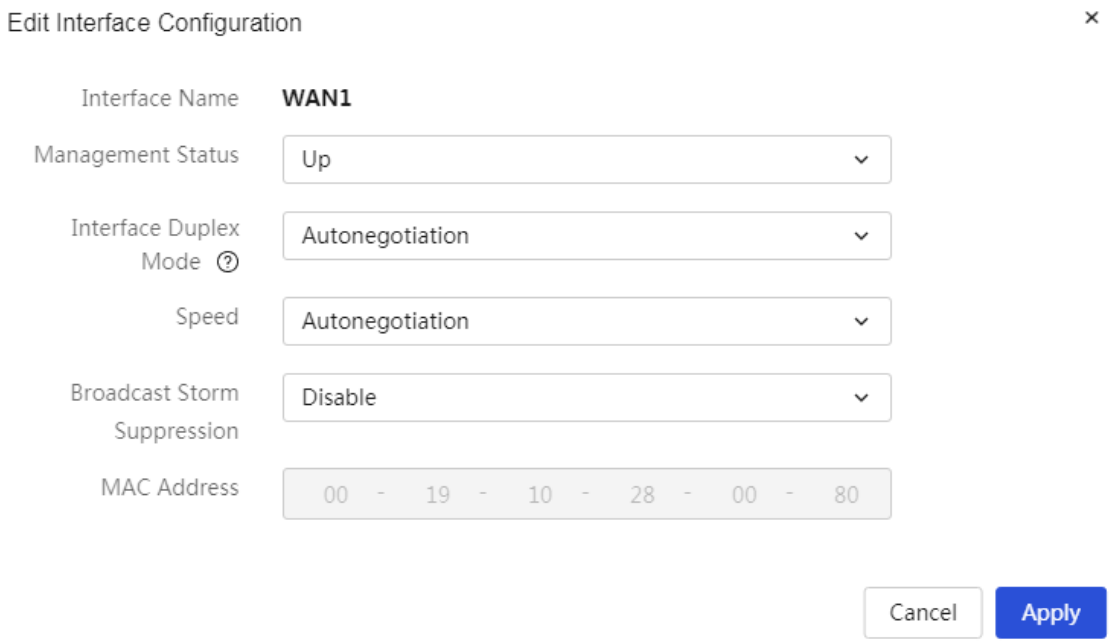
About this feature

Use the port management function to view the interface type, interface duplex mode, speed, MAC address, and broadcast storm suppression information of each physical interface on the device, set the management status of the WAN interfaces, and edit interface configuration.

Procedure

1. From the left navigation pane, select **Network Settings** > **Ports**.
2. In the physical interface list, click the **Edit** icon in the **Actions** column for an interface.
3. From the **Management Status** list, select **Up** or **Down** to enable or disable the interface, respectively.
4. From the **Interface Duplex Mode** list, select a duplex mode.
5. From the **Speed** list, select a speed.
6. From the **Broadcast Storm Suppression** list, select a suppression level or disable this feature. Suppression levels include **Low**, **Medium**, and **High**. The number of broadcast packets permitted to pass increases sequentially for the three levels.
7. In the **MAC Address** field, view the MAC address of the interface.
8. Click **Apply**.





Configure NAT

About this feature

Network Address Translation (NAT) translates an IP in the IP packet header to another IP address. It enables private hosts to access external networks and external hosts to access private network resources.

NAT supports the following address translation methods:

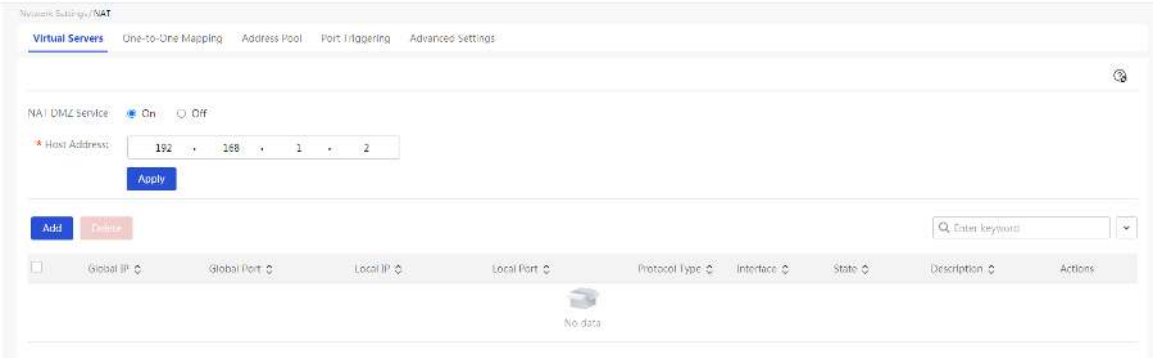
- **Port mapping**—Allows multiple internal servers (for example, Web, mail, and FTP servers) to provide services for external hosts by using one public IP address and different port numbers. This method saves public IP address resources.
- **One-to-one mapping**—Creates a fixed mapping between a private address and a public address. Use this method for fixed network access requirements. This method is preferred if you need to use a fixed public IP address to access an internal server.
- **Port triggering**—For some applications (for example, IP telephones or video conferences), when a client in the LAN accesses a server on the Internet, the server must initiate a connection request to the client. By default, the device denies all connection requests initiated from the WAN side and communication is interrupted. By configuring a port triggering rule, the device automatically opens the port requested by the server to ensure communication when the client accesses the server and the access triggers the rule. If the client and device have not communicated with each other for a long time, the device automatically closes the port to ensure correct operation of the applications and LAN security.

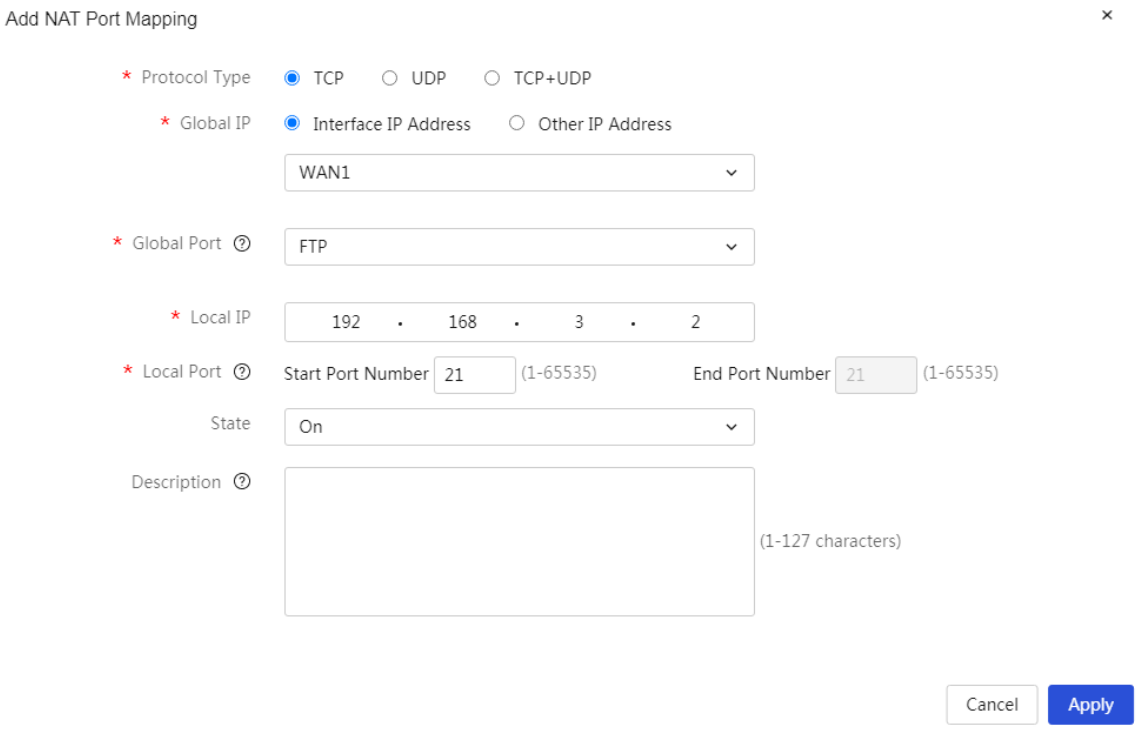
NAT provides the following advanced features:

- **NAT hairpin**—Allows internal users to access internal servers through NAT addresses. This feature is applicable if you want the gateway to control the internal user traffic destined for the internal server that provides services for external users through a public IP address.
- **NAT ALG**—If an application layer service (for example, FTP or RTSP) exists between the internal and external networks, enable NAT ALG for the application layer protocol. It ensures that the data connection of this protocol can be correctly established after address translation.

Configure a virtual server

1. From the left navigation pane, select **Network Settings** > **NAT**.
2. Click the **Virtual Servers** tab.
3. Select **On** for the **NAT DMZ Service** field.
4. In the **Host Address** field, enter the IP address of the DMZ host.
5. Click **Apply**.
6. Click **Add**. The **Add NAT Port Mapping** dialog box opens.
7. Select **TCP**, **UDP** or **TCP+UDP** for the **Protocol Type** field. Select a protocol based on the transport layer protocol used by the internal server. For example, select **TCP** for an FTP server and **UDP** for a TFTP server.
8. Select **Interface IP Address** or **Other IP Address** for the **Global IP** field as required.
9. From the **Global Port** list, select **FTP**, **TELNET**, or **User-Defined Ports**. If the host does not provide the FTP or Telnet service, enter the port number used by the provided service. For example, configure port 8080 if the host provides the HTTP service.
10. In the **Local IP** field, enter the private IP address that can be accessed by the external network.
11. In the **Local Port** field, enter the port number used by private network resources.
12. From the **State** list, select whether to enable the mapping.
13. Click **Apply**.





Configure one-to-one mappings

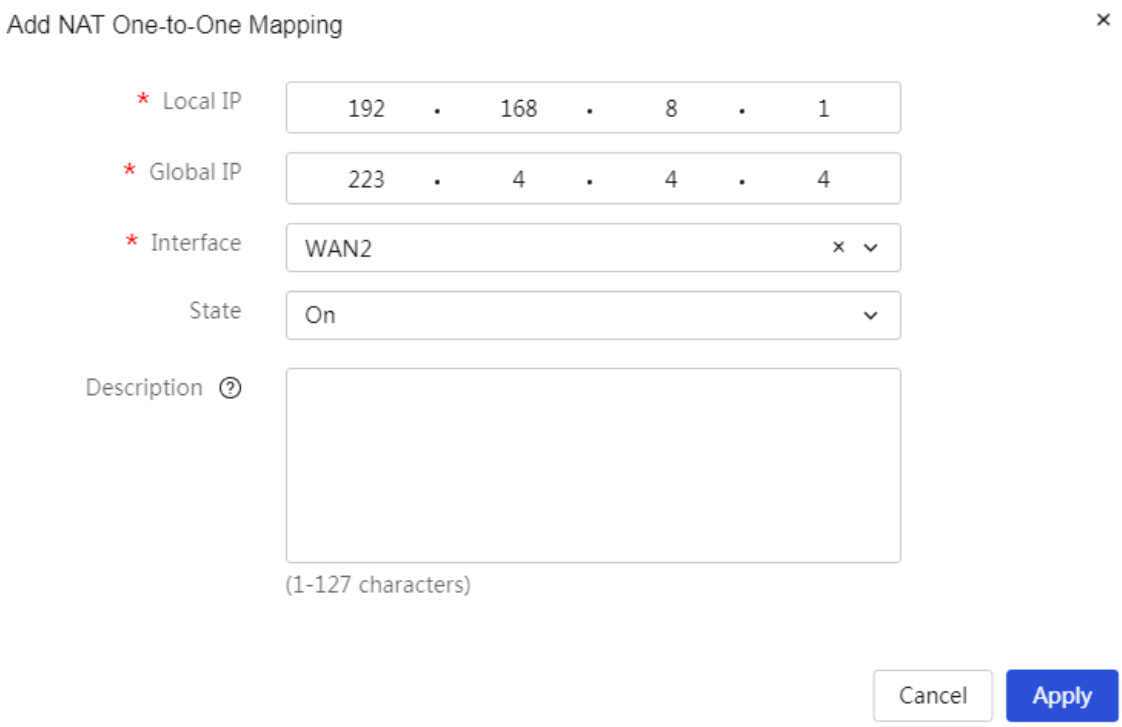
Restrictions and guidelines

If the device has only one public address, do not configure a one-to-one mapping by using the public address.

Procedure

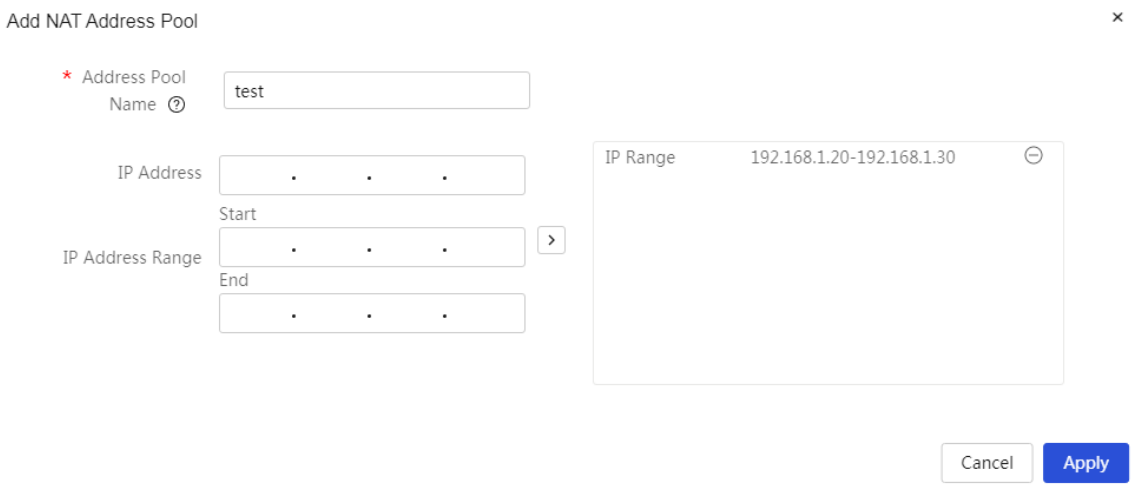
1. From the left navigation pane, select **Network Settings** > **NAT**.
2. Click the **One-to-One Mapping** tab.
3. Select **Enable** for the **One-to-One Mapping** field.
4. Click **Add**. The **Add NAT One-to-One Mapping** dialog box opens.
5. In the **Local IP** field, enter a private IP address.
6. In the **Global IP** field, enter an available public address.
7. From the **Interface** list, select an interface to which the mapping is applied. If you do not specify any interface, the mapping applies to all WAN interfaces.
8. From the **State** list, select whether to enable the mapping.

9. Click **Apply**.



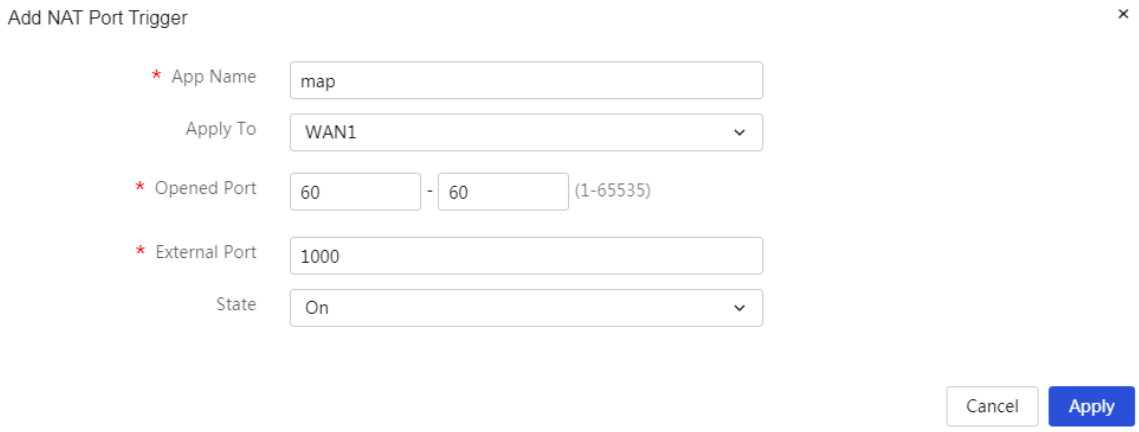
Configure address pools

1. From the left navigation pane, select **Network Settings** > **NAT**.
2. Click the **Address Pool** tab.
3. Click **Add**. The **Add NAT Address Pool** dialog box opens.
4. In the **Address Pool Name** field, enter the name of a public IP address pool used for NAT. The name can contain Chinese characters, digits, letters, and underscores (_).
5. In the **IP Address** field, enter an IP address.
6. In the **Start** field, enter the start IP address of an address range.
7. In the **End** field, enter the end IP address of the address range. An address range can contain a maximum of 256 IP addresses and make sure all the IP addresses in the address range are valid.
8. To submit the configured IP address or IP address range, click **>**.
9. Repeat steps 5 to 8 to add multiple addresses or address ranges to the address pool.
10. Click **Apply**.



Configure port triggering

1. From the left navigation pane, select **Network Settings** > **NAT**.
2. Click the **Port Triggering** tab.
3. Click **Add**. The **Add NAT Port Trigger** dialog box opens.
4. In the **App Name** field, enter the name of a port trigger.
5. From the **Apply To** list, select an interface to receive packets.
6. In the **Opened Port** field, specify a port range used by the clients in the LAN to initiate requests to the external server.
7. In the **External Port** field, enter the port requested by the external server from the clients in the LAN. You can specify a single port, a port range, or a combination of both. Separate the ports or port ranges by commas (,), for example, 100,200-300,400. You can specify a maximum of 10 ports or port ranges.
8. From the **State** list, select whether to enable the port triggering feature.
9. Click **Apply**.



Configure NAT hairpin

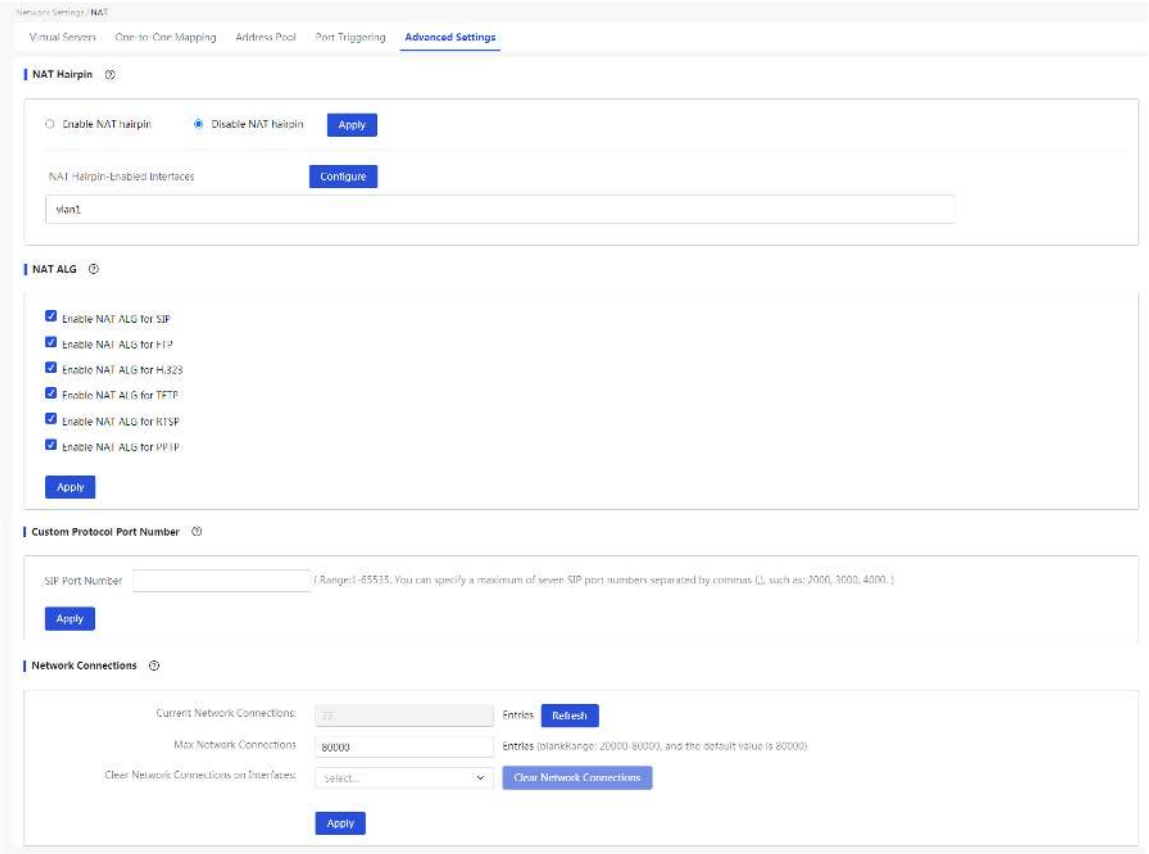
Prerequisites

Before you configure NAT hairpin, perform more than one of the following tasks:

- Configure a mapping between the internal server IP address and port and the public IP address and port on the virtual server configuration page.
- Configure a mapping between the private user IP address and public IP address on the one-to-one mapping configuration page.

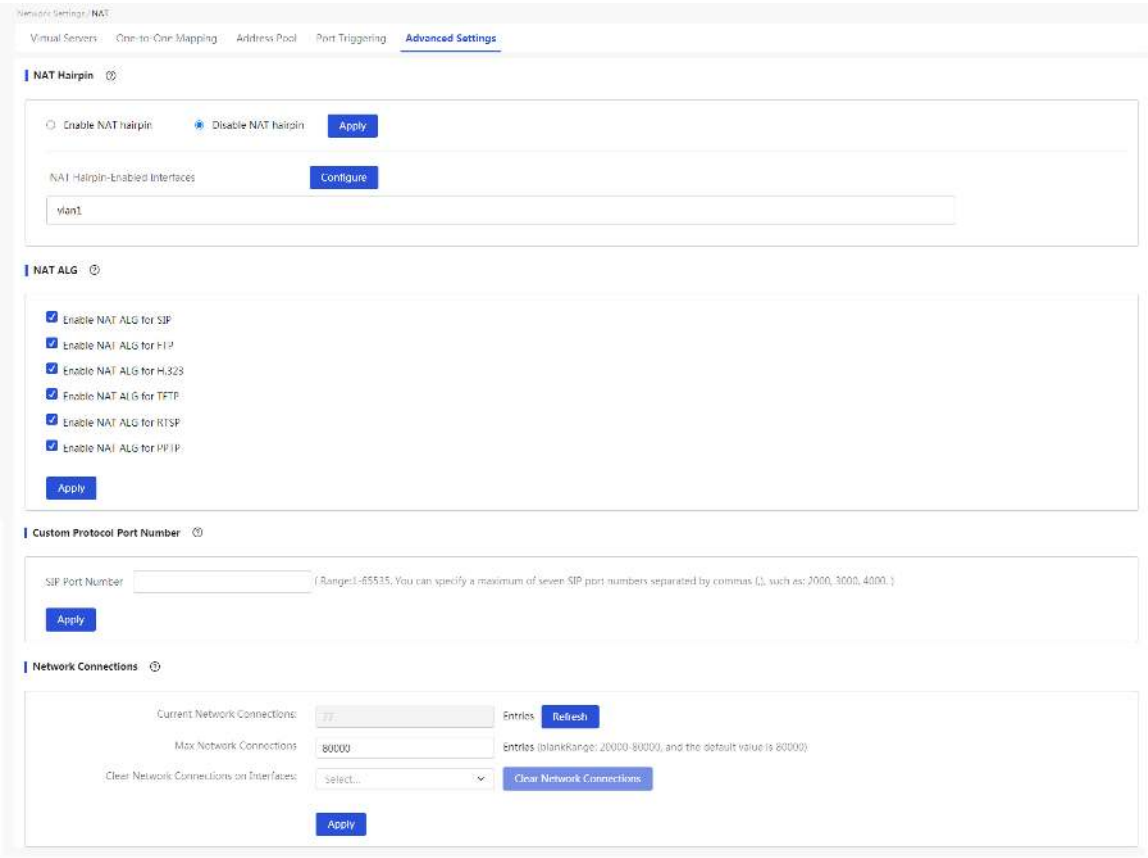
Procedure

1. From the left navigation pane, select **Network Settings** > **NAT**.
2. Configure a NAT server mapping or one-to-one mapping.
3. Click the **Advanced Settings** tab.
4. In the **NAT Hairpin** area, select **Enable NAT hairpin**.
5. Click **Configure**. The **Configure NAT Hairpin for Interfaces** dialog box opens. Enable NAT hairpin for interfaces as required.
   - Select interfaces from the left box, click **>** to add the interfaces to the right box, and then click **Apply**. All interfaces in the right box are enabled with NAT hairpin.
   - Select interfaces from the right box, click **<** to remove the interfaces from the right box, and then click **Apply**. The interfaces removed from the right box are disabled with NAT hairpin.
6. Click **Apply**.



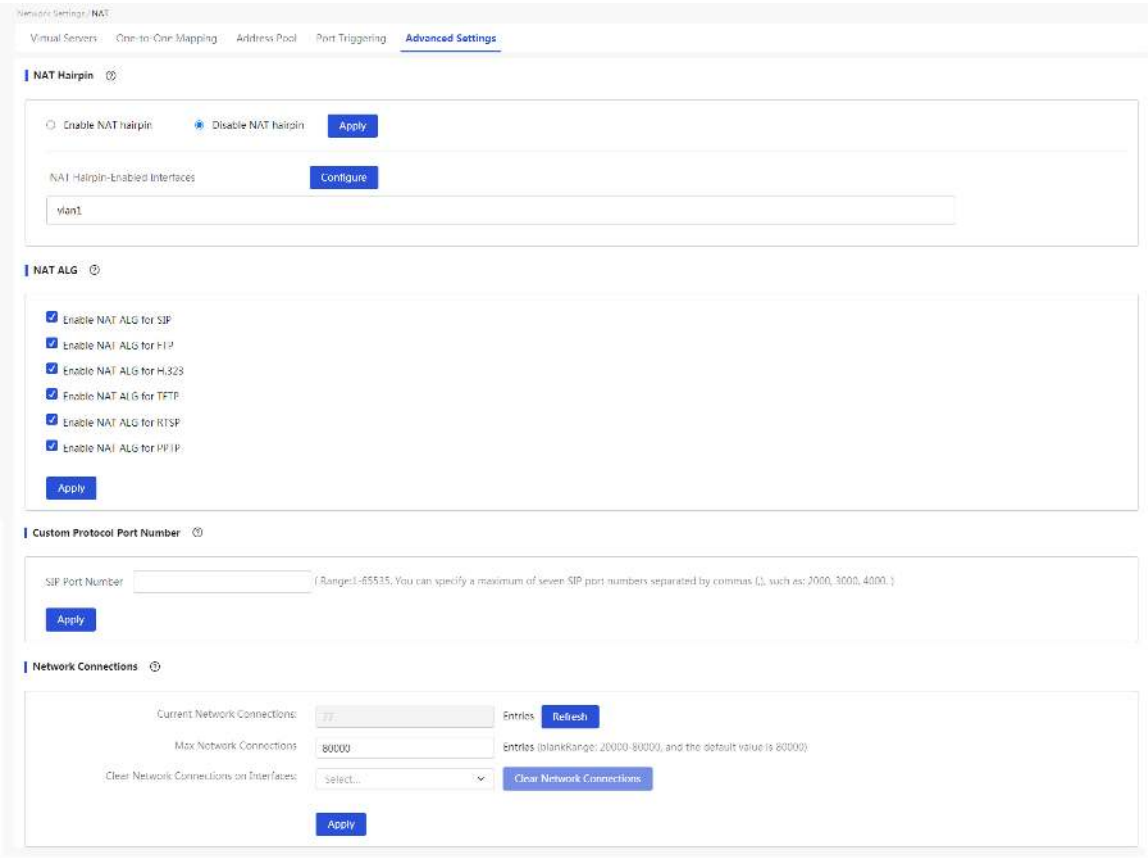
Configure NAT ALG

1. From the left navigation pane, select **Network Settings** > **NAT**.
2. Click the **Advanced Settings** tab.
3. In the **NAT ALG** area, enable NAT ALG for protocols as required.
4. Click **Apply**.



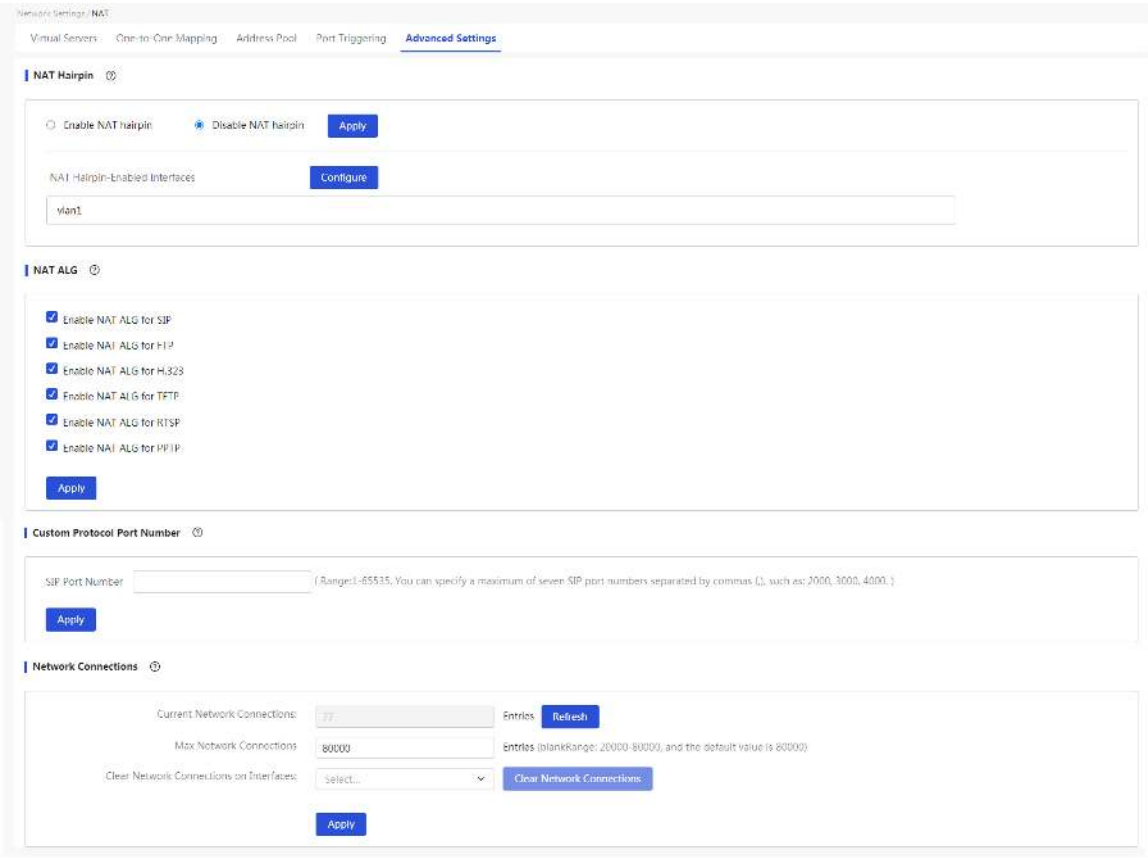
Configure user-defined protocol port numbers

1. From the left navigation pane, select **Network Settings** > **NAT**.
2. Click the **Advanced Settings** tab.
3. In the **Custom Protocol Port Number** area, specify a SIP port number as required. When you set up a SIP server, if the SIP port number in use is not 5060, specify a SIP port number.
4. Click **Apply**.



Configure network connections

1. From the left navigation pane, select **Network Settings** > **NAT**.
2. Click the **Advanced Settings** tab.
3. In the **Network Connection** area, configure the following parameters:
   - In the **Current Network Connections** field, you can view the current number of network connections. To refresh the number, click **Refresh**.
   - In the **Max Network Connections** field, enter the maximum number of network connections that can be created on the device. As a best practice, use the default value. The value range and default value for this field varies by device model. For more information, see the Web interface for the device.
   - From the **Clear Network Connections on Interfaces** list, select interfaces for which you want to clear network connections.
4. Click **Apply**.



Configure address groups

About this feature

An address group is a group of host names or IP addresses. An address group can contain multiple members, which can be IP addresses or IP address ranges. Address groups can be used by some features (for example, bandwidth management) to identify packets.

Restrictions and guidelines

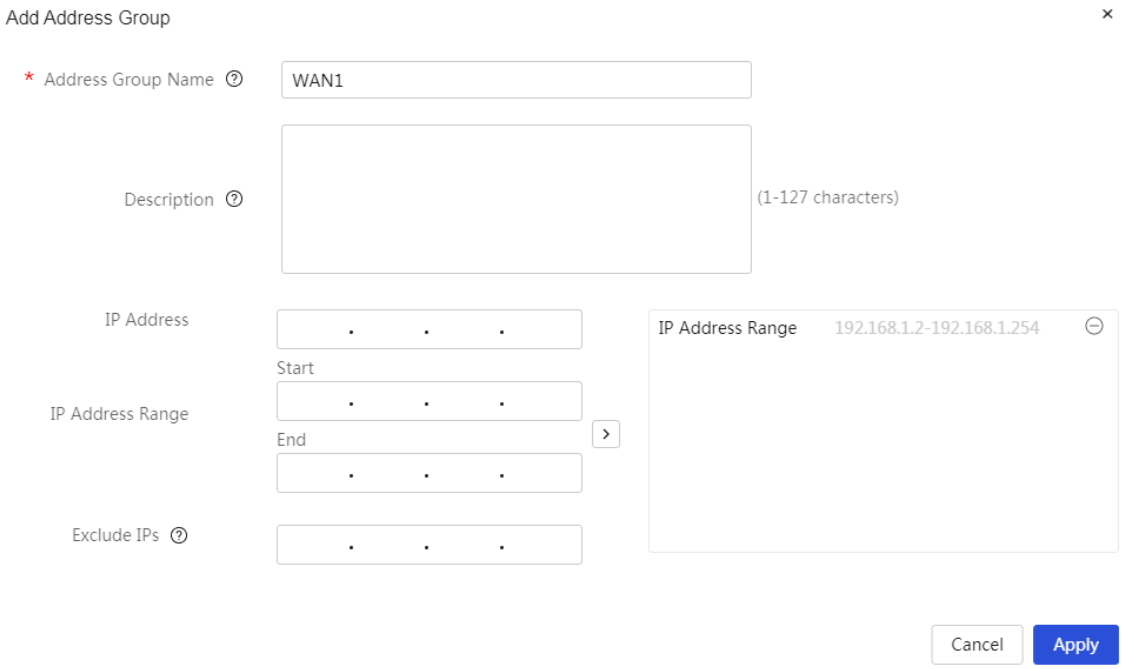
- An address group can contain only IPv4 addresses.
- The start address in an IP address range must be lower than the end address.
- An address range can contain a maximum of 256 IP addresses and make sure all the IP addresses in the address range are valid.

Procedure

1. From the left navigation pane, select **Network Settings** > **Address Groups**.
2. Click **Add**. The **Add Address Group** dialog box opens.
3. In the **Address Group Name** field, enter an address group name.
4. In the **Description** field, enter the description of the address group.
5. Configure the address group as follows:

- Specify an IP address to be added to the address group.
- Specify the start IP address and end IP address of an address range to be added to the address group.
- Specify IP addresses to be excluded from the address group.

6. To submit the configured IP address or address range, click **>**.
7. Repeat steps 5 and 6 to add multiple members of the same type.
8. Click **Apply**.



Configure PoE

Support for this feature varies by device model.

About this feature

Power over Ethernet (PoE) enables a device to supply power for powered devices (PDs) over twisted pair cables.

Configure PoE power supply

About this task

Enable PoE for PoE interfaces on the device.

Procedure

1. From the left navigation pane, select **Network Settings** > **PoE**.
2. Click the toggle button under a LAN interface to enable or disable PoE for that interface.

Configure time range groups

About this feature

If you want some features (for example, bandwidth management or network behavior management) to take effect only during the specified time period, you can create a time range group and reference it when configuring such features.

A time range group can contain one or more time ranges. Time ranges have the following types:

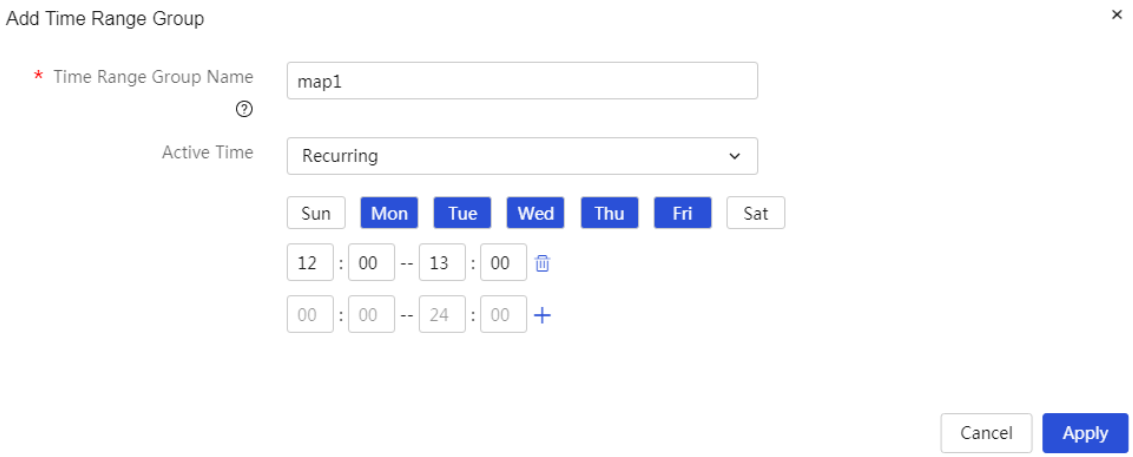
- **Recurring**: This type of time range begins and ends on a recurring basis. For example, 8:00 am to 12:00 am every Monday.
- **Non-recurring**: This type of time range begins on a specific date and ends on a specific date. For example, 8:00 am to 6:00 pm every day between January 1, 2015 and January 3, 2015.

Restrictions and guidelines

- You can create a maximum of 64 time range groups.
- A time range group can contain a maximum of 16 recurring time ranges and a maximum of 16 non-recurring time ranges.

Procedure

1. From the left navigation pane, select **Network Settings** > **Time Range Groups**.
2. Click **Add**. The **Add Time Range Group** dialog box opens.
3. In the **Time Range Group Name** field, enter a time range group name.
4. From the **Active Time** list, select **Recurring** or **Absolute** as required. Then, configure time ranges. Choose one of the following options as needed:
   - Select **Recurring** from the **Active Time** list. Select days of the week, enter the start time and end time, and then click the plus sign.
   - Select **Absolute** from the **Active Time** list. Select the start and end dates, enter the start time and end time, and then click the plus sign.
5. Click **Apply**.



Configure application groups

About this feature

If you want bandwidth management to take effect only on some applications, you can create multiple applications, add them to an application group, and reference the application group when configuring bandwidth management.

Configure user-defined applications

About this task

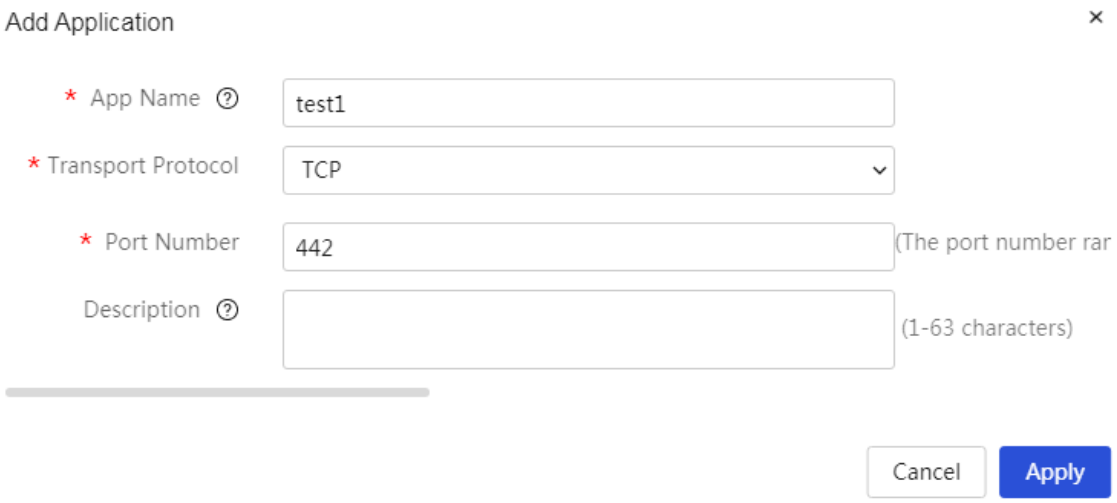
Perform this task to perform strict bandwidth management on specific application protocols and port numbers.

Restrictions and guidelines

After you create user-defined applications, add them to an application group, and reference the application group when configuring bandwidth management.

Procedure

1. From the left navigation pane, select **Network Settings** > **App Groups**. Click the **User-Defined Applications** tab.
2. Click **Add**. The **Add Application** dialog box opens.
3. In the **App Name** field, enter an application name.
4. From the **Transport Protocol** list, select **TCP**, **UDP**, or **TCP+UDP**.
5. In the **Port Number** field, enter the port number of the application.
6. In the **Description** field, enter the description of the application.
7. Click **Apply**.



Configure application groups

About this task

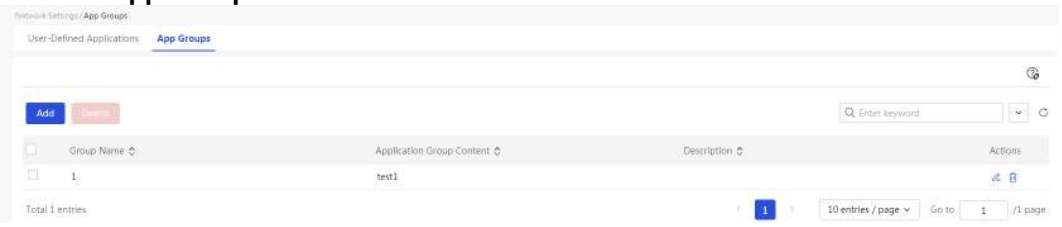
Perform this task to add user-defined applications to an application group for strict bandwidth management on all applications in the group.

Restrictions and guidelines

After you create an application group, you must reference the application group when configuring bandwidth management.

Procedure

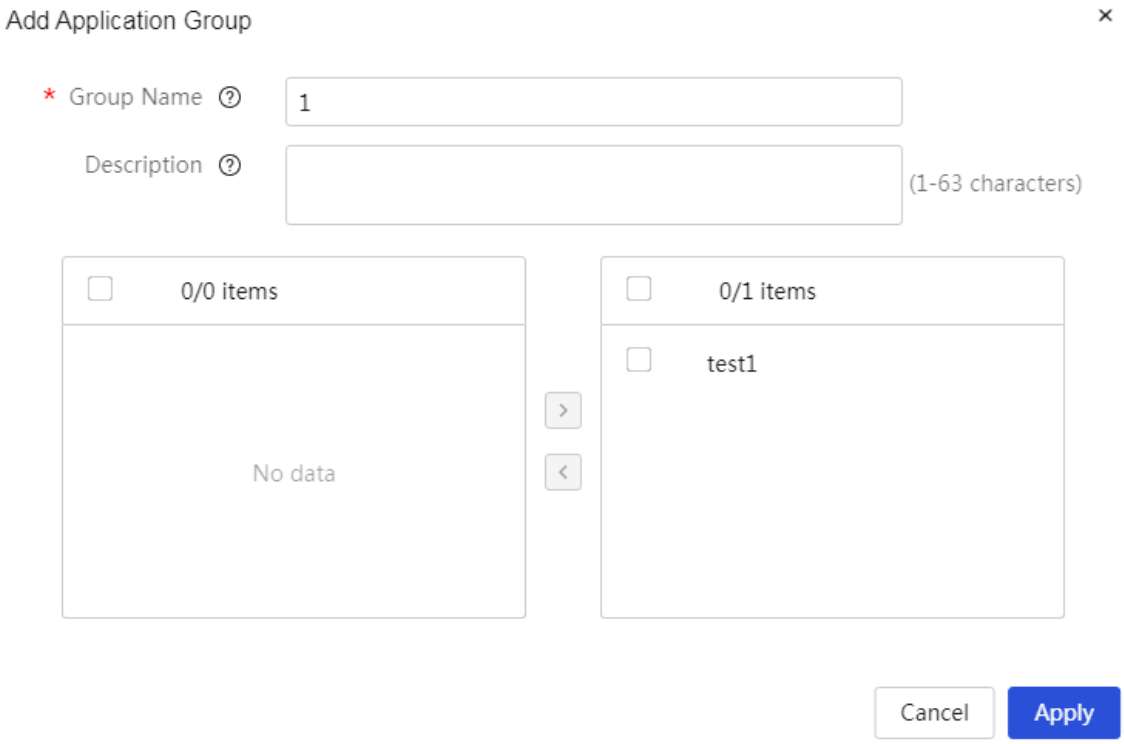
1. Click the **App Groups** tab.



2. Click **Add**. The **Add Application Group** dialog box opens.
3. In the **Group Name** field, enter an application group name.
4. In the **Description** field, enter the description of the application group.
5. Add applications to or remove applications from the application group as required.
   - To add applications to the application group, select applications from the left box, and then click **>**.

- To remove applications from the application group, select applications from the right box, and then click **<**.

6. Click **Apply**.



Configure network behavior management

Configure tasks at a glance

Limit the bandwidth of a WAN interface

To limit the bandwidth of a WAN interface, perform the following tasks:

Task	Remarks
(Optional.) Configure address groups	Add IP addresses to be rate limited to an address group.
(Optional.) Configure time range groups	Set the time period during which the bandwidth is limited.
(Required.) Configure rate limiting	Configure a rate limiting profile.

Limit the bandwidth for applications

To limit the bandwidth for applications, perform the following tasks:

Task	Remarks
(Required.) Configure user-defined network applications	Configure the custom applications to be rate limited.
(Required.) Configure application groups	Create an application group, and add the applications to be rate limited to the application group.
(Required.) Configure the restricted channel	Configure the restricted channel to limit the bandwidth for applications in an application group.

Guarantee the bandwidth for applications

To guarantee the bandwidth for applications, perform the following tasks:

Task	Remarks
(Required.) Configure user-defined network applications	Configure the custom applications to be guaranteed.
(Required.) Configure application groups	Create an application group, and add the applications to be guaranteed to the application group.
(Required.) Configure the green channel	Configure the green channel to guarantee the bandwidth for applications in an application group.

Limit the applications that can be used

To limit the applications that can be used, perform the following tasks:

Task	Remarks
(Optional.) Configure address groups	Add IP addresses to an address group.
(Optional.) Configure time range groups	Set the time period during which the applications are limited
(Required.) Configure application control	To limit common applications, you can specify them when configuring application control (see "Configure application control"). To limit uncommon applications, you must first define custom applications (see "Configure user-defined network applications").

Configure the URLs that can be visited through an allowlist

To configure the URLs that can be visited through an allowlist, perform the following tasks:

Task	Remarks
(Optional.) Configure address groups	Add IP addresses to an address group.
(Optional.) Configure time range groups	Set the time period during which URLs can be visited.
(Required.) Configure URL control	Enable URL allowlist mode, and add a custom URL category.

Configure the URLs that cannot be visited through a denylist

To configure the URLs that cannot be visited through a denylist, perform the following tasks:

Task	Remarks
(Optional.) Configure address groups	Add IP addresses to an address group.
(Optional.) Configure time range groups	Set the time period during which URLs cannot be visited.
(Required.) Configure URL control	Enable URL denylist mode, and add a custom URL category.

Limit the types of files that can be downloaded

To limit the types of files that can be downloaded, perform the following tasks:

Task	Remarks
(Optional.) Configure address groups	Add IP addresses to an address group.
(Optional.) Configure time range groups	Set the time period during which the files can be downloaded.
(Required.) Configure file control	Configure the types of file that can be downloaded.

Configure bandwidth management

About this feature

Bandwidth management can perform fine-grained control over traffic based on address groups and time range groups. For bandwidth-intensive packets to be rate limited (for example, P2P packets), you can enable the restricted channel to limit the bandwidth consumed by them. For delay-sensitive interactive packets, you can enable the green channel to guarantee the bandwidth for them.

Restrictions and guidelines

- You can forward delay-sensitive packets such as gaming packets and interactive packets through the green channel. You can forward bandwidth-sensitive packets such as P2P packets through the restricted channel. Other packets will be forwarded through the normal channel.
- The match order of packets is as follows:
  - If a packet matches the rule for the green channel, it enters the green channel.
  - If a packet does not match the rule for the green channel but matches the rule for the restricted channel, it enters the restricted channel.
  - If a packet does not match either rule, it enters the normal channel. The normal channel is limited by the rate limiting configuration.
- The configured maximum traffic rate applies to all traffic that enters the restricted channel.
- When both the packet length and port are used to identify packets for the green channel, a packet is matched if it matches either the packet length or the port.

Configure rate limiting

About this task

Perform this task to enforce bandwidth management on interfaces and users.

Prerequisites

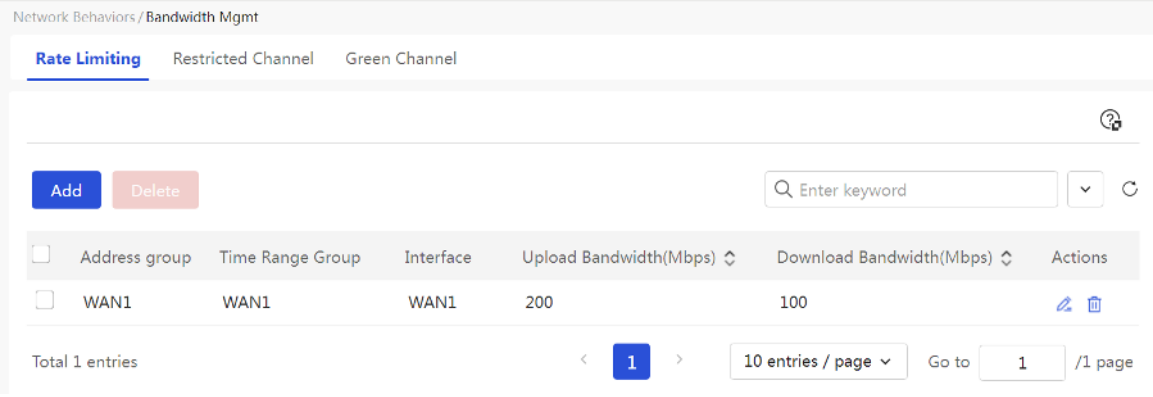
Configure the uplink bandwidth and downlink bandwidth from the **Network Settings** > **External Network Settings** > **WAN Settings** page. Alternatively, you can click the **configured** link in the **Rate Limit** area to navigate to the **WAN Settings** page to configure the uplink bandwidth and downlink bandwidth.

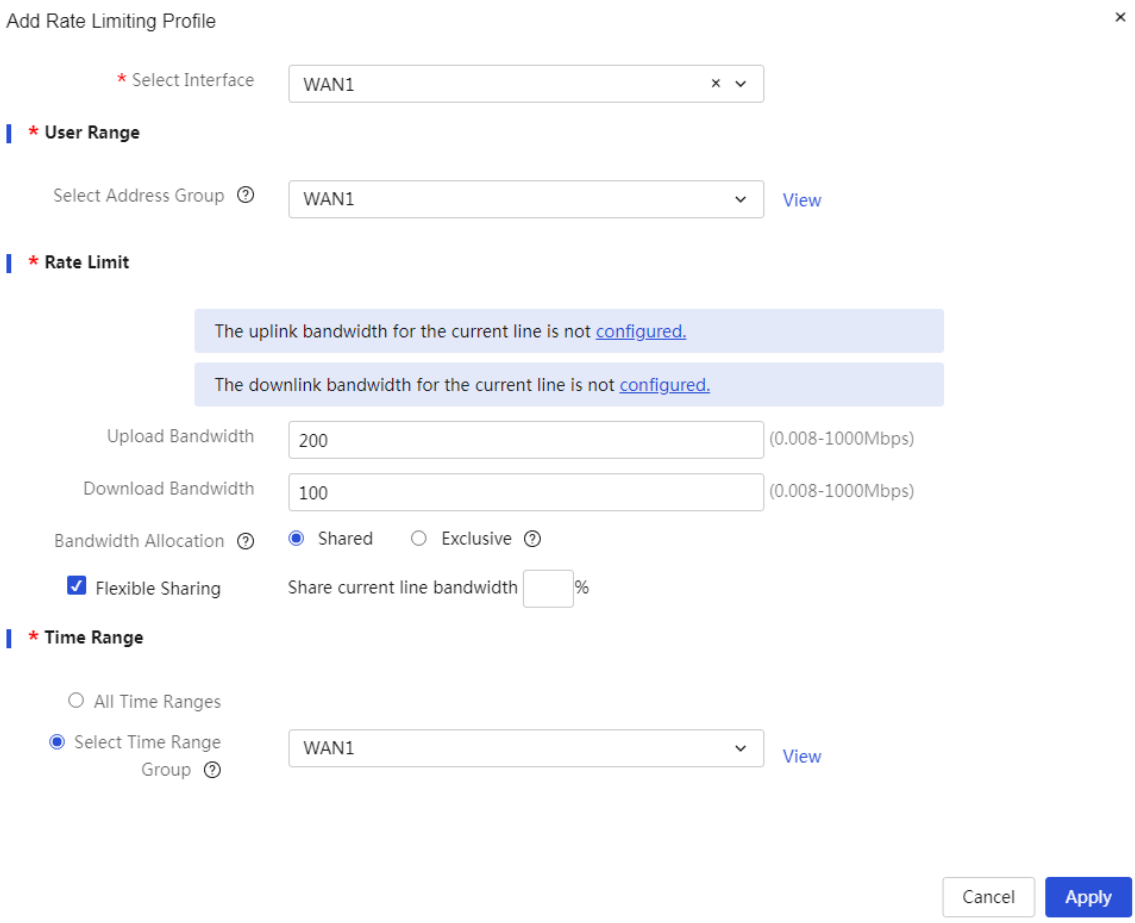
Procedure

1. From the left navigation pane, select **Network Behaviors** > **Bandwidth Mgmt**.
2. On the **Rate Limiting** tab, click **Add**. The **Add Rate Limiting Profile** window appears.
3. Select an interface to apply the rate limiting profile.
4. In the **User Range** area, select an address group to apply the rate limiting profile.
5. In the **Rate Limit** area, configure the following parameters:
   - Click the **configured** link to configure the uplink bandwidth for the current line according to the actual uplink bandwidth provided by your ISP.
   - Click the **configured** link to configure the downlink bandwidth for the current line according to the actual downlink bandwidth provided by your ISP.
   - **Upload Bandwidth**: Specify the maximum upload bandwidth for users in the address group.
   - **Download Bandwidth**: Specify the maximum download bandwidth for users in the address group.

- **Bandwidth Allocation**: Select either of the following bandwidth allocation method:
  - **Shared**: All addresses in the address group share the specified bandwidth.
  - **Exclusive**: Each address in the address group exclusively uses the specified bandwidth (upper limit).
- **Flexible Sharing**: When the traffic rate of a user exceeds the configured bandwidth limit, the user can share the specified percentage of the uplink or downlink bandwidth. This parameter can be configured if you have selected **Shared**.
- In the **Time Range** area, select time ranges during which the rate limiting profile is in effect.

6. Click **Apply**.





Configure the restricted channel

About this task

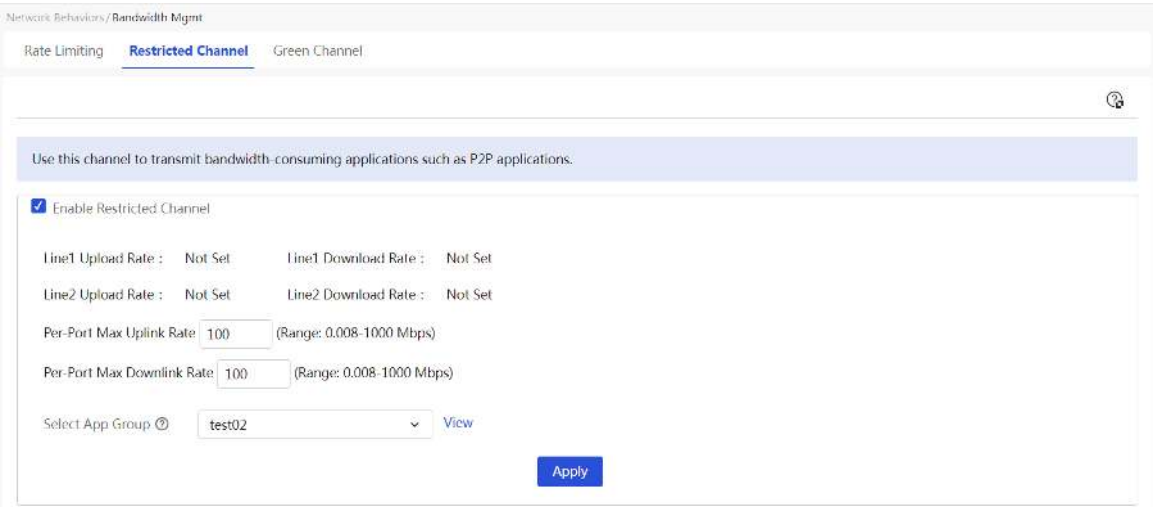
Perform this task to enforce bandwidth management on bandwidth-sensitive application traffic (for example, P2P traffic).

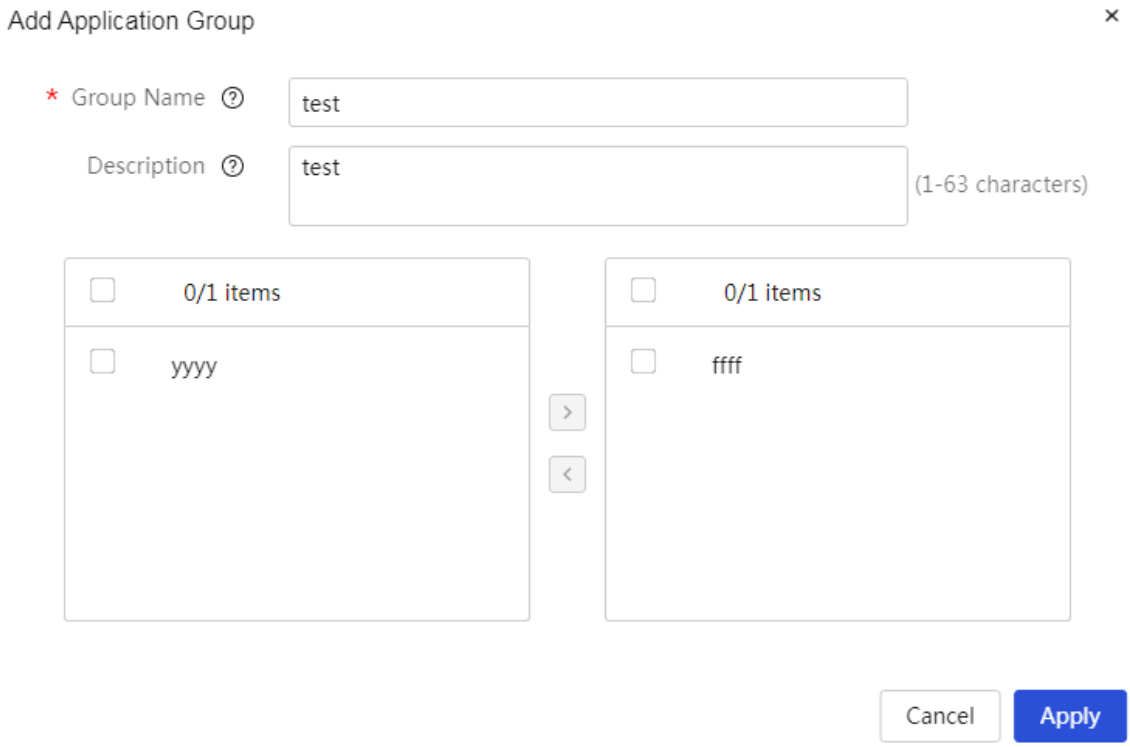
Restrictions and guidelines

Only packets matching the specified application group are forwarded through the restricted channel.

Procedure

1. Click the Restricted Channel tab to access the Restricted Channel page.
2. Select **Enable Restricted Channel**.
3. In **Per-Port Max Uplink Rate** field, enter the maximum uplink traffic rate allowed for each port. If the uplink bandwidth of line *n* has been configured, this parameter must be smaller than or equal to it.
4. In **Per-Port Max Downlink Rate** field, enter the maximum downlink traffic rate allowed for each port. If the downlink bandwidth of line *n* has been configured, this parameter must be smaller than or equal to it.
5. Select App Group: Select an existing application group or click **Add** to add a new application group. To view all existing application groups, click **View**.
6. Click **Apply**.





Configure the green channel

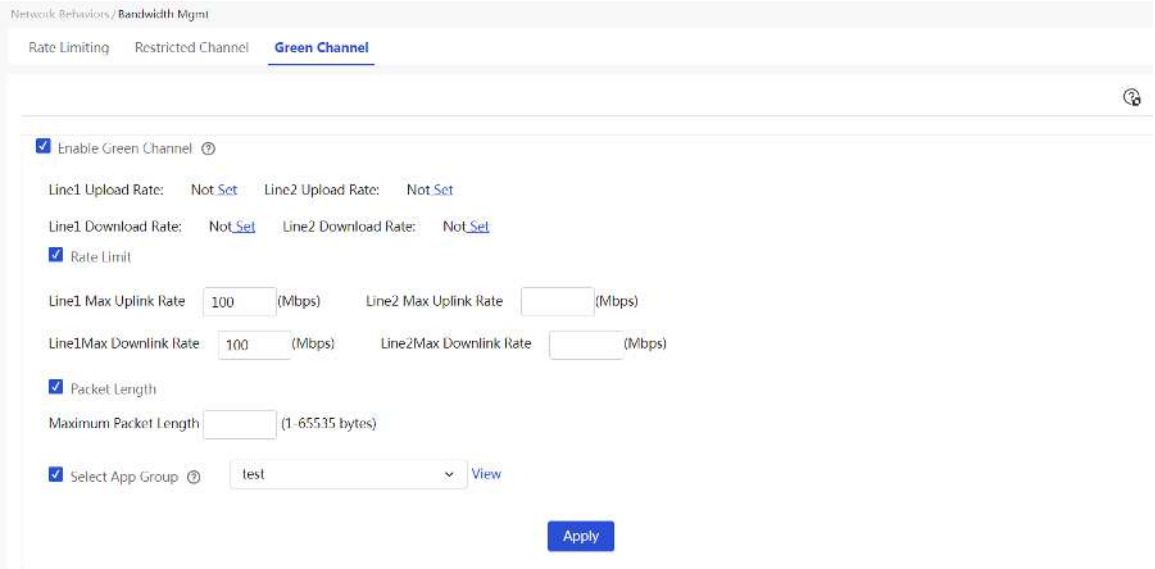
Restrictions and guidelines

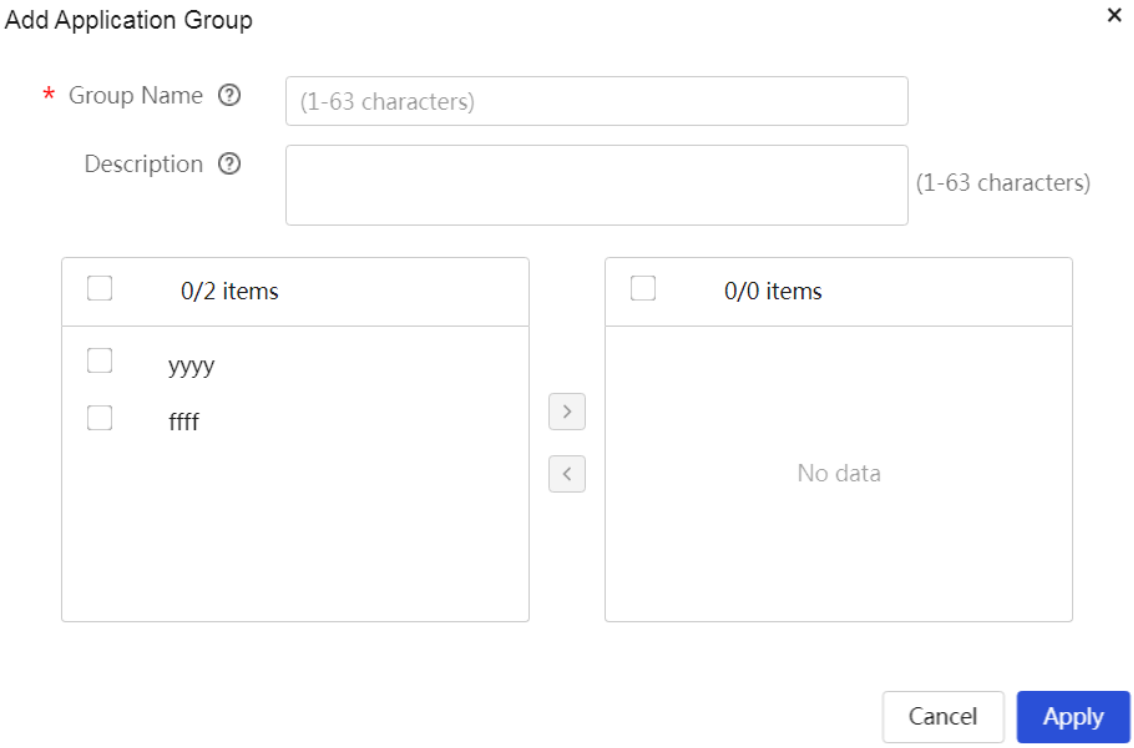
- To avoid affecting common traffic, do not set large a bandwidth value for the green channel.
- Only packets matching the specified application group or shorter than the maximum packet length are forwarded through the green channel.
- You can forward delay-sensitive packets such as gaming packets and interactive packets through the green channel. You can bandwidth-sensitive packets such as P2P packets through the restricted channel. Other packets will be forwarded through the normal channel.
- The match order of packets is as follows:
  - If a packet matches the rule for the green channel, it enters the green channel.
  - If a packet does not match the rule for the green channel but matches the rule for the restricted channel, it enters the restricted channel.
  - If a packet does not match either rule, it enters the normal channel. The normal channel is limited by the rate limiting configuration.

Procedure

1. Click the **Green Channel** tab to access the **Green Channel** page.
2. Select **Enable Green Channel**, and set the upload and download line rates. If a rate is not set, click the **Set** link to set it. The **Set** link leads you to the **WAN Settings** page. On the **WAN Settings** page, click the edit icon in the **Actions** column for a line. Set the uplink network bandwidth and downlink network bandwidth, and click **Apply**.
3. Select **Rate Limit**, and set the maximum uplink and downlink bandwidth values for lines to guarantee bandwidth for interactive applications.
4. Select **Packet Length**, and set the maximum packet length.

5. Select **Select App Group**, and select an existing application group or click **Add** to add a new application group. To view all existing application groups, click **View**.
6. Click **Apply**.





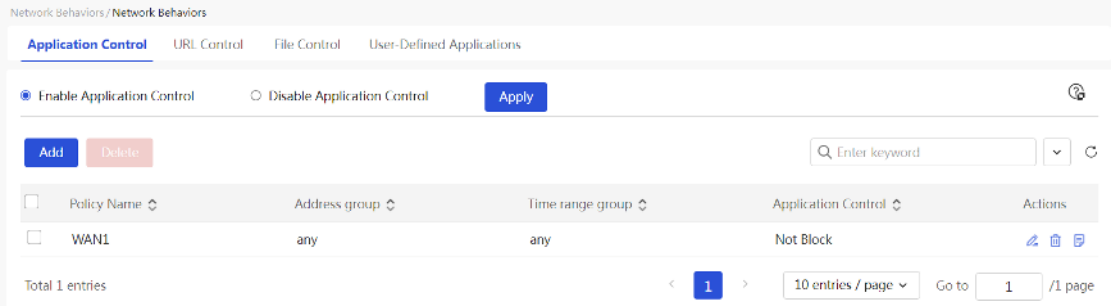
Configure network behavior management

About this feature

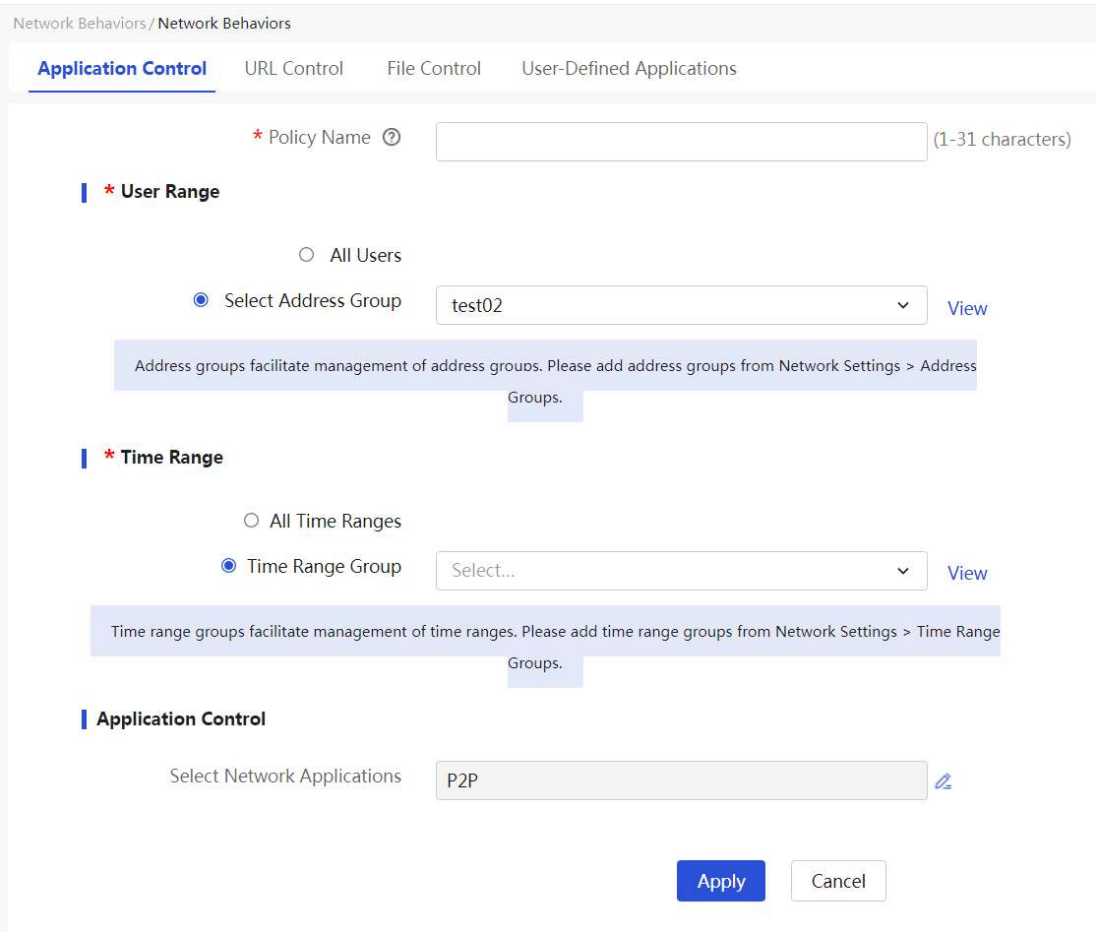
This function manages network behaviors of users based on address groups, time range groups, and applications.

Configure application control

1. From the left navigation pane, select Network Behaviors > Network Behaviors.
2. On the Application Control tab, select **Enable Application Control**, and click **Apply**.



3. Click **Add** to add an application control policy. On the page that opens, configure the following parameters:
   - In the **Policy Name** field, enter a policy name.
   - In the **User Range** area, select an address group to apply the application control policy.
   - In the **Time Range** area, select time ranges during which the application control policy is in effect.



   - In the **Application Control** area, click the details icon to select network applications and configure actions. The following actions are available:
     - Block: Block access to the applications.

- No Blocking or Rate Limit: Do not limit access to the applications.
- Rate Limit: Rate limit access to the applications. You can set the maximum uplink bandwidth and maximum downlink bandwidth per user.

4. Click **Apply**.

Select Network Applications ×

Application Type	Action ☐ Block All
⊖ P2P	
IQiYi	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
Thunder	◉ Block ○ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
YouKu(PC)&TuDou	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
⊖ game	
Fantasy Westward Journey	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
Sky:Children of the Light	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
PUBG	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
DOTA2	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
DNF	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
CrossFire	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
League of Legends: Wild Rift	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
League of Legends	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
Identity V	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
Clashofclans	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
TeamfightTactics	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
SubwaySurfers	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
RodeoStampede	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
TalkingTomGoldRun	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
SoulKnight	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
Minecraft	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
QQSpeed	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
Sausage Man	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
Tom and Jerry	○ Block ◉ No Blocking or Rate Limit ○ Rate limit Upload Rate 100 (kbps) Download Rate 100 (kbps)
⊕ Shopping	
⊕ Media	
⊕ Customization	

Cancel Apply

Configure URL control

About this task

Perform this task to allow users to access or prevent users from accessing the specified URLs.

Restrictions and guidelines

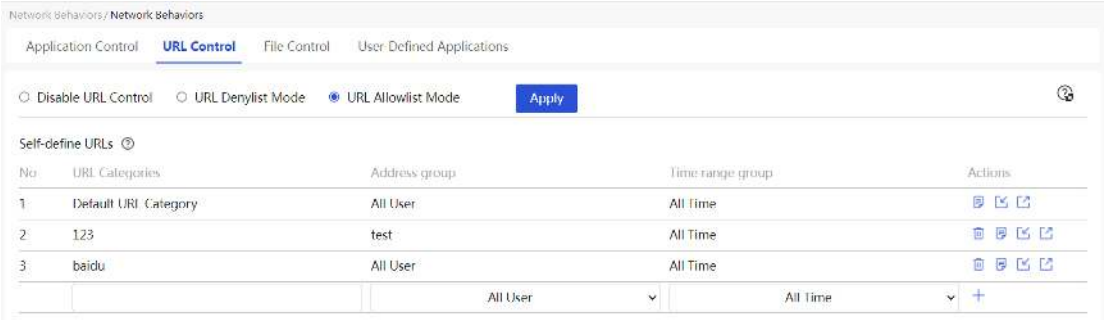
- After you enable URL denylist mode, the device prevents users from accessing the URLs in the custom URL category during the specified time period. The users can access the URLs not in the custom URL category. Suppose you create a URL denylist, with the URL category as URL group A and the address group as user group A. The match rules are as follows:
  - If user 1 belongs to user group A, user 1 cannot access URLs in URL group A.
  - If user 2 does not belong to user group A, user 2 can access any URLs.
- After you enable URL allowlist mode, the device allows users to access the URLs in the custom URL category during the specified time period. The users cannot access the URLs not in the custom URL category. Suppose you create the following allowlists:
  - URL allowlist A: The URL category is URL group A and the address group is user group A.
  - URL allowlist B: The URL category is URL group B and the address group is user group B.

  The match rules are as follows:
  - If user 1 belongs to both user group A and user group B, user 1 can access only URLs in URL group A and URL group B.
  - If user 2 belongs to user group A, user 1 can access only URLs in URL group A.
  - If user 3 does not belong to user group A or user group B, user 3 cannot access any URLs.
- If the IE browser is used to export custom URLs and Excel fails to be started, modify the browser settings as follows:

  Select **Tools** > **Internet Options**, click the **Security** tab, and click **Custom level**. Under ActiveX controls and plug-ins, select **Enable** for **Initialize and script ActiveX controls not marked**.
- To exactly match a URL, do not add wildcards (*) in the URL keyword, for example, **www.baidu.com**. To perform fuzzy matching, add wildcards (*) in the URL keyword, for example, ***.baidu.com**, **www.baidu***, or ***baidu***. To match all URLs, set the URL keyword to ***.***.

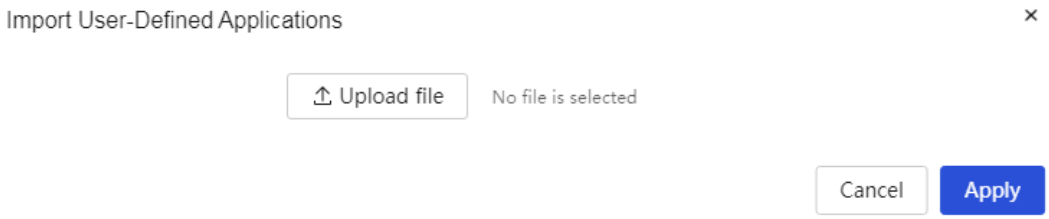
Procedure

1. From the left navigation pane, select **Network Behaviors** > **Network Behaviors**.
2. Click the **URL Control** tab.
3. Select Disable URL Control, URL Denylist Mode, or URL Allowlist Mode. If you select URL Denylist Mode or URL Allowlist Mode, you must click Apply to enable URL control.
4. In the text box below **Default URL Category**, enter a URL category name.
5. In the text box below **All User**, select an address group to apply the URL control policy.
6. In the text box below **All Time**, select an time range group to apply the URL control policy.
7. Click the + button to add the URL category.



8. To add URLs to the URL category:
   - Click the **Detail** icon in the **Actions** column for the URL category. The **Set URL Keyword** dialog box appears. In the **URL Keywords** text box, enter URL keywords. A URL keyword is a case-insensitive sting of 1 to 63 characters and can contain letters, digits, and special characters (except /\'"<>;&`:). It cannot contain spaces. To exactly match a URL, do not add wildcards (*) in the URL keyword, for example, **www.baidu.com**. To perform fuzzy matching, add wildcards (*) in the URL keyword, for example, ***.baidu.com**, **www.baidu***, or ***baidu***. To match all URLs, set the URL keyword to ***.***. Click the + plus to add a URL keyword. Click **Apply**.

   - To import custom URLs, click the **Import** icon in the **Actions** column for the URL category. On the dialog box that opens, click **Upload file**, select a the target file, and click **Apply**.



Configure file control

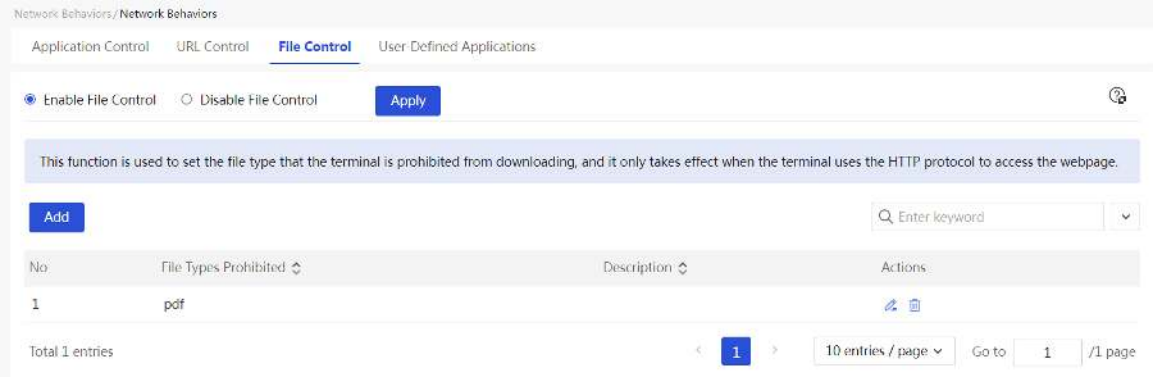
Restrictions and guidelines

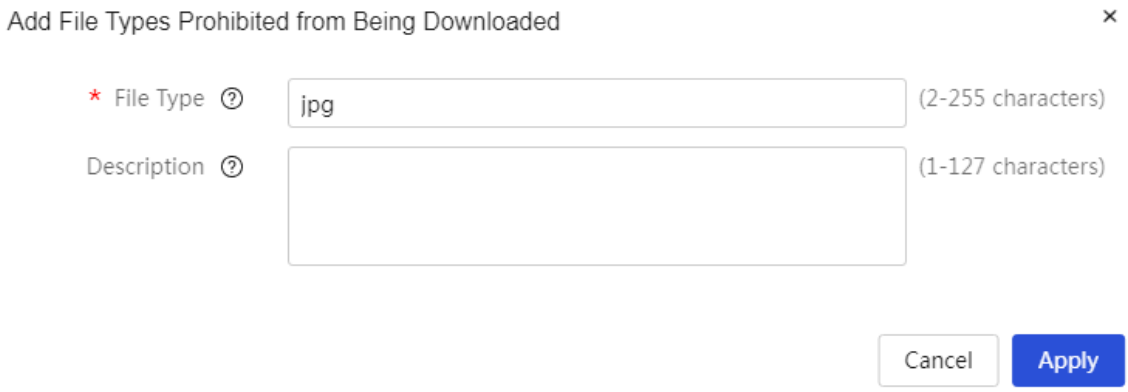
This feature takes effect only when a user uses HTTP to download files.

Procedure

1. From the left navigation pane, select **Network Behaviors** > **Network Behaviors**.
2. Click the **File Control** tab.
3. Select Enable File Control, and click Apply.
4. Click Add. The Add File Types Prohibited from Being Downloaded dialog box appears.
5. In the **File Type** field, enter an extension of files that cannot be downloaded.
6. In the **Description** field, enter a description for the file control policy.

7. Click **Apply**.





Configure user-defined network applications

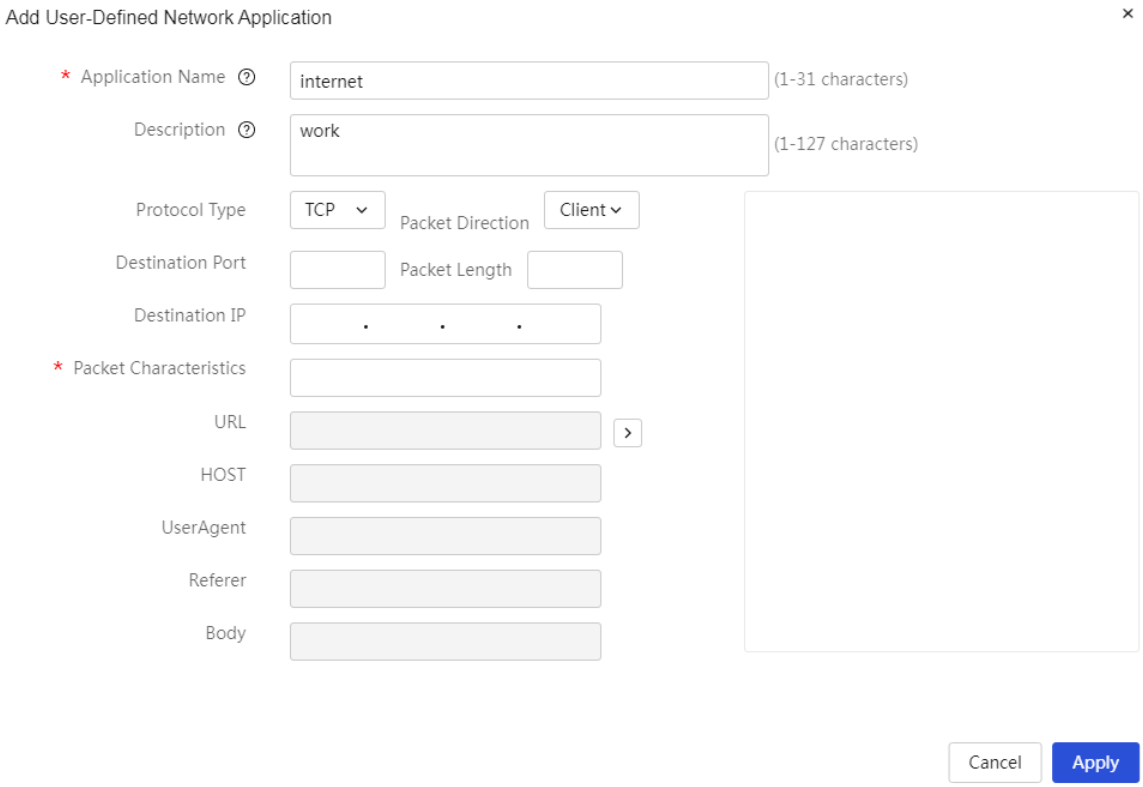
Restrictions and guidelines

- To limit the network applications that can be accessed by users according to the packet characteristics of those applications, you can add user-defined network applications and reference them in an application control policy.
- After you add user-defined network applications, you must reference them in an application control policy.
- After a user-defined network application is referenced in an application control policy, it cannot be deleted.

Procedure

1. Click the User-Defined Applications tab.
2. Click **Add** to add a user-defined application. On the dialog box that opens, configure the following parameters:
3. In the **Application Name** field, enter an application name.
4. In the **Description** field, enter a description for the application.
5. From the **Protocol Type** list, select a protocol type. From the **Packet Direction** list, select a packet direction. Supported protocol types are TCP, UDP, HTTP, HTTPS, and SSL. When the protocol type is TCP or UDP, the packet characteristics must be configured. When the protocol type is SSL, the destination port and the HOST parameter must be configured. Supported packet directions are Client, Server, and Any. Any indicates all packets received by the device.
6. In the **Destination Port** field, enter the destination port number of the application. In the **Packet Length** field, enter a packet length.

7. In the **Destination IP** field, enter the destination IP address of the application.
8. The following items can be defined to match the packet content::
   - Packet Characteristics: Define the characteristics for TCP packets and UDP packets.
   - URL: Define the URL information for HTTP packets.
   - HOST: Define the HOST information for HTTP packets, HTTPS packets, and SSL packets.
   - UserAgent: Define the UserAgent information for HTTP packets.
   - Referer: Define the Referer information for HTTP packets.
   - Body: Define the Body information for HTTP packets.
9. Click **>** to add the packet characteristics to the right box.
10. Repeat the preceding steps to add new packet characteristics to the right box.
11. Click **Apply** to add the user-defined application.



Configure audit logs

About this feature

This feature allows you to audit logs of the application control and URL control functions and send the logs to the specified server.

Configure application audit logs

About this task

Perform this task to audit logs of the application control function.

Prerequisites

To enable application log auditing, first enable application control.

Procedure

1. From the left navigation pane, select **Network Behaviors** > **Audit Logs**.
2. On the **App Audit Log** tab, select **Enable App Audit Logging**.
3. To clear all application audit logs, click **Clear Logs**. In the confirmation dialog box, click **Apply**.
4. To export all application audit logs to an Excel file, click **Export to Excel**.

Configure URL filter logs

About this task

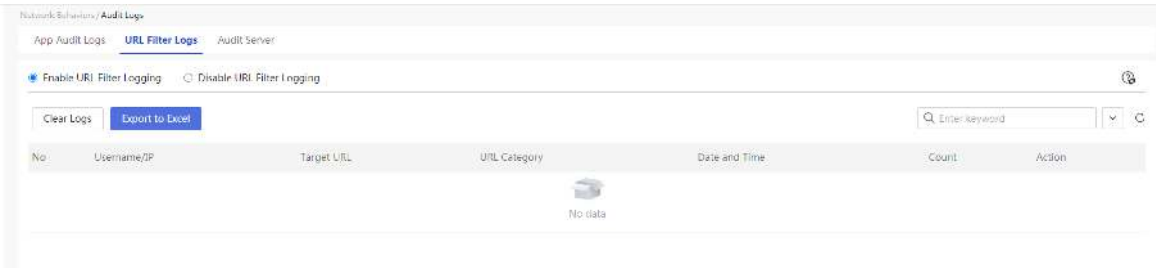
Perform this task to audit logs of the URL control function.

Prerequisites

To enable URL filter log auditing, first enable URL control.

Procedure

1. Click the **URL Filter Log** tab.
2. Select Enable URL Filter Logging.
3. To clear all URL filter logs, click **Clear Logs**. In the confirmation dialog box, click **Apply**.
4. To export all URL filter logs to an Excel file, click **Export to Excel**.



Configure an audit server

About this task

Perform this task to configure an audit server to send audit logs.

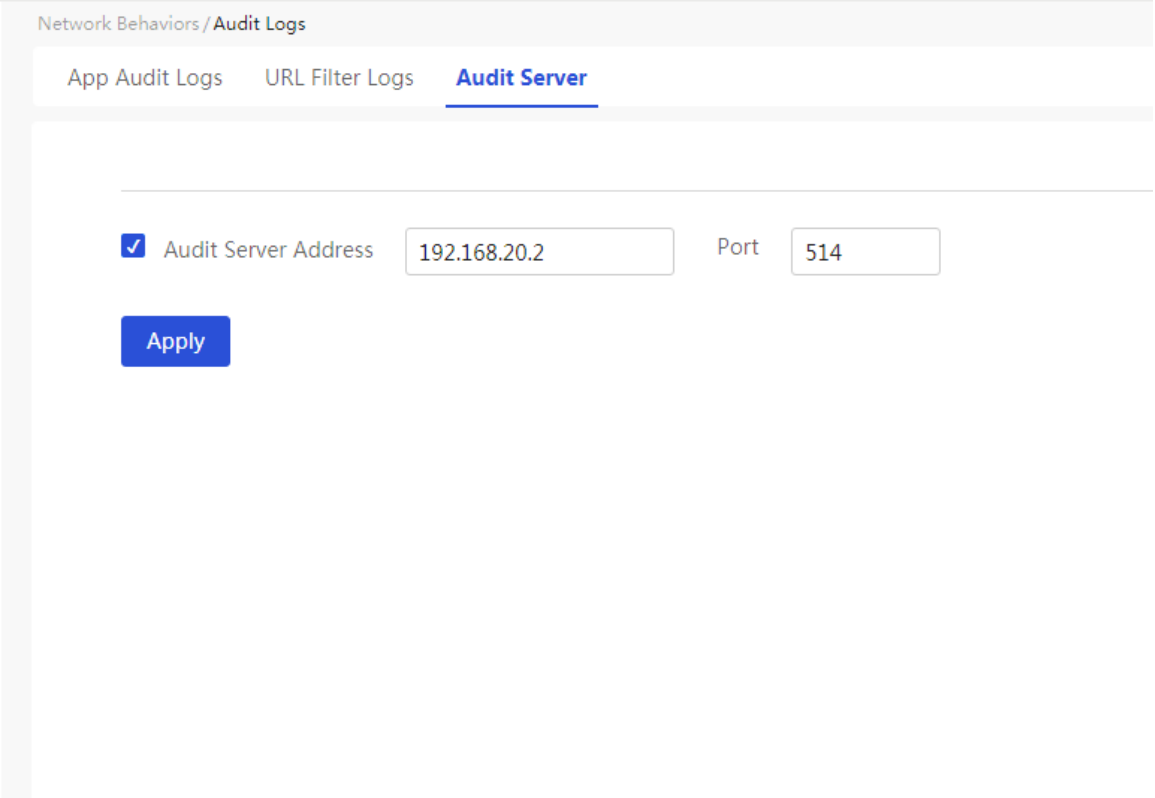
Prerequisites

Make sure the IP address of the audit server can communicate with the IP address of the device.

Procedure

1. Click the **Audit Server** tab.
2. Select **Audit Server Address** to enable sending audit logs to an audit server.

3. In the **Audit Server Address** field, enter the IP address or domain name of the audit server.
4. In the **Port** field, enter the port number of the audit server.
5. Click **Apply**.



Configure network security

Deny inter-VLAN communication

Configure tasks at a glance

To deny inter-VLAN communication, perform the following tasks:

Task	Remarks
(Required.) Configure VLANs	Create VLANs for different departments.
(Required.) Configure the firewall	Configure firewall settings to deny inter-VLAN communication.

Configure the firewall

About this feature

This feature allows you to configure firewall settings for network security protection. The firewall matches packets in the network based on a series of security rules to block invalid packets and forward valid packets.

Restrictions and guidelines

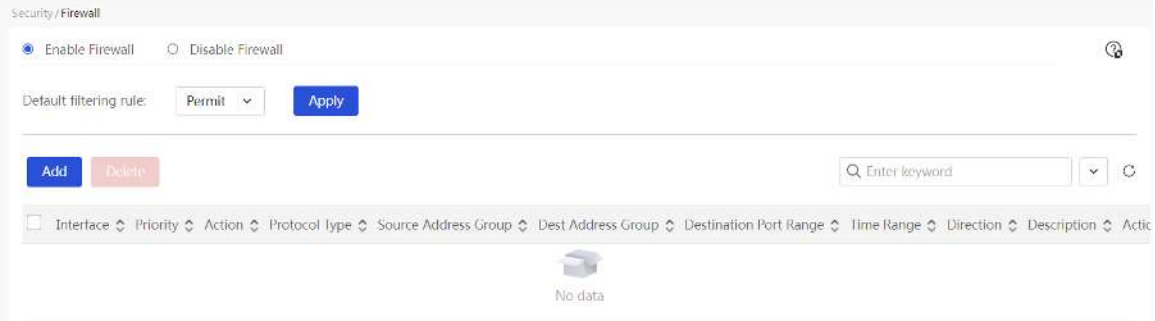
- After a packet matches a firewall security rule, it will no longer match other rules. To avoid incorrect packet filtering actions because of security rule matching errors, set the priorities for security rules to appropriate values.
- If the default filtering rule is **Permit**, you do not need to configure any security rules. All internal network endpoints connecting to the device can access each other and the external network.
- If the default filtering rule is Permit, you can restrict the access permissions for specific internal network endpoints:
  - To deny specific internal network endpoints in a VLAN from accessing the external network, configure a deny security rule between the corresponding VLAN interface and WAN interface.
  - To deny specific internal network endpoints in a VLAN from accessing endpoints in another VLAN, configure a deny security rule between the corresponding VLAN interfaces.
- If the default filtering rule is **Deny** and you have not configured any security rules, no internal network endpoints can access the external network and endpoints in different VLANs cannot access each other.
- If the default filtering rule is **Deny**, you can assign access permissions to specific internal network endpoints:
  - To allow specific internal network endpoints in a VLAN to access the external network, configure both incoming and outgoing permit security rules between the corresponding VLAN interface and WAN interface.
  - To allow specific internal network endpoints in a VLAN to access endpoints in another VLAN, configure both incoming and outgoing permit security rules between the corresponding VLAN interfaces.

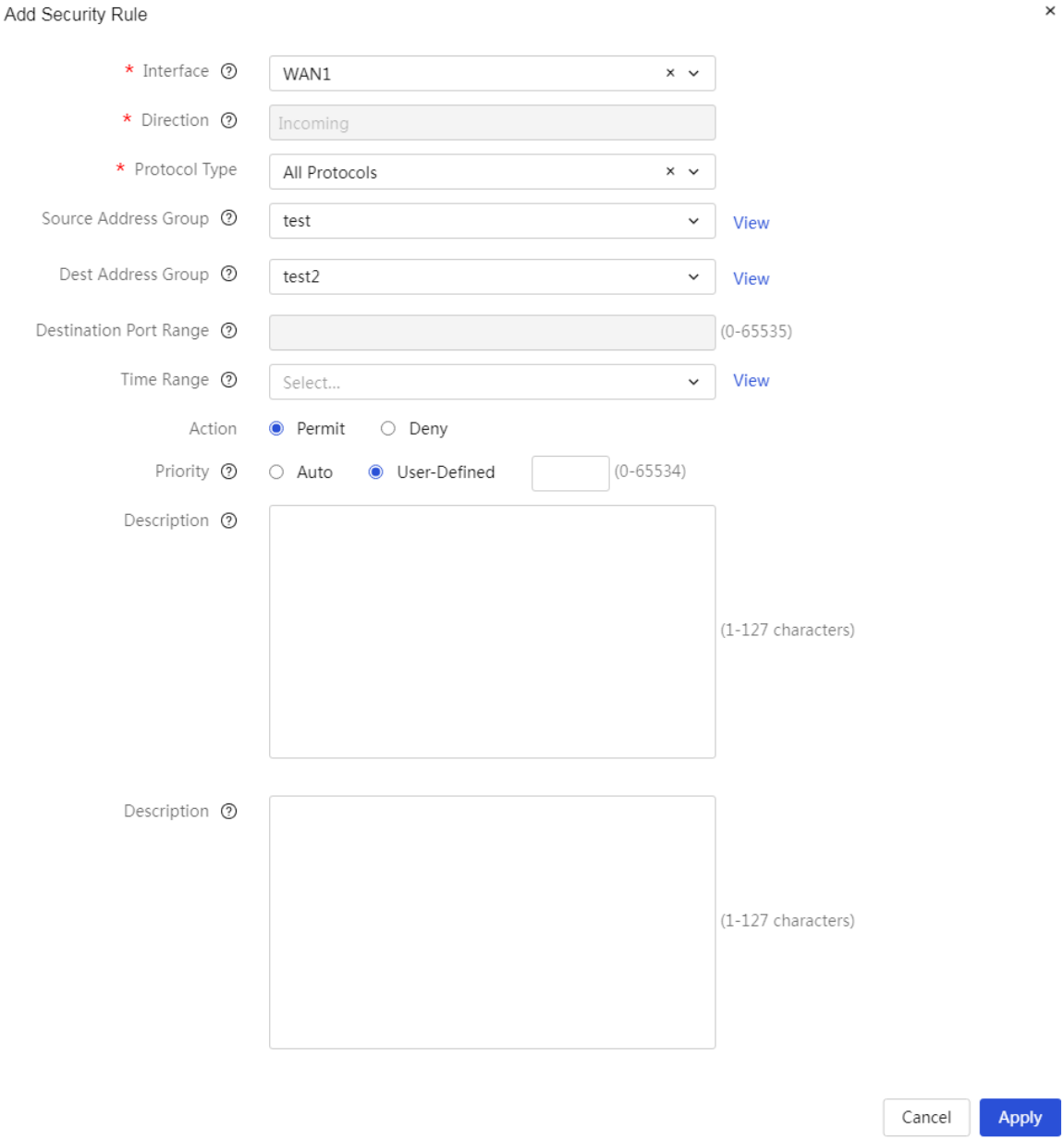
Prerequisites

- Before adding firewall security rules, first complete configuration on the **External Networks** page.
- To specify the time range and address groups for a firewall security rule, you can go to the **Time Range Groups** and **Address Groups** pages to complete corresponding configurations, respectively.

Procedure

1. From the left navigation pane, select **Security** > **Firewall**.
2. Select Enable Firewall.
3. From the **Default filtering rule** list, select an action to take on the packets that do not match any security rules. If you select **Permit**, packets that do not match any security rules are permitted. If you select **Deny**, packets that do not match any security rules are denied. Click **Apply**.
4. Click **Add** to add a security rule.
5. From the **Interface** list, select an interface to apply the security rule.
6. The **Direction** list displays the direction to apply the security rule. If you have selected a WAN interface, the direction is **Incoming**, and the security rule controls the traffic from the external network to the device. If you have selected a VLAN interface, the direction is **Outgoing**, and the security rule controls the traffic from the internal network to the device.
7. From the **Protocol Type** list, select a protocol type to match packets. To match TCP or UDP packets, select TCP or UDP, respectively. To match ICMP packets such as ping or tracert packets, select ICMP. To match packets of all protocols, select All Protocols.
8. From the **Source Address Group** list, select an existing source address group to match packets. You can also create an address group by clicking the **Add** icon from the list.
9. From the **Dest Address Group** list, select an existing destination address group to match packets. You can also create an address group by clicking the **Add** icon from the list.
10. From **Destination Port Range** list, enter a destination port range to match packets.
11. From **Time Range** list, select an existing time range group during which the security rule is in effect.
12. Select an action to take on the packets matching the rule.
    - Permit: Permit the packets to pass through.
    - Deny: Deny the packets from passing through.
13. Configure a priority for the rule.
    - Auto: The system automatically assigns a priority to the rule. The priorities of rules are assigned in the rule creation order at a step of 5. A rule created earlier has a higher priority.
    - User-Defined: Specify a user-defined priority for the rule. The smaller the number, the higher the priority.
14. In the **Description** field, enter a description for the rule.
15. Click **Apply**.


Security / Firewall
Enable Firewall
Disable Firewall
Default filtering rule:
Permit
Apply
Add
Delete
Enter keyword
Interface
Priority
Action
Protocol Type
Source Address Group
Dest Address Group
Destination Port Range
Time Range
Direction
Description
No data


Add Security Rule
* Interface
WAN1
* Direction
Incoming
* Protocol Type
All Protocols
Source Address Group
test
View
Dest Address Group
test2
View
Destination Port Range
(0-65535)
Time Range
Select...
View
Action
Permit
Deny
Priority
Auto
User-Defined
(0-65534)
Description
(1-127 characters)
Description
(1-127 characters)
Cancel
Apply

Configure connection limits

About this feature

This function is a security mechanism used to limit the number of connections initiated by IP addresses. With this function configured, the device can allocate resources reasonably and prevent malicious connections.

When the number of TCP or UDP connections from an IP address exceeds the specified number, the device denies new connections from the IP address. When the number of TCP or UDP connections from an IP address falls below the specified number, the device accepts new connections from the IP address.

The device supports the following connection limit types:

- Per-IP connection limit: Limits the number of connections initiated by each IP address in an IP address range. This limit type limits the number of connections received on all interfaces of the device.
- VLAN-based connection limit: Limits the number of connections initiated by each IP address to a VLAN interface. This limit type limits the number of connections received on one VLAN interface.

Restrictions and guidelines

- In a per-IP connection limit rule, a connection limit is applied separately to each IP address. If an address group contains only one IP address, only the IP address is limited.
- If multiple connection limit rules contain overlapping IP address ranges, the connection rule configure earlier has higher priority. If you configure connection limit rules with the same IP address range, the connection limit rule configured earlier takes effect.
- You can delete or edit a connection limit rule configured earlier. Editing a connection limit rule does not change the priority of the connection limit rule.
- A per-IP connection limit controls the number of connections that an internal IP address initiates to the Internet. The following connections are not counted: connections to the device and to other internal IP addresses, and connections from the Internet to the internal IP address.
- The total connections contain TCP connections, UDP connections, and other connections (connections other than TCP connections and UDP connections, for example, ICMP connections). An IP address can establish new connection only if the number of connections that have been established by it does not exceed the connection limit. If an IP address wants to establish a TCP connection, its total number of connections cannot exceed the total connection limit, and its number of TCP connections cannot exceed the TCP connection limit. This rule applies to UDP connection establishment and establishment of any other connections.
- If you set the TCP connection limit to 0, no TCP connections can be established. If you leave this parameter blank, the number of TCP connection allowed is limited by only the total connection limit. This rule also applies to UDP connections.
- A VLAN-based connection limit rule limits the total number of connections established in a VLAN. In a VLAN-based connection limit rule, a connection limit applies to all IP addresses in a VLAN instead of to each IP address separately.
- The total connections contain TCP connections, UDP connections, and other connections (connections other than TCP connections and UDP connections, for example, ICMP connections). An IP address in a VLAN can establish new connection only if the total number of connections that have been established all IP addresses in the VLAN does not exceed the connection limit. If an IP address in a VLAN wants to establish a TCP connection, its total number of connections cannot exceed the total connection limit, and its number of TCP

connections cannot exceed the TCP connection limit. This rule applies to UDP connection establishment.

- A VLAN-based connection limit controls the number of connections that an IP address in the VLAN initiates to the Internet. The following connections are not counted: connections to the device and to other IP addresses in the same VLAN, connections to IP addresses in different VLANs, and connections from the Internet to an IP address in the VLAN.
- If you set the TCP connection limit to 0, no TCP connections can be established. If you leave this parameter blank, the number of TCP connection allowed is limited by only the total connection limit. This rule also applies to UDP connections.

Configure per-IP connection limits

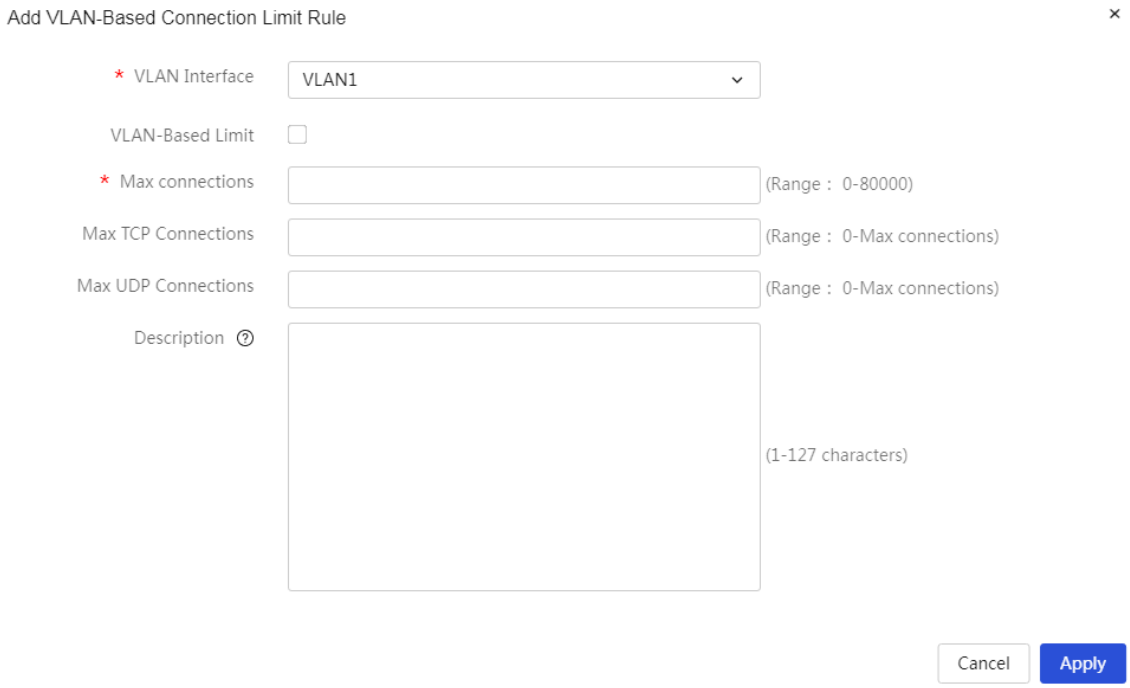
1. From the left navigation pane, select **Security** > **Connection Limits**.
2. On the Per-IP Connection Limits tab,
3. Select Enable Per-IP Connection Limits.
4. Click **Add** to add a per-IP connection limit rule.
5. From the **Select Address Group** list, select an existing address group to match packets. You can also create an address group by clicking the **Add** icon from the list.
6. In the **Per-IP Connection Limit** field, enter the total maximum number of connections allowed for each IP address.

   Packets with the same source IP address but a different source port, destination IP address, destination port, or protocol type belong to different connections.
7. In the **Per-IP TCP Connection Limit** field, enter the maximum number of TCP connections allowed for each IP address. You can separately limit the TCP connections in addition to limiting the total connections.
8. In the **Per-IP UDP Connection Limit** field, enter the maximum number of UDP connections allowed for each IP address. You can separately limit the UDP connections in addition to limiting the total connections.
9. In the **Description** field, enter a description for the rule.
10. Click **Apply**.

Configure VLAN-based connection limits

1. From the left navigation pane, select **Security** > **Connection Limits**.
2. Click the VLAN-Based IP Connection Limits tab.
3. Select Enable VLAN-Based Connection Limits.
4. Click **Add** to add a VLAN-based connection limit rule.
5. From the **VLAN Interface** list, select a VLAN interface to apply the rule.
6. Select VLAN-Based Limit.
7. In the **Max Connections** field, enter the total maximum number of connections allowed for the VLAN interface.

   Packets with the same source IP address but a different source port, destination IP address, destination port, or protocol type belong to different connections.
8. In the **Max TCP Connections** field, enter the maximum number of TCP connections allowed for the VLAN interface. You can separately limit the TCP connections in addition to limiting the total connections.
9. In the **Max UDP Connections** field, enter the maximum number of UDP connections allowed for the VLAN interface. You can separately limit the UDP connections in addition to limiting the total connections.
10. In the **Description** field, enter a description for the rule.
11. Click **Apply**.



Configure MAC filter

About this feature

If you want to restrict packets sent from certain devices (allow or disallow them), you can configure the MAC address filtering feature on VLAN interfaces. This feature filters the source MAC address of the received packets based on the MAC allowlist and denylist.

The following filtering methods are available:

- **Allowlist**—Allows source MAC addresses on the allowlist to access the external network, while denying access for others.
- **Denylist**—Denies source MAC addresses on the denylist from accessing the external network, while allowing access for others.

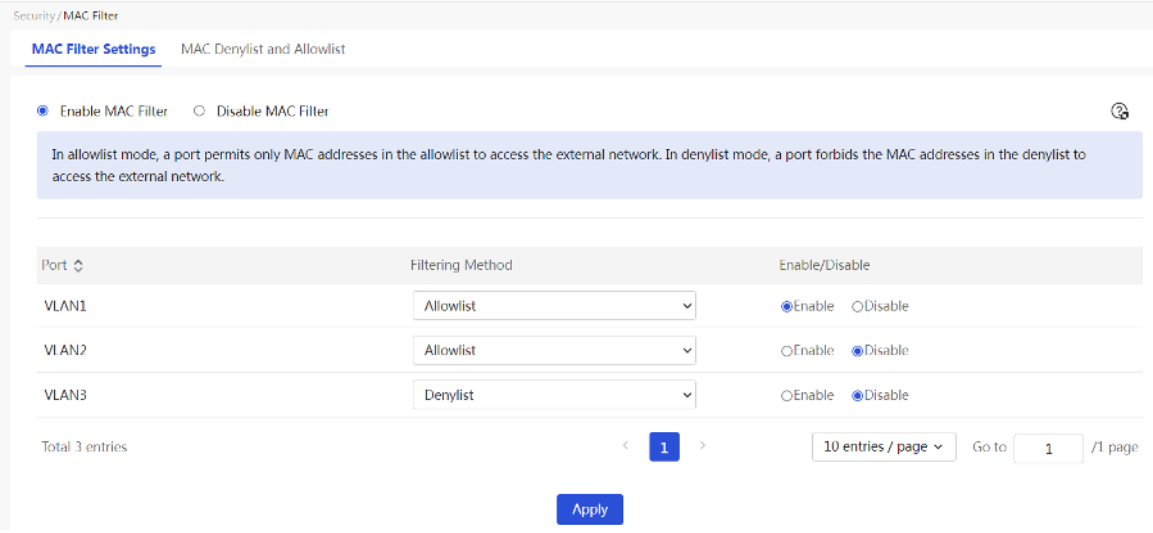
Configure MAC filter settings

Restrictions and guidelines

- If you need to enable MAC address filtering on the interface connected to the administrator's terminal, ensure that the administrator's terminal MAC address is added to the allowlist or not added to the denylist.
- Characters in MAC addresses are not case sensitive.

Procedure

1. From the left navigation pane, select **Security** > **MAC Filter**.
2. Click the **MAC Filter Settings** tab.
3. Check the **Enable MAC Filter** option to enable the MAC address filtering feature.
4. Select the **Allowlist** or **Denylist** option in the **Filtering Method** column of the specified interface, and select the **Enable** option in the **Enable/Disable** column.
5. Click **Apply**.



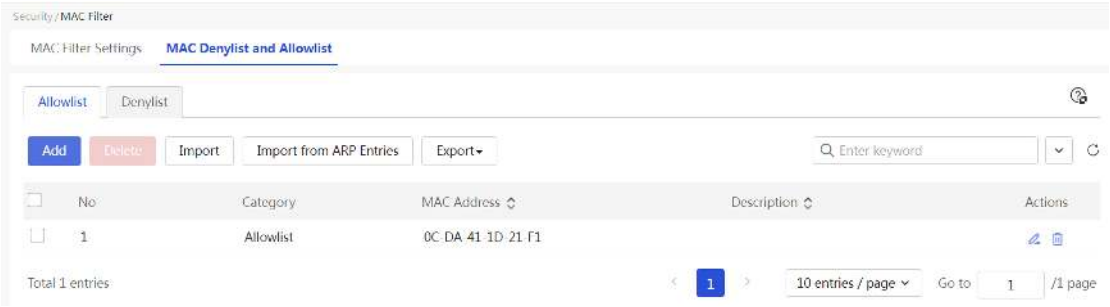
Configure MAC denylist and allowlist

Restrictions and guidelines

The methods of adding allowlist and denylist entries are the same. The following takes allowlist as an example to introduce the configuration steps.

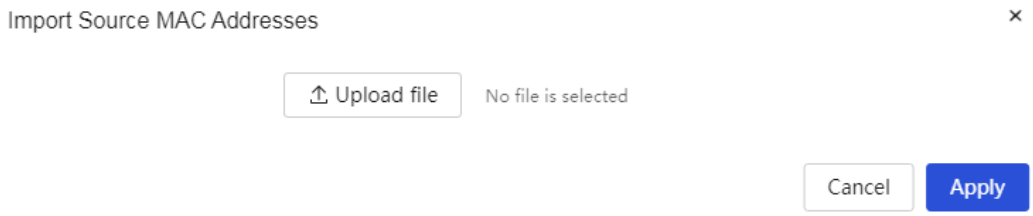
Procedure

1. From the left navigation pane, select **Security** > **MAC Filter**.
2. Click the **MAC Denylist and Allowlist** tab.
3. Click the **Allowlist** tab to enter the allowlist settings page.

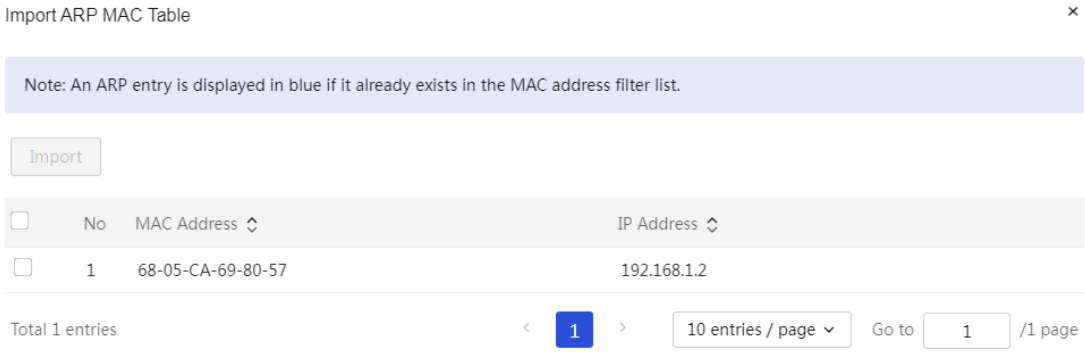


4. To add a single MAC address, follow the steps below:
   a. Click **Add**. The **Add Source MAC** dialog box opens.
   b. In the **MAC Address** field, enter an MAC address.
   c. In the **Description** field, enter description information for the source MAC address.
   d. Click **Apply**. The MAC address will be added to the allowlist.

5. To add MAC addresses in bulk, follow these steps:
   a. Click **Export** and select **Export Template**.
   b. Open the downloaded template, add source MAC addresses, and save the template file locally.
   c. Click **Import** to open the **Import Source MAC Addresses** dialog box.
   d. Click **Upload File**.
   e. In the dialog box that opens, select the edited template and click **Open**.
   f. Click **Apply**. The MAC addresses in the template will be added to the allowlist in bulk.



6. To import MAC addresses from ARP entries, follow these steps:
   a. Click **Import from ARP Entries** to open the **Import ARP MAC Table** dialog box.
   b. Select the MAC addresses to be imported.
   c. Click **Import**. A confirmation dialog box opens.
   d. Click **Yes**. The selected MAC addresses will be imported from the ARP table to the allowlist.



Configure ARP attack protection

About this feature

The ARP protocol itself has vulnerabilities. Attackers can easily exploit the vulnerabilities of the ARP protocol to attack it. The ARP attack protection technology provides various ARP attack protection techniques to prevent, detect, and resolve ARP attacks and ARP viruses in a local area network.

ARP attack protection features include:

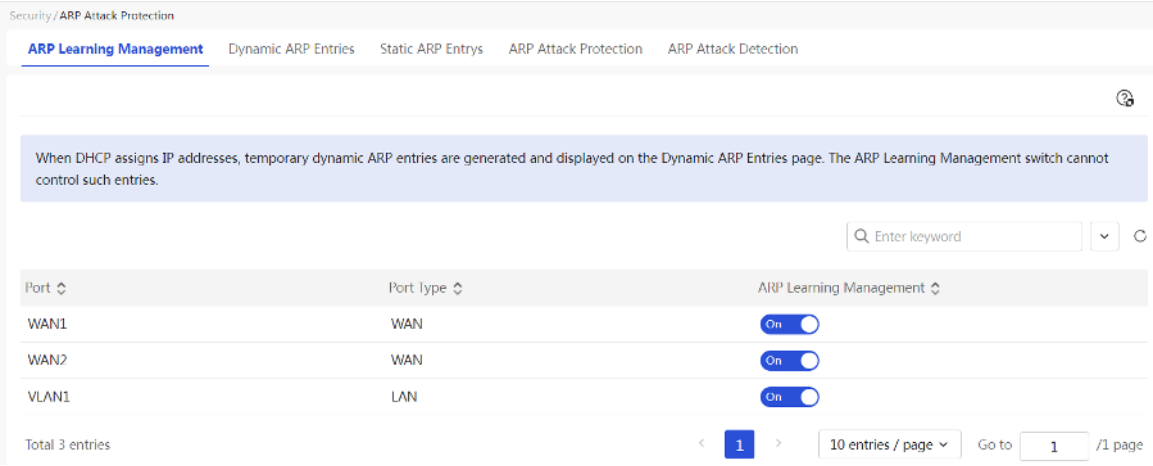
- **ARP learning management**—This feature supports enabling and disabling dynamic ARP learning of an interface. When dynamic ARP learning of an interface is disabled, the interface cannot learn new dynamic ARP entries, which improves security. When an interface on the device has learned the ARP entries for all legitimate users on that interface, it is recommended to disable dynamic ARP learning.
- **Dynamic ARP management**—Includes dynamic ARP entry management, ARP scanning, and fixed ARP. ARP scanning automatically scans users within the local area network and creates dynamic ARP entries for them. Fixed ARP converts the generated dynamic ARP entries into static ARP entries. As a best practice, use ARP scanning and fixed ARP in a small and stable network environment such as an Internet cafe. First enabling ARP scanning and fixed ARP and then disabling dynamic ARP learning can prevent devices from learning incorrect ARP entries.
- **Static ARP management**—Includes manage, refresh, add, import, and export functions of static ARP entries. Refresh function refers to refreshing the static ARP entry list; Add function refers to manually adding static ARP entries; Import function refers to bulk obtaining static ARP entries from a file; Export function refers to exporting existing static ARP entries to a local file.
- **ARP attack protection**—Includes ARP packet validity check and gratuitous ARP functions. ARP packet validity check is to verify the legality of ARP packets by setting rules. A gratuitous ARP packet is a special type of ARP packet where the sender IP address and target IP address carried in the packet are both the local IP address, the source MAC address of the packet is the local MAC address, and the destination MAC address of the packet is the broadcast address. A device achieves the following functions by sending gratuitous ARP packets:
  - Determines if the IP address of other devices conflicts with the IP address of the local device. When other devices receive a gratuitous ARP packet and find that the IP address in the packet is the same as their own IP address, they send an ARP reply to the device that sent the gratuitous ARP packet, informing it of an IP address conflict.

- Notifies hardware address change. After the device has changed its hardware address, it notifies other devices to update their ARP entries by sending a gratuitous ARP packet.

- **ARP attack detection**—Detects all online devices on the specified interface and checks if their information conflicts with the existing ARP entries. According to the search results, ARP binding can be performed.

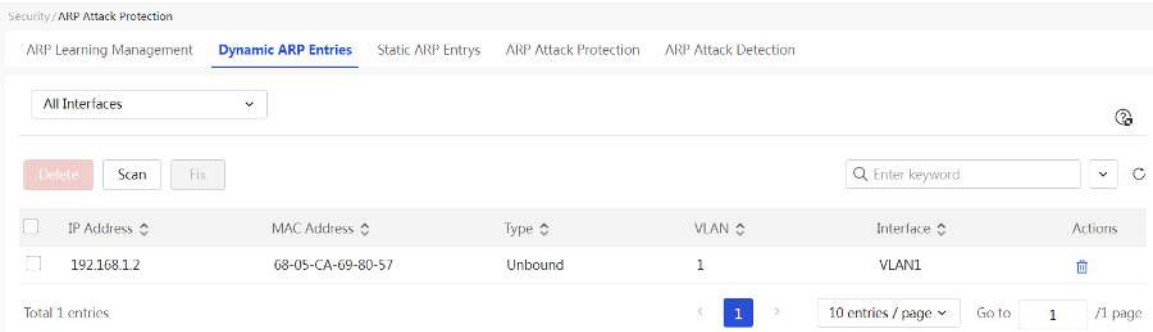
Manage ARP learning

1. From the left navigation pane, select **Security** > **ARP Attack Protection**.
2. Click the **ARP Learning Management** tab.
3. In the **ARP Learning Management** column for an interface, set whether to allow the interface to learn dynamic ARP entries.
   - If you set it to **On**, the interface allows learning dynamic ARP entries.
   - If you set it to **Off**, the interface will not allow dynamic ARP entries to be learned.



Manage dynamic ARP entries

1. From the left navigation pane, select **Security** > **ARP Attack Protection**.
2. Click the **Dynamic ARP Entries** tab to open the page for managing dynamic ARP entries.

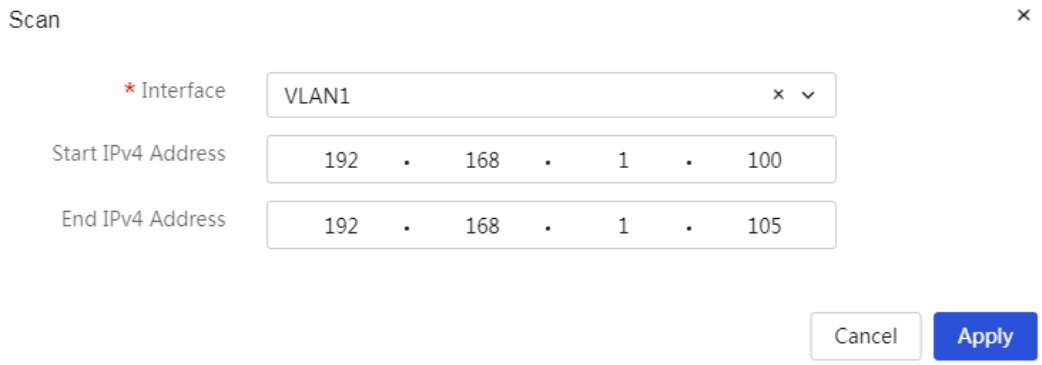


3. You can perform the following management operations on existing dynamic ARP entries:
   - Click **Refresh** to refresh the display information of the current dynamic ARP entries.
   - Select specific dynamic ARP entries, and then click **Delete**. Click **Apply** in the confirmation dialog box to delete the selected entries.
   - Click **Scan** to open the scanning configuration dialog box.

Select the interface where you want to perform ARP scanning.

Set the start and end IP addresses for the ARP scan operation. The start and end IP addresses must be in the same network segment as the IP address of the interface.

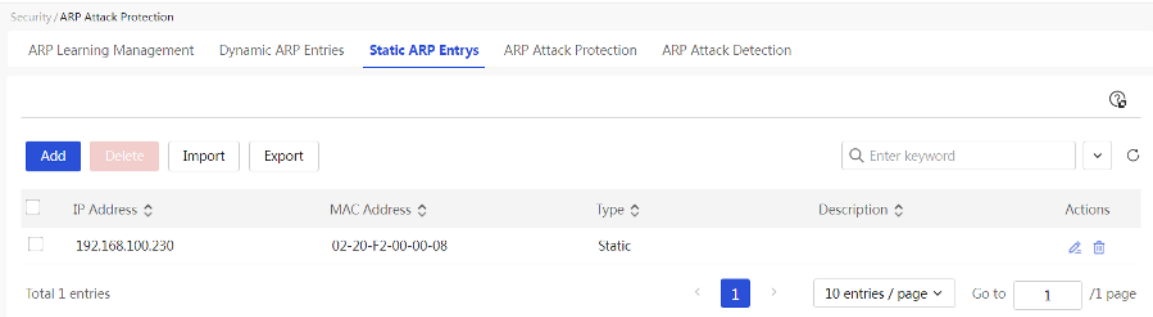
Click **Apply**.

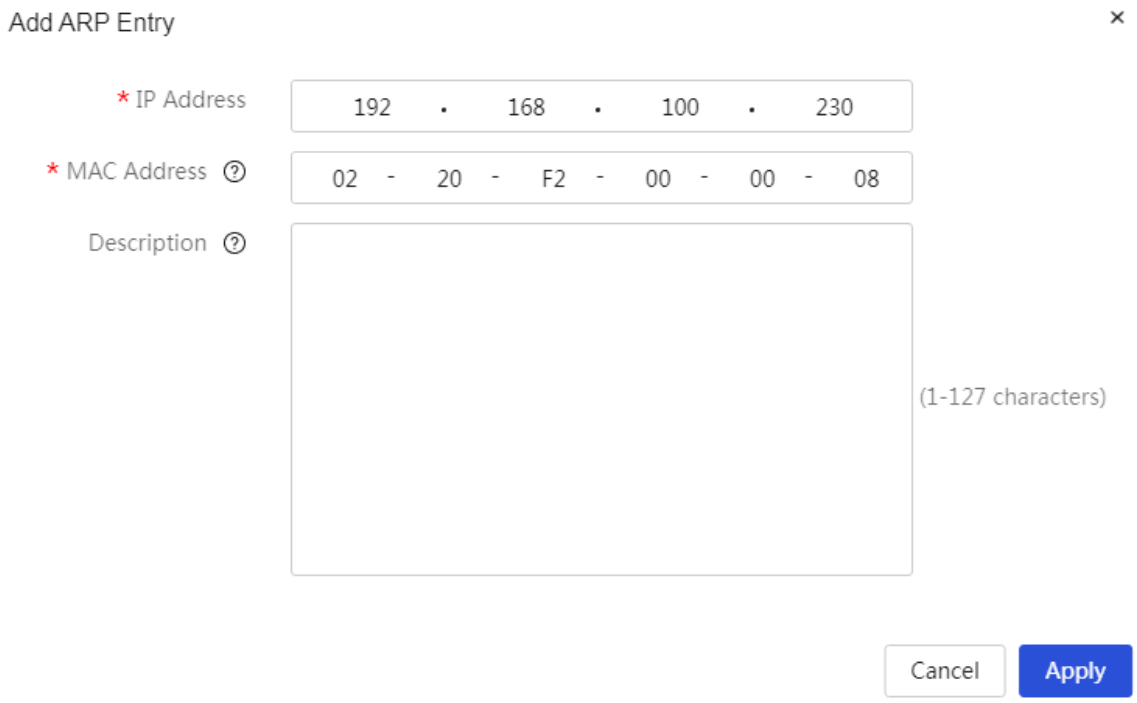


- Select dynamic ARP entries, and then click **Fix** to convert these dynamic ARP entries into static ARP entries.

Manage static ARP entries

1. From the left navigation pane, select **Security** > **ARP Attack Protection**.
2. Click the **Static ARP Entries** tab.
3. To add a single static ARP entry, follow these steps:
4. Click **Add** to open the **Add ARP Entry** dialog box.
   a. Enter the IP address of the static ARP entry.
   b. Enter the MAC address of the static ARP entry.
   c. Enter a description for the static ARP entry.
   d. Click **Apply**.
5. To add static ARP entries in bulk, follow these steps:
   a. Click **Export** download the export template.
   b. Open the downloaded template, add a static ARP entry, and save template file locally.
   c. Click **Import** to open the **Import ARP Entry** dialog box.
   d. Click **Upload file** and then select the edited template.
   e. Click **Apply**.





Configure ARP attack protection

Restrictions and guidelines

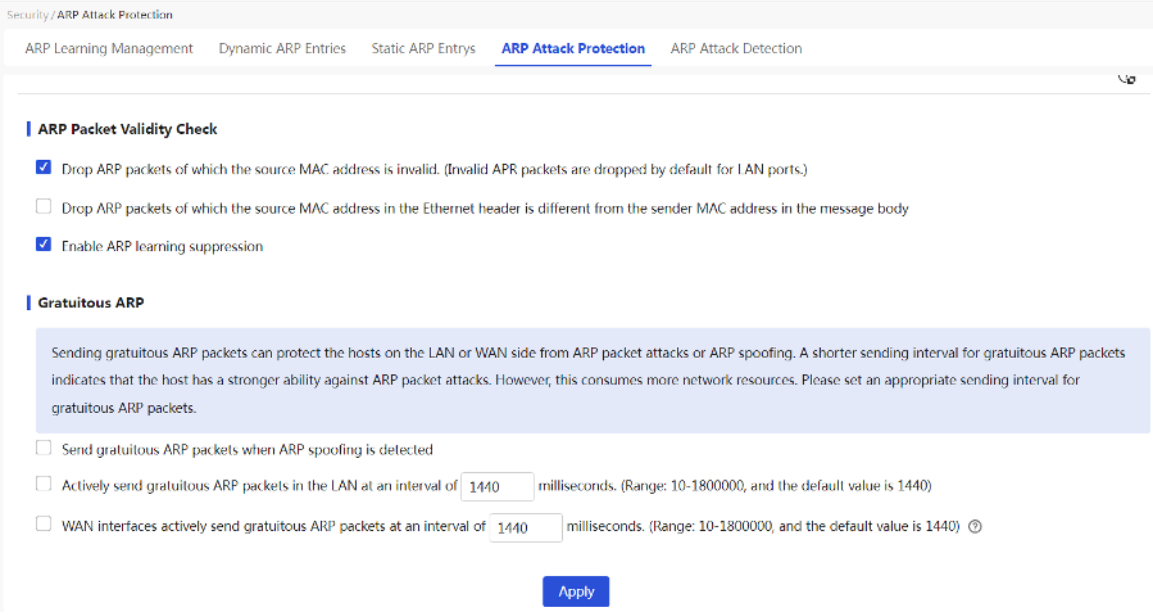
- Sending gratuitous ARP packets from the device can protect hosts on the LAN or WAN side from ARP attacks and spoofing. A smaller gratuitous ARP sending interval can provide stronger ability to prevent ARP attacks, but it will consume more network resources. Set the gratuitous ARP sending interval reasonably.
- Due to possible restrictions on ARP packets by certain devices (such as switches), excessive ARP packets may be deemed as an attack. Enable sending gratuitous ARP with caution and make appropriate parameter settings.
- The device supports scheduled sending of gratuitous ARP packets, which can quickly notify other devices to update ARP entries or MAC address entries to prevent ARP attacks from spoofed gateways and prevent host ARP entry aging.

Procedure

1. From the left navigation pane, select **Security** > **ARP Attack Protection**.
2. Click the **ARP Attack Protection** tab.
3. In the **ARP Packet Validity Check** section, you can make the following settings:
   - **Drop ARP packets of which the source MAC address is invalid. (Invalid ARP packets are dropped by default for LAN ports.)**—If the source MAC address of the ARP packet received by the device is an all-zero, multicast, or broadcast MAC address, the device will not learn this ARP packet and will directly drop it.
   - **Drop ARP packets of which the source MAC address in the Ethernet header is different from the sender MAC address in the message body**—If such an ARP packet is received, the device will not learn this ARP packet and will directly drop it.
   - **Enable ARP learning suppression**—When a device sends an ARP request and receives multiple different ARP reply packets, the device only learns the first received ARP reply.
4. In the **Gratuitous ARP** section, you can make the following settings:

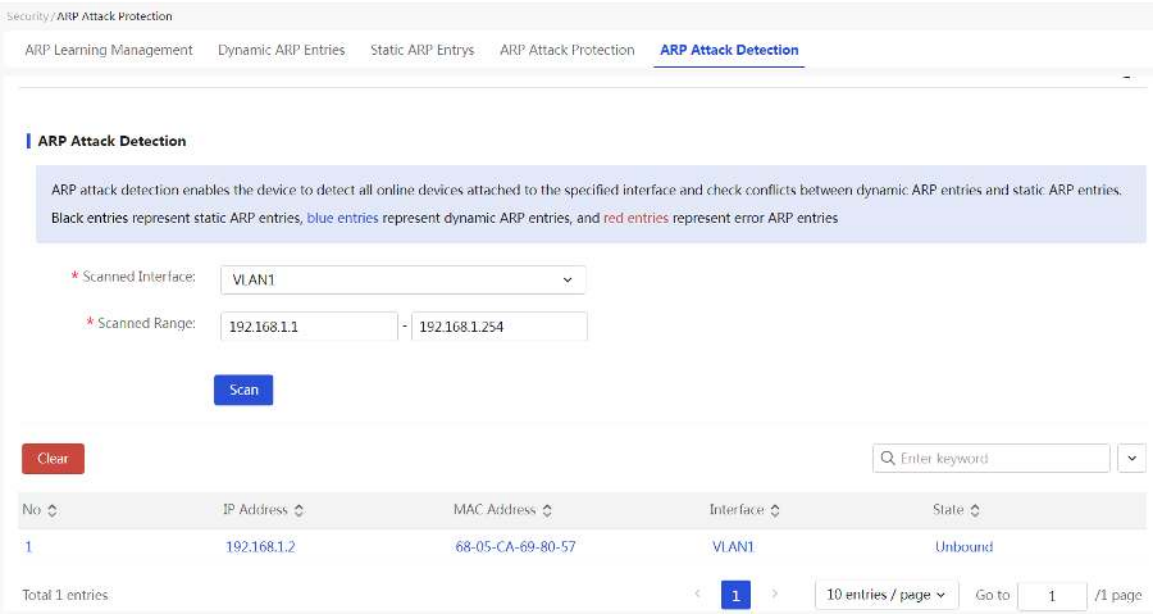
- **Send gratuitous ARP packets when ARP spoofing is detected**—The device sends unsolicited gratuitous ARP packets when it detects ARP spoofing (for example, an ARP packet's source IP address is the device interface IP address but the source MAC address is not the device interface MAC address).
- **Actively send gratuitous ARP packets within the LAN at an interval of *xx* milliseconds**—The device sends unsolicited gratuitous ARP packets within the LAN regularly at the specified interval.
- **WAN interfaces actively send gratuitous ARP packets at an interval of *xx* milliseconds**—WAN interfaces send unsolicited gratuitous ARP packets regularly at the specified interval.

5. Click **Apply**.



Configure ARP attack detection

1. From the left navigation pane, select **Security** > **ARP Attack Protection**.
2. Click the **ARP Attack Detection** tab.
3. Select a scanned interface.
4. Specify the scanned range by entering the start and end IP addresses.
5. Click **Scan** to start the ARP attack detection. The detection results will be displayed in a list, with black entries indicating static ARP entries, blue entries indicating dynamic ARP entries, and red entries indicating error ARP entries. More specifically:
   - **Static ARP entry**—Indicates that this entry is manually configured or automatically bound.
   - **Dynamic ARP entry**—Indicates that this entry is dynamically learned and not automatically bound.
   - **Error ARP entry**: Indicates the existence of an ARP entry conflict.
6. Click **Clear** to clear the current detection results.



Configure DDoS attack prevention

About this feature

DDoS attacks are a type of attack that is widely present on the Internet. They can cause greater harm than traditional DoS attacks. DDoS attack prevention can protect devices from common attack types from both external and internal networks by discarding attack packets. The device can also log corresponding attack events.

- **Attack prevention**: This feature protects devices and networks from the following DDoS attacks:
  - **Single packet attack**—Attackers utilize malformed packets to launch an attack, aiming to disable the target system. For example, the Land attack packet is a TCP packet with both the source IP and destination IP being the target IP. This attack exhausts the target server's connection resources, causing it to be unable to handle normal business.
  - **Abnormal flow attack**—Attackers send a large number of forged requests to the target system, causing the target system to be overwhelmed with useless information, thus unable to provide normal services to legitimate users.
  - **Scanning attack**—Attackers scan host addresses and ports, probe the target network topology and open service ports to prepare for further intrusion into the target system.
- **Attack prevention statistics**: This feature can display statistics for single-packet attack prevention and abnormal flow attack prevention separately, and can export the statistics to an Excel file.
- **Packet source authentication**: This feature enables the device to authenticate the source IP/MAC of received internal network packets to determine if the peer end is a valid host. This is to prevent potential invalid packet attacks within the internal network and avoid the consumption of device and network resources caused by such invalid packets, thus enhancing the overall network stability.
- **Abnormal traffic prevention**: This feature refers to controlling hosts with abnormally large amounts of traffic on the internal network to prevent them from overly occupying bandwidth and consuming system performance. There are three levels of protection, and you can choose the most suitable level based on your actual network condition. To avoid invalid disguised packet

flows being counted as valid host traffic, it is recommended to enable the relevant authentication functions on the packet source authentication page.

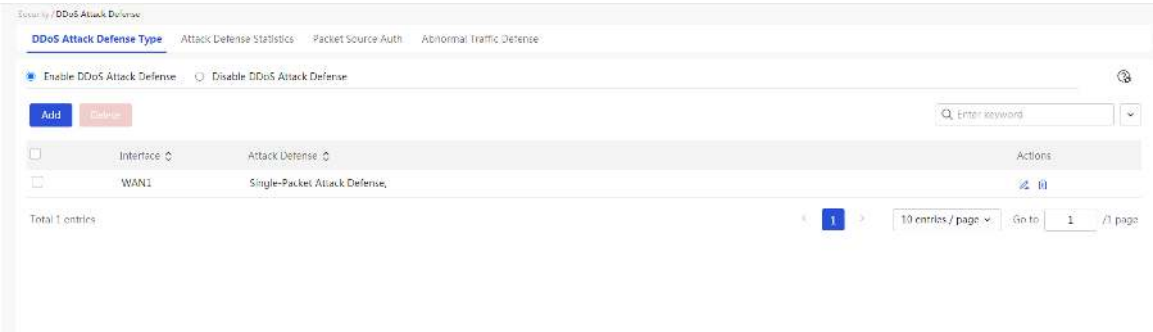
Specify attack prevention types

Restrictions and guidelines

- Enabling the logging feature will reduce the system's ability to resist attacks. Enable logging only if necessary.
- DDoS attack prevention cannot defend L2TP tunnel-encapsulated traffic from the WAN side.
- For WAN interfaces with PPPoE, it is not supported to configure Smurf attack prevention in single-packet attack prevention.

Procedure

1. From the left navigation pane, select **Security** > **DDOS Attack Prevention**.
2. Click the **DDoS Attack Prevention Type** tab.
3. Check the **Enable DDoS Attack Prevention** option to enable the DDoS attack prevention function.

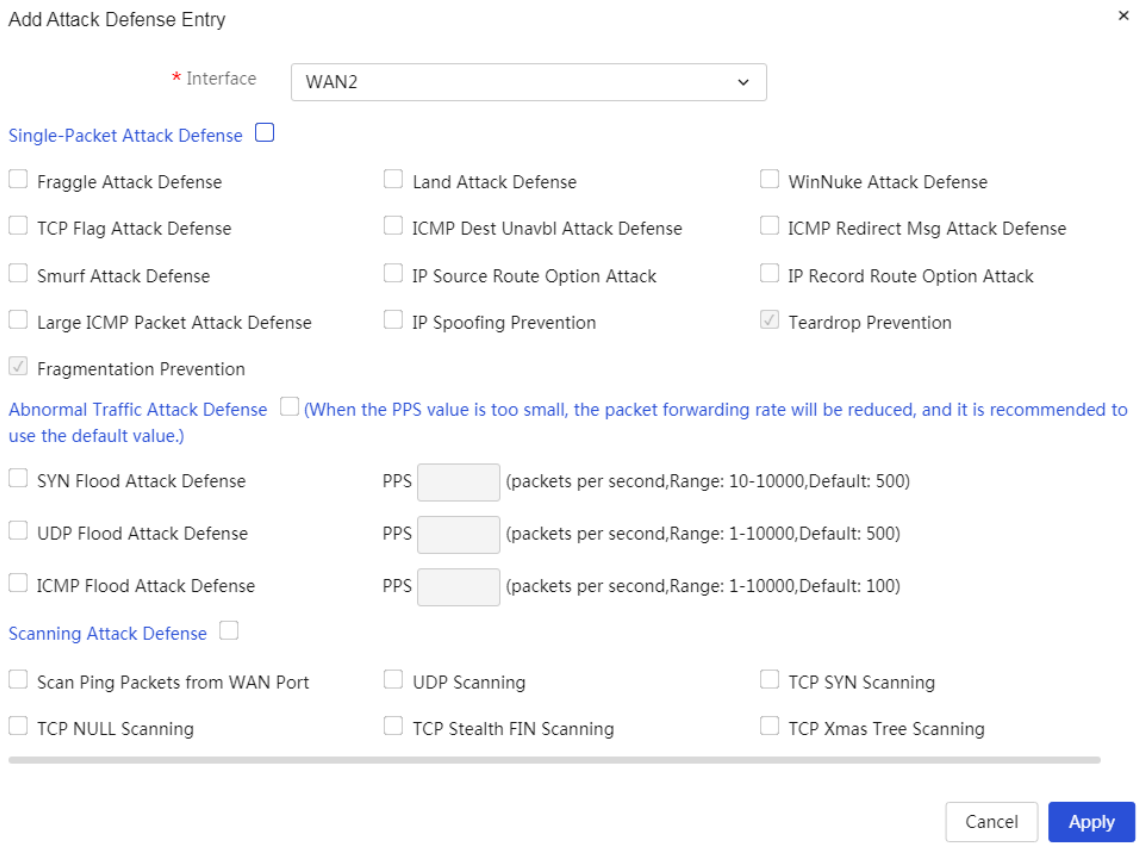


4. Click **Add** to open the dialog for creating a new attack prevention entry.
5. In the **Interface** list, select the interface to which the DDOS attack prevention entry is to be applied.
6. In the **Single-Packet Attack Prevention** section, select the single-packet attack types that need to be enabled for prevention. As a best practice, enable all single-packet attack prevention types.
   - **Fraggle Attack Prevention**: Enabling this option allows the device to effectively prevent Fraggle attacks. This attack involves the attacker sending UDP packets to the subnet broadcast address with the source address as the target network or target host. Each host within the subnet sends response packets to the target network or host, causing network congestion or host crash.
   - **Land Attack Prevention**: Enable this option to effectively prevent Land attacks on the device. This attack involves the attacker sending TCP packets with the SYN flag to the target. The source and destination addresses of these packets are set to the IP address of the target. Upon receiving such packets, the target host initiates repetitive internal response storms, resulting in significant CPU resource consumption.
   - **WinNuke Attack Prevention**: Enable this option to effectively prevent WinNuke attacks. This attack involves attackers exploiting the Out of Band (OOB) vulnerability in the NetBIOS protocol to the target and cause certain hosts to crash or blue screen.
   - **TCP Flag Attack Prevention**: Enabling this option allows the device to effectively prevent TCP flag attacks. This attack involves the attacker sending packets with non-standard TCP flags to probe the target host's operating system type. If the operating system handles such packets improperly, the attacker can achieve the goal of crashing the target host system.

- **ICMP Dest Unavbl Attack Prevention**: Enable this option to effectively prevent ICMP unreachable message attacks. This attack involves the attacker sending ICMP unreachable messages to the target, effectively disconnecting the target host from the network.
- **ICMP Redirect Msg Attack Prevention**: Enabling this option allows the device to effectively prevent ICMP Redirect message attacks. This attack involves the attacker sending ICMP Redirect messages to the target, altering the target's routing table and disrupting the normal forwarding of IP packets.
- **Smurf Attack Prevention**: Enabling this option allows the device to effectively prevent Smurf attacks. The attack is similar to Fraggle attack. It involves an attacker broadcasting an ICMP echo request (ICMP ECHO REQUEST) message to a network segment, with the source address being the targeted host. When all hosts in the segment receive the echo request, they will respond to the targeted host with ICMP ECHO REPLY messages, causing network blockage or system crash.
- **IP Source Route Option Attack Prevention**: Enabling this option allows the device to effectively prevent IP attacks with source route options. This attack involves the attacker sending IP packets with source route options to the target, aiming to explore the network structure.
- **IP Record Route Option Attack Prevention**: Enabling this option allows the device to effectively prevent IP attacks with record route options. This attack involves the attacker sending IP packets with record route options to the target, achieving the goal of probing the network structure.
- **Large ICMP Packet Attack Prevention**—Enable this option to defend against large ICMP packet attacks. This attack involves the attacker sending oversized ICMP packets to the target host, causing it to crash.
- **IP Spoofing Prevention**: Enabling this option allows the device to effectively prevent IP Spoofing attacks. This attack involves the attacker sending IP packets with a modified source IP address to pretend to be a valid host, and accessing critical information. The attacker usually modify the source address to an IP within the LAN.
- **TearDrop Prevention**: Enable this option to effectively prevent TearDrop attacks. This option is enabled by default and cannot be disabled. This attack involves the attacker sending overlapping fragmented packets to the target host, which may cause system crashes when processing such fragments.
- **Fragmentation Prevention**: Enable this option to effectively prevent fragment packet attacks. This option is enabled by default and cannot be disabled. This attack involves the attacker sending partial fragments of packets to the target host without sending all the fragments. As a result, the target host will wait indefinitely until the timer expires. If the attacker sends a large number of fragmented packets, it will exhaust the resources of the target host, causing it to be unable to respond to normal IP packets.

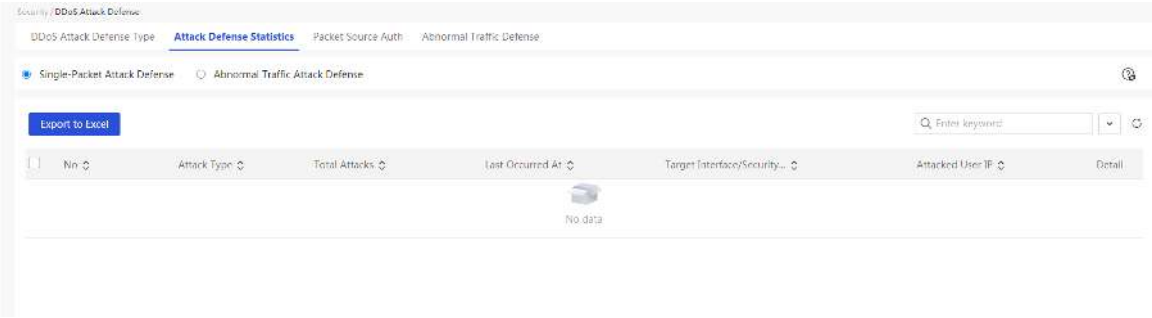
7. In the **Abnormal Traffic Attack Prevention** section, select the types of abnormal traffic attacks to enable.
   - **SYN Flood Attack Prevention**: Select this option and set the threshold for preventing SYN Flood attacks. When the traffic rate exceeds this threshold, the device will enable SYN Flood attack prevention. This attack involves the attacker sending a large number of SYN packets to the target, depleting the target's connection resources and rendering the target system unable to accept new connections.
   - **UDP Flood Attack Prevention**: Select this option and set the threshold for preventing UDP Flood attacks. When the traffic rate exceeds this threshold, the device will enable UDP Flood attack prevention. This attack involves the attacker sending a large number of UDP packets to the target, causing the target host to be overwhelmed with processing these UDP packets and unable to continue processing normal packets.
   - **ICMP Flood Attack Prevention**: Select this option and set the threshold for preventing ICMP Flood attacks. When the traffic rate exceeds this threshold, the device will enable ICMP Flood attack prevention. This attack involves the attacker sending a large number of ICMP packets to the target, causing the target host to be overwhelmed with processing these ICMP packets and unable to continue processing normal packets.

8. In the **Scanning Attack Prevention** section, select the scanning attack types that need to be enabled for prevention.
   - **Scan Ping Packets from WAN Port**: Enabling this option prevents the device from responding to Ping requests from the Internet, protecting against malicious Ping probes.
   - **UDP Scanning**: Enabling this option allows the device to effectively prevent UDP scanning attacks. This attack involves the attacker sending UDP packets to the target port to determine if the port is open.
   - **TCP SYN Scanning**: Enabling this option allows the device to effectively prevent TCP SYN scanning attacks. This attack involves the attacker sending SYN packets to the target port as if establishing a normal TCP connection, then waiting for the target host's response to determine if the port is open.
   - **TCP NULL Scanning**: Enabling this option allows the device to effectively prevent TCP NULL scanning. This attack characterized by the attacker sending TCP packets to the target port with all flags unset, and then waiting for a response from the target host to determine if the port is open.
   - **TCP Stealth FIN Scanning**: Enabling this option allows the device to effectively prevent TCP Stealth FIN scans. This attack involves the attacker sending TCP packets to the target port with only the FIN flag set, then waiting for a response from the target host to determine if the port is open.
   - **TCP Xmas Tree Scanning**: Enabling this option allows the device to effectively prevent TCP Xmas Tree scanning. This attack involves the attacker sending TCP packets with the FIN, URG, and PUSH flags set to the target port, and then waiting for a response from the target host to determine if the port is open.
9. Click **Apply**.



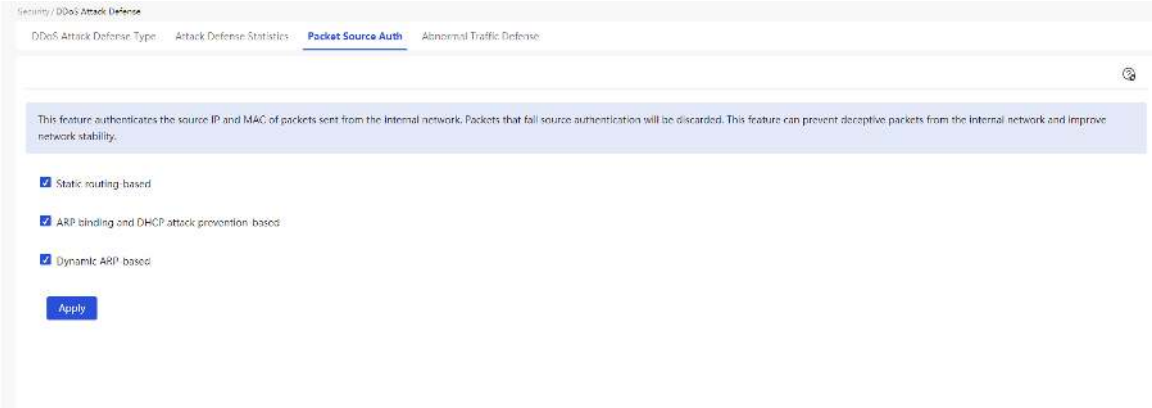
View attack prevention statistics

1. From the left navigation pane, select **Security** > **DDOS Attack Prevention**.
2. Click the **Attack Prevention Statistics** tab.
3. Select the **Single-Packet Attack Prevention** option to display statistics for single-packet attack prevention in a list.
4. Select the **Abnormal Traffic Attack Prevention** option to display statistics for abnormal traffic attack prevention in a list.
5. Click the **Export to Excel** button to export the statistics of attack prevention to an Excel file for saving.



Configure packet source authentication

1. From the left navigation pane, select **Security** > **DDOS Attack Prevention**.
2. Click the **Packet Source Auth** tab.
3. Set the following parameters according to your needs:
   - **Static routing-based**—After enabling this function, the device allows the following traffic coming from an internal device to pass through: traffic of which the source IP belongs to the same network segment as the LAN interface; or traffic coming from an internal device which is accessible via the static route with the outgoing interface as the LAN interface. Data packets from other network segments will be discarded by the device.
   - **ARP binding and DHCP attack prevention-based**—After enabling this function, the device will authenticate incoming packets from the internal network based on the static binding entries in the ARP binding table and the corresponding entries in the DHCP allocation list. If there is a conflict between the source IP/MAC of a packet and the IP/MAC in the ARP binding table, the device will discard the packet.
   - **Dynamic ARP-based**—After enabling this function, the device will intelligently authenticate the source IP/MAC of the internal network data packet, determining whether the peer end is an existing legitimate host. If the source IP/MAC of the data packet conflicts with the IP/MAC of a confirmed legitimate host, the device will discard the data packet. If there are applications in the network with the same MAC address but different IP addresses, bind the corresponding IP/MAC addresses statically to ARP to ensure normal service access.
4. Click **Apply**.



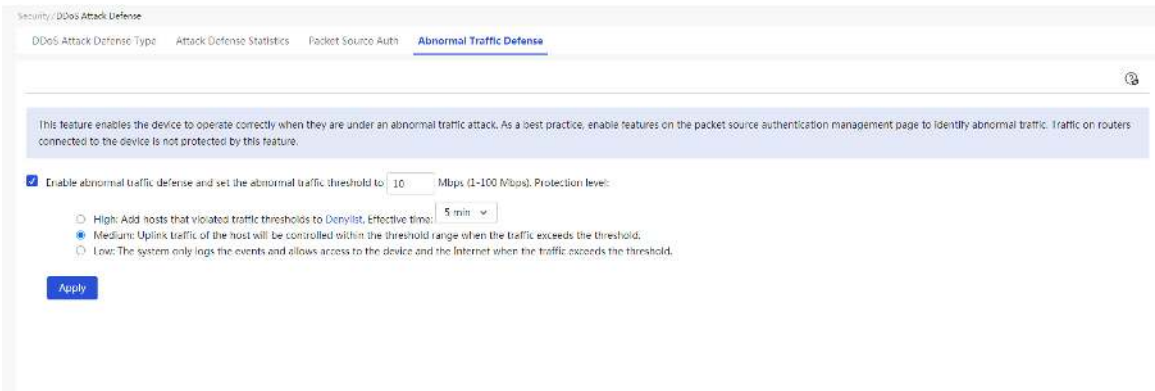
Configure abnormal traffic prevention

Restrictions and guidelines

When the abnormal traffic prevention feature is enabled and the protection level is set to high, detected abnormal hosts will be automatically added to the denylist. If the protection level is lowered or the abnormal traffic prevention feature is turned off, the abnormal hosts that have been added to the denylist will be removed from the denylist.

Procedure

1. From the left navigation pane, select **Security** > **DDOS Attack Prevention**.
2. Click the **Abnormal Traffic Prevention** tab.
3. Select the **Enable abnormal traffic prevention and set the abnormal traffic threshold to xxx Mpbs** option.
4. Select a protection level as needed:
   - **High**— At high protection level, the device will detect abnormal host traffic, and automatically add an attacking host detected to the denylist. Within the specified effective time period, this host is not allowed to access the device and the Internet, so as to minimize the impact of this abnormal host on the network.
   - **Medium**— At medium protection level, the device will limit the uplink traffic of a single internal network host under the abnormal traffic threshold. Traffic exceeding the threshold will be discarded by the device.
   - **Low**— At low protection level, the device only logs abnormal traffic from a host and still allows the host to access the device and the Internet.
5. Click **Apply**.



Configure security statistics

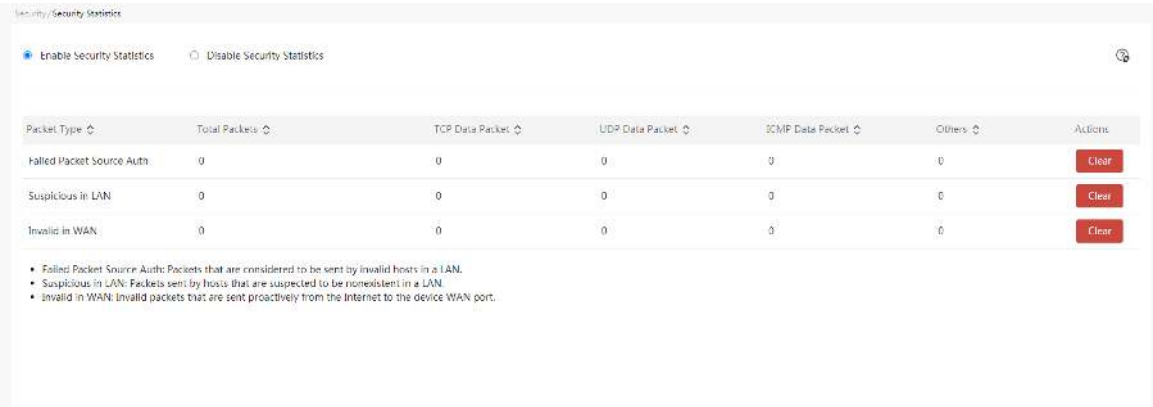
About this feature

The security statistics feature is used to count the invalid or suspicious data packets received by the device, helping identify deception or attack behaviors in the network. This feature supports the statistics of the following types of data packets:

- **Failed Packet Source Auth**—Data packets failed packet source authentication, that is, data packets sent from illegal hosts in the LAN network. To count this type of data packet, you need to enable the relevant source packet authentication functions first.
- **Suspicious in LAN side**—Data packets sent by hosts in the LAN network whose authenticity cannot be confirmed.
- **Invalid in WAN**—Invalid data packets sent by the Internet side to the WAN interface of the device.

Procedure

1. From the left navigation pane, select **Security** > **Security Statistics**.
2. Select the **Enable Security Statistics** option to display security statistical information in the list.
3. Click the **Clear** button in the **Actions** column for a packet type to clear the statistics for that packet type.
4. In the dialog box that opens, click **Apply**.



Manage denylist

About this feature

The denylist management feature is used to view and remove users that have been added to the denylist.

Procedure

1. From the left navigation pane, select **Security** > **Denylist**.
2. Click the icon in the **Actions** column for a user in the list to remove the user from the denylist.

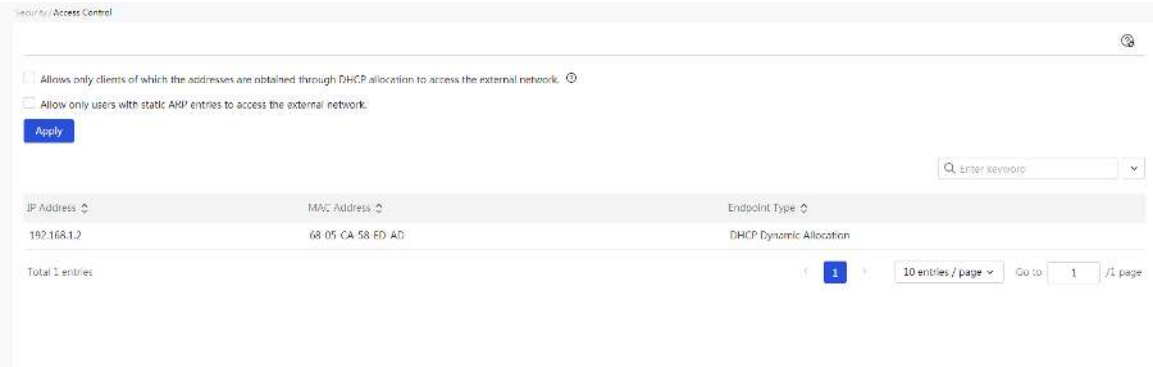
Configure access control

About this feature

The access control feature can simultaneously match the source MAC address and source IP address in data packets. Only the endpoints that have both the MAC address and IP address matched are allowed to access the external network.

Procedure

1. From the left navigation pane, select **Security** > **Access Control**.
2. Set the following rules as needed:
   - **Allows only clients of which the addresses are obtained through DHCP allocation to access the external network—**Only clients with IP addresses assigned by the DHCP server can access the external network. Clients not in the DHCP server's assigned client list will be unable to access the external network. If you cannot access the external network after enabling this feature, configure the management PC to obtain an IP address through DHCP.
   - **Allows only users with static ARP entries to access the external network**—Only clients in the ARP static binding table are allowed to access the external network. Clients not in the ARP static binding table will be unable to access the external network. Note that before enabling this feature, add the IP or MAC address of the management PC to the ARP static binding table. Otherwise, after enabling this feature, the management PC will not be able to access the external network.
3. Click **Apply**.



Configure VPNs

Configuration tasks at a glance

Set up an IPsec VPN

When setting up an IPsec VPN, you must configure devices on both ends.

To set up an IPsec VPN, perform the following tasks:

Task	Remarks
(Optional.) Configure VLANs	Modify the IP address of VLAN-interface 1 or create a new VLAN.
(Required.) Configure WAN settings	Connect the WAN interfaces to the Internet and complete WAN configuration.
(Required.) Configure an IPsec branch node or Configure an IPsec HQ node	Add an IPsec policy as needed.

Set up an L2TP VPN

When setting up an L2TP VPN, you must configure devices on both ends. Configure one end as an L2TP server and the other end as an L2TP client.

To set up an L2TP VPN, perform the following tasks:

Task	Remarks
(Required.) Configure WAN settings	Connect the WAN interfaces to the Internet and complete WAN configuration.
(Required.) Configure L2TP settings or "Configure L2TP users	Enable the L2TP server and create L2TP groups and add L2TP users as needed.
(Required.) Configure L2TP settings	Enable the L2TP client and create new L2TP groups as needed.

Set up an IPsec VPN

About this feature

IPsec VPN is a virtual private network established by using IPsec technology. IPsec protects user data transmitted between specific communication parties by establishing a tunnel known as an IPsec tunnel.

The IPsec protocol provides a comprehensive security architecture for network data security at the IP layer, including Authentication Header (AH), Encapsulating Security Payload (ESP), Internet Key Exchange (IKE), and algorithms for network authentication and encryption. Among them, the AH protocol and ESP protocol provide security services, and the IKE protocol is used for key exchange.

Two IPsec VPN networking modes are supported on the device:

- **HQ-branch network**—The enterprise branch gateways will actively establish IPsec tunnels to the HQ gateway, allowing internal endpoints in branches to securely access the HQ network resources.
- **Branch-branch network**—IPsec tunnels can be established between each enterprise branch gateway to protect data communication between branches.

Configure an IPsec branch node

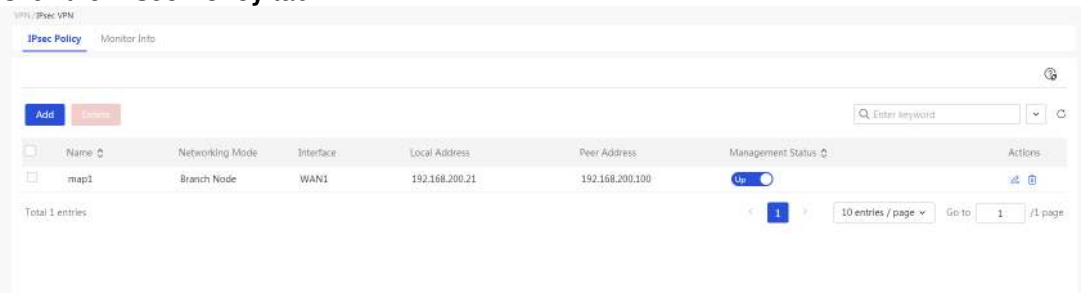
About this task

In the branch-branch network, devices can proactively establish IPsec tunnels between them.

Procedure

Configure basic IPsec settings

1. From the left navigation pane, select **VPN** > **IPsec VPN**.
2. Click the **IPsec Policy** tab.



3. Click **Add**.
4. In the **Name** field, enter an IPsec policy name.
5. From the **Interface** list, select an interface to which the IPsec policy applies.

   Make sure this interface can reach the peer device at Layer 3.
6. In the **Networking Mode** field, select **Branch Node**.
7. In the **Peer Gateway Address** field, enter the IP address or domain name of the peer end of the IPsec policy.

   Typically, enter the WAN interface address of the HQ gateway or the peer branch gateway.
8. From the **Auth Method** list, select an IPsec tunnel authentication method.

   This parameter only supports the preshared key authentication in the current software version.
9. In the **Preshared Key** field, enter the same preshared key as that on the peer device.

   The key must be negotiated and advertised in advance.
10. In the **Traffic Protection Rules** area, perform the following tasks:
    a. From the **Protocol** list, select the protocol type for the packets protected by the IPsec tunnel.
    b. In the **Local Subnet/Mask** field, enter the local protected subnet.
    c. In the **Local Port** field, enter the local protected port.

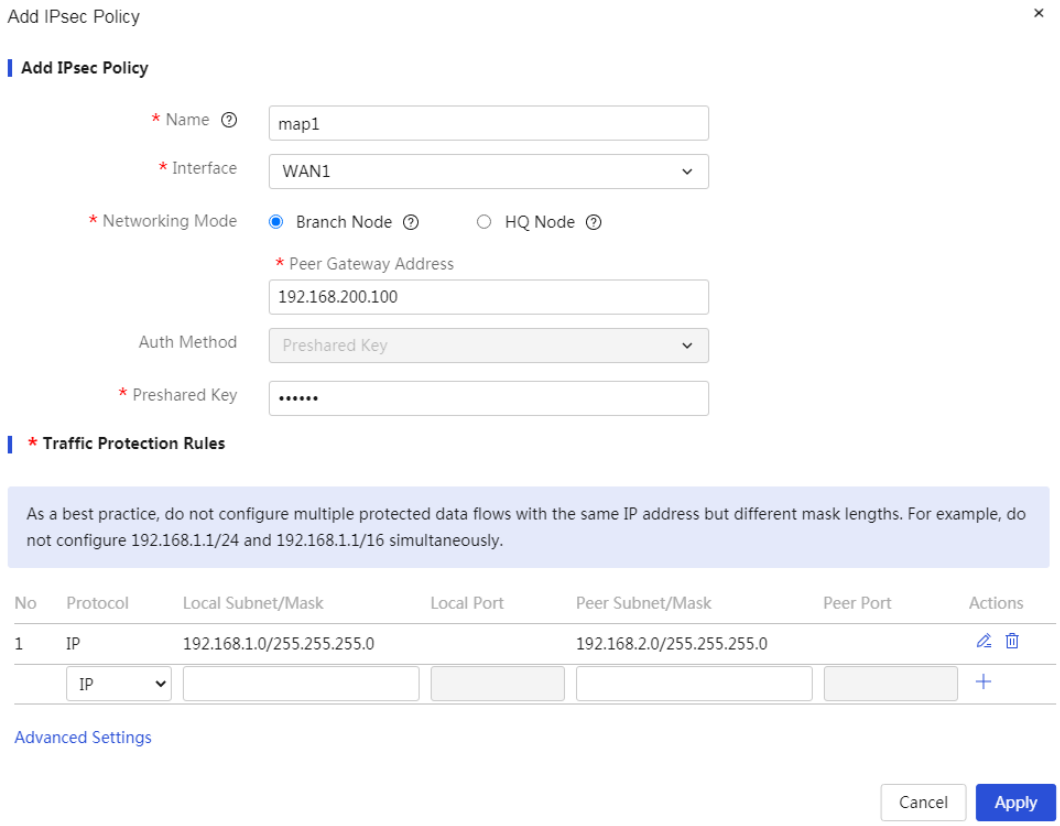
       This parameter is supported only when the protected protocol is TCP or UDP.

       The packets sent by the protected port of hosts in the local protected subnet will be encapsulated in IPsec tunnel mode by the device.
    d. In the **Peer Subnet/Mask** field, enter the peer protected subnet.
    e. In the **Peer Port** field, enter the peer protected port.

This parameter is supported only when the protected protocol is TCP or UDP.

Only the packets sent by the protected port of hosts in the peer protected subnet can be decapsulated in IPsec tunnel mode by the device.

f. To add multiple protected flows, click the icon in the **Actions** column.



Configuring advanced IKE settings

To change the default IKE settings of the device, perform the following tasks.

1. Complete basic IPsec settings as described above.
2. Click **Advanced Settings**.
3. Click the **IKE Settings** tab.
4. From the **IKE Version** list, select an IKE version.
5. From the **Negotiation Mode** list, select an IKE negotiation mode.
   - **Main**—This mode involves more negotiation steps. In this mode, identity authentication occurs after the key exchange process. This mode is suitable for scenarios with higher identity protection requirements.
   - **Aggressive**—This mode involves fewer negotiation steps. In this mode, identity authentication and key exchange are performed simultaneously. This mode is suitable for scenarios with low identity protection requirements.

   When the IKE version is V1, this parameter can be configured. If the device's public IP address is dynamically allocated, select the aggressive mode as the IKE negotiation mode as a best practice.
6. In the **Local ID** field, configure the local device ID type and the ID for IKE authentication.

   ID types include IP address, FQDN, and user FQDN. This parameter must be consistent with the peer ID type and ID configured in step 7 on the peer device.

   If you have selected the main mode as the IKE negotiation mode in step 5, you must configure the local device ID type as IP address.

7. In the **Peer ID** field, configure the peer device ID type and the ID for IKE authentication.

   ID types include IP address, FQDN, and user FQDN. This parameter must be consistent with the local ID type and ID configured in step 6 on the peer device.

8. In the **Dead Peer Detection** field, select whether to enable dead peer detection (DPD).

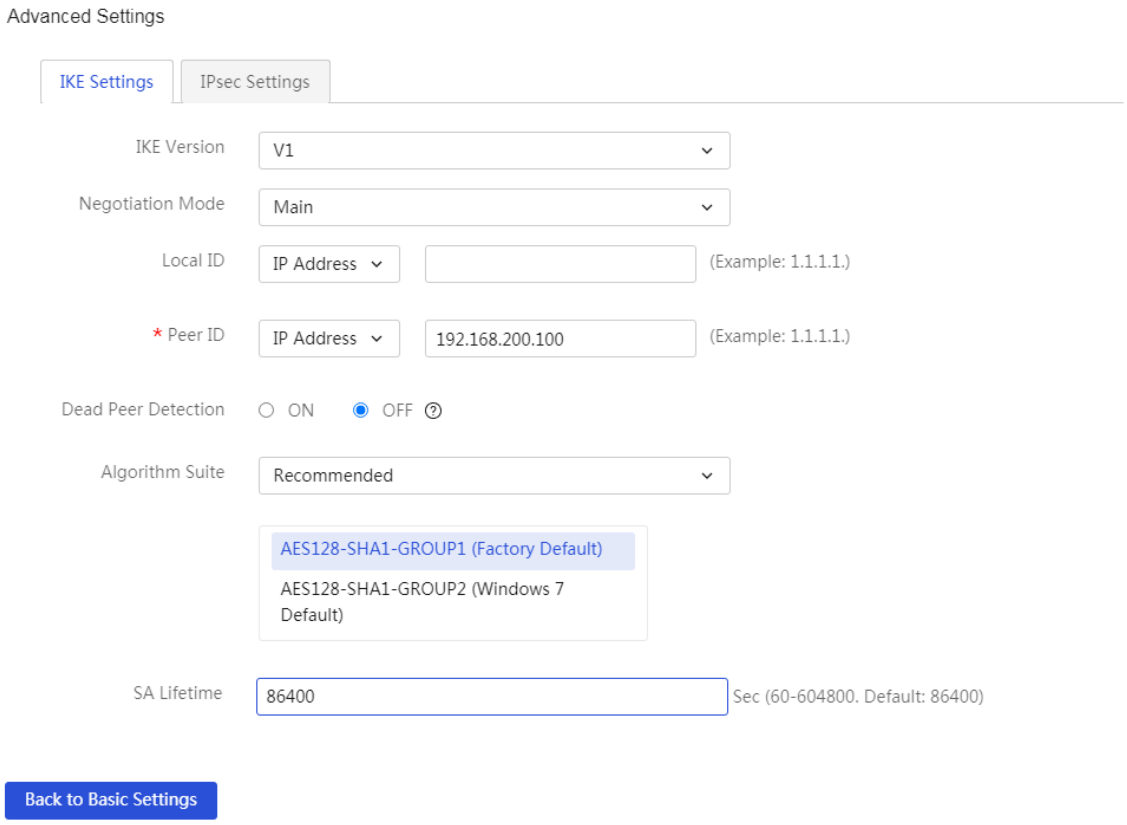
   This feature detects whether the peer is alive, and the device will tear down the IPsec tunnel if the peer is inactive. As a best practice, enable this feature so that the device can promptly obtain the availability of the IPsec tunnel.

9. From the **Algorithm Suite** list, select the encryption and authentication algorithms required for IKE protocol interaction.
   - If the **Recommended** option is selected, you must select a recommended algorithm suite.
   - If the **Custom** option is selected, you must set custom authentication algorithm, encryption algorithm, and PFS algorithm.

   The authentication algorithm, encryption algorithm, and PFS algorithm must be consistent at both ends of the IPsec tunnel.

10. In the **SA Lifetime** field, enter the time interval for IKE re-negotiation.

    When the configured time expires, the re-negotiation of IKE-related parameters will be triggered. As a best practice, set the SA lifetime to no less than 600 seconds.



Configure advanced IPsec settings

To change the default advanced IPsec settings of the device, perform the following tasks.

1. Complete basic IPsec settings as described above.
2. Click the **IPsec Settings** tab.
3. From the **Algorithm Suite** list, select the security protocol and the corresponding encryption and authentication algorithms for the IPsec protocol interaction.
   - If the **Recommended** option is selected, you must select a recommended algorithm suite.

- If the **Custom** option is selected, you must set the custom security protocol, ESP authentication algorithm, and ESP encryption algorithm.

The security protocol, authentication algorithm, encryption algorithm, encapsulation mode, and PFS algorithm must be consistent at both ends of the IPsec tunnel.

4. In the **Encapsulation Mode** field, select an IPsec tunnel encapsulation mode.

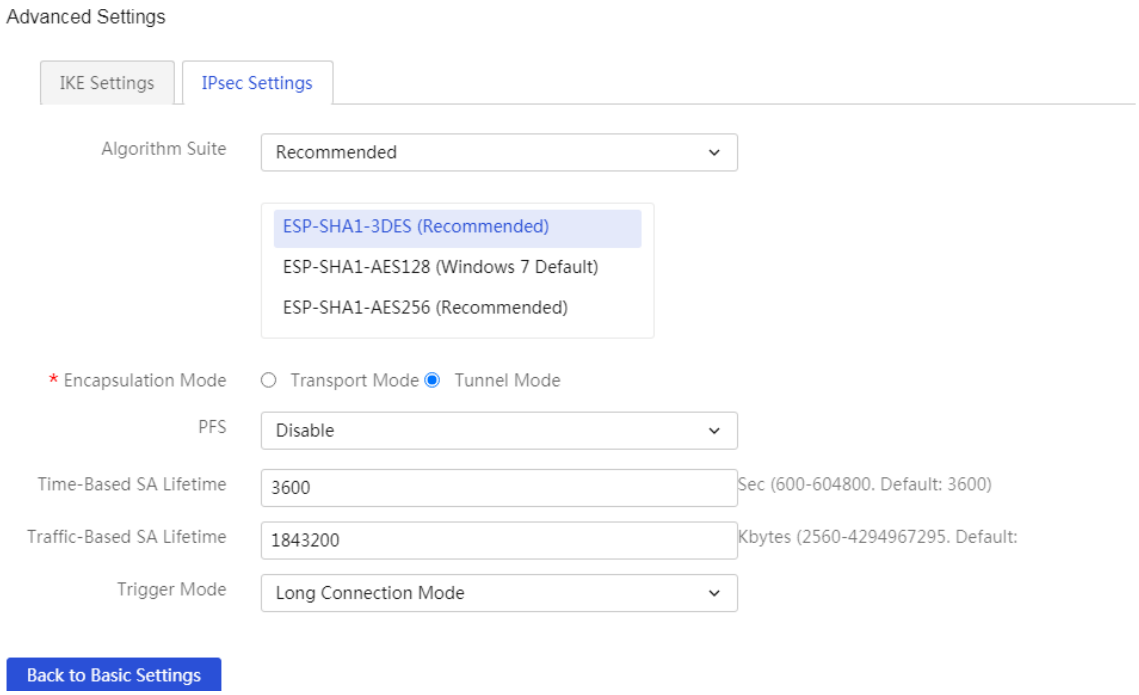
   If the protected subnets at both ends of the IPsec tunnel are private subnets, select the tunnel mode as a best practice.

   The encapsulation mode must be consistent at both ends of the IPsec tunnel.
5. From the **PFS** list, select the PFC algorithm for the IPsec tunnel.

   The PFS algorithm must be consistent at both ends of the IPsec tunnel.
6. In the **Time-Based SA Lifetime** field, enter the time interval for triggering IPsec re-negotiation.

   If the configured time expires, the re-negotiation of IPsec-related parameters will be triggered.
7. In the **Traffic-Based SA Lifetime** field, enter the traffic size for triggering IPsec re-negotiation.

   If the configured traffic size is exceeded, the renegotiation of IPsec-related parameters will be triggered.
8. From the **Trigger Mode** list, select the mode of triggering IPsec re-negotiation.
9. Click **Back to Basic Settings** to return to the **Add IPsec Policy** page.
10. Click **Apply**.



Configure an IPsec HQ node

About this task

In the HQ-branch network, branch nodes must proactively establish IPsec tunnels to the HQ node for communication.

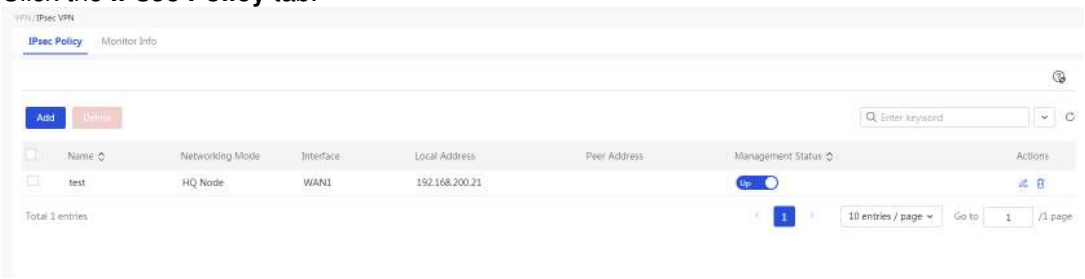
Restrictions and guidelines

When the device acts as the HQ node, only one HQ node policy can be configured on an interface. When selecting an interface for adding an IPsec HQ node policy, make sure the interface has not been configured with an HQ node policy.

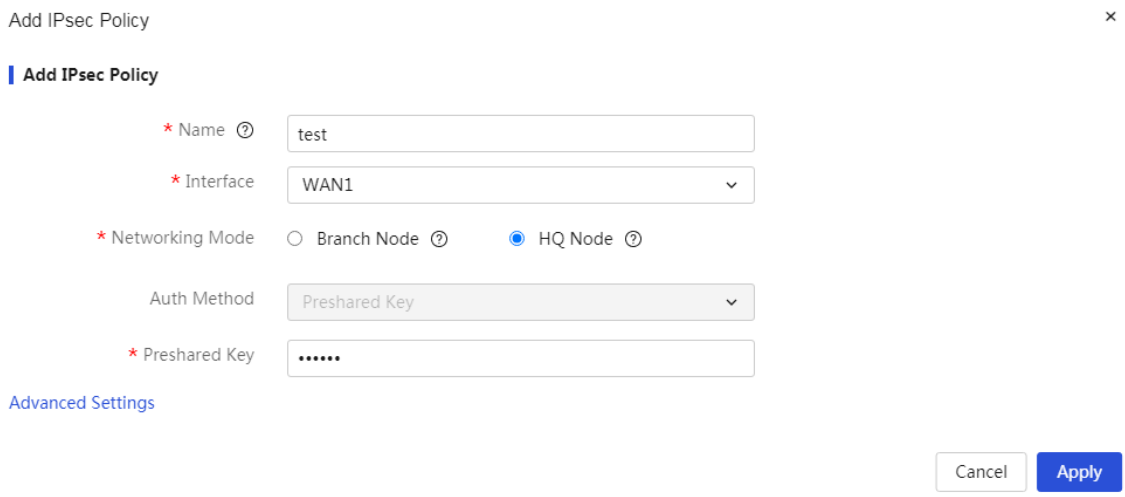
Procedure

Configure basic IPsec settings

1. From the left navigation pane, select **VPN** > **IPsec VPN**.
2. Click the **IPsec Policy** tab.



3. Click **Add**.
4. In the **Name** field, enter an IPsec policy name.
5. From the **Interface** list, select an interface to which the IPsec policy applies.
   Make sure this interface can reach the branch node device at Layer 3.
6. In the **Networking Mode** field, select **HQ Node**.
7. In the **Preshared Key** field, enter the same preshared key as that on the peer device.
   The key must be negotiated and advertised in advance.



Configure IKE settings

To change the default IKE settings of the device, perform the following tasks.

1. Complete basic IPsec settings as described above.
2. Click **Advanced Settings**.
3. Click the **IKE Settings** tab.
4. From the **IKE Version** list, select an IKE version.
5. From the **Negotiation Mode** list, select an IKE negotiation mode.

- **Main**—This mode involves more negotiation steps. In this mode, identity authentication occurs after the key exchange process. This mode is suitable for scenarios with higher identity protection requirements.
- **Aggressive**—This mode involves fewer negotiation steps. In this mode, identity authentication and key exchange are performed simultaneously. This mode is suitable for scenarios with low identity protection requirements.

When the IKE version is V1, this parameter can be configured. If the device's public IP address is dynamically allocated, select the aggressive mode as the IKE negotiation mode as a best practice.

6. In the **Local ID** field, configure the local device ID type and the ID for IKE authentication.

   ID types include IP address, FQDN, and user FQDN. This parameter must be consistent with the peer ID type and ID configured on the branch node device.

   If you have selected the main mode as the IKE negotiation mode in step 5, you must configure the local device ID type as IP address.

7. In the **Dead Peer Detection** field, select whether to enable dead peer detection (DPD).

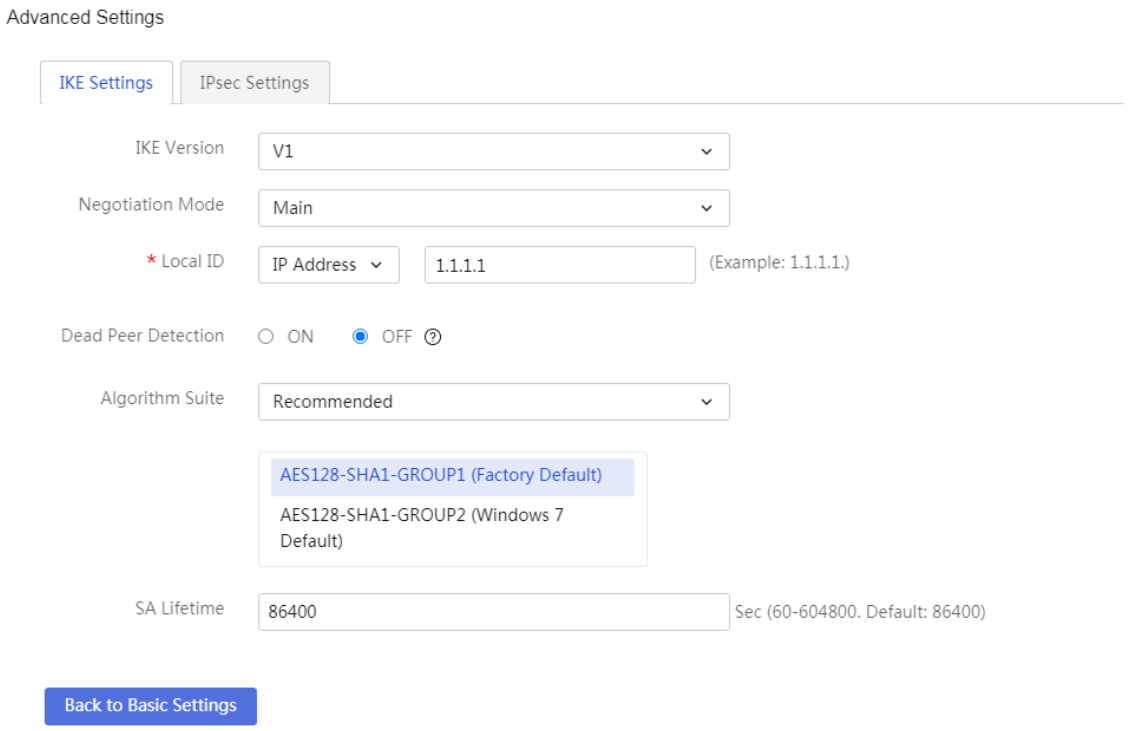
   This feature detects whether the peer is alive, and the device will tear down the IPsec tunnel if the peer is inactive. As a best practice, enable this feature so that the device can promptly obtain the availability of the IPsec tunnel.

8. From the **Algorithm Suite** list, select the encryption and authentication algorithms required for IKE protocol interaction.
   - If the **Recommended** option is selected, you must select a recommended algorithm suite.
   - If the **Custom** option is selected, you must set custom authentication algorithm, encryption algorithm, and PFS algorithm.

   The authentication algorithm, encryption algorithm, and PFS algorithm must be consistent at both ends of the IPsec tunnel.

9. In the **SA Lifetime** field, enter the time interval for IKE re-negotiation.

   When the configured time expires, the re-negotiation of IKE-related parameters will be triggered. As a best practice, set the SA lifetime to no less than 600 seconds.



Configure advanced IPsec settings

To change the default advanced IPsec settings of the device, perform the following tasks.

1. Complete basic IPsec settings as described above.
2. Click the **IPsec Settings** tab.
3. From the **Algorithm Suite** list, select the security protocol and the corresponding encryption and authentication algorithms for the IPsec protocol interaction.
   - If the **Recommended** option is selected, you must select a recommended algorithm suite.
   - If the **Custom** option is selected, you must set the custom security protocol, ESP authentication algorithm, and ESP encryption algorithm.

   The security protocol, ESP authentication algorithm, and ESP encryption algorithm must be consistent at both ends of the IPsec tunnel.
4. In the **Encapsulation Mode** field, select an IPsec tunnel encapsulation mode.

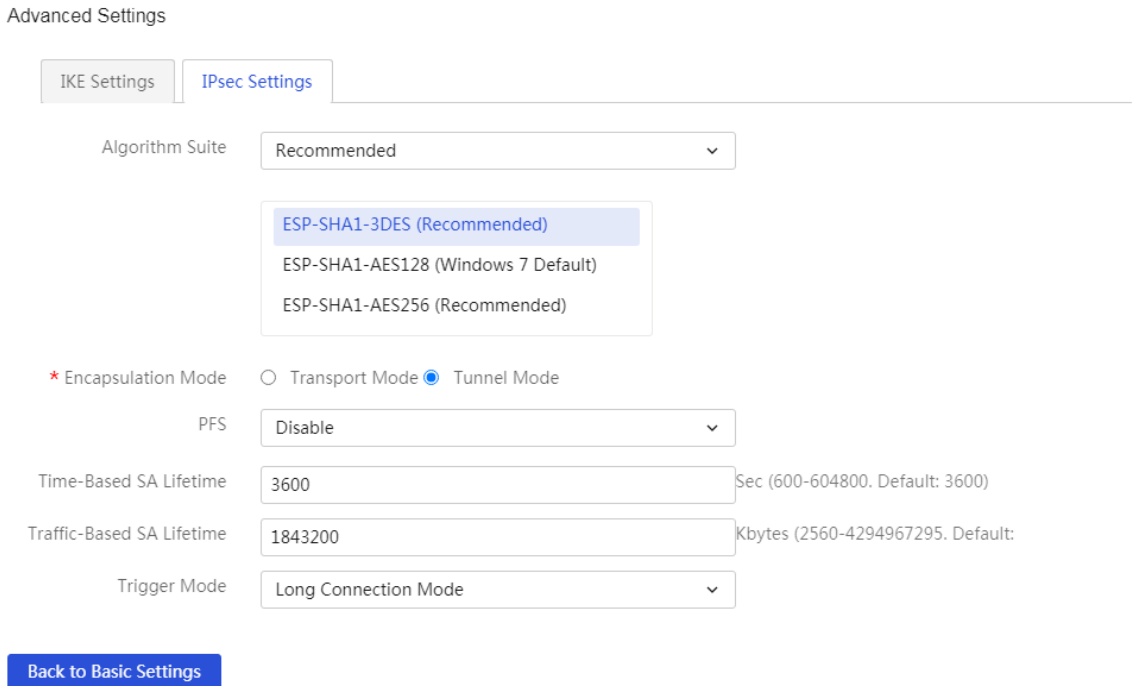
   If the protected subnets at both ends of the IPsec tunnel are private subnets, select the tunnel mode as a best practice.

   The encapsulation mode must be consistent at both ends of the IPsec tunnel.
5. From the **PFS** list, select the PFC algorithm for the IPsec tunnel.

   The PFS algorithm must be consistent at both ends of the IPsec tunnel.
6. In the **Time-Based SA Lifetime** field, enter the time interval for triggering IPsec re-negotiation.

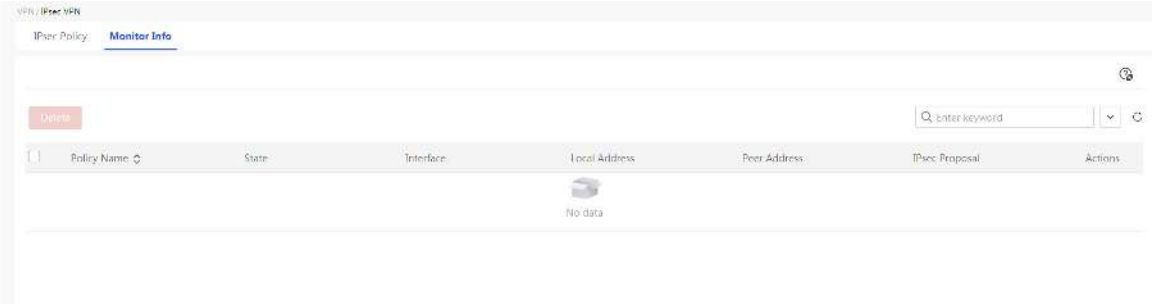
   If the configured time expires, the re-negotiation of IPsec-related parameters will be triggered.
7. In the **Traffic-Based SA Lifetime** field, enter the traffic size for triggering IPsec re-negotiation.

   If the configured traffic size is exceeded, the renegotiation of IPsec-related parameters will be triggered.
8. From the **Trigger Mode** list, select the mode of triggering IPsec re-negotiation.
9. Click **Back to Basic Settings** to return to the **Add IPsec Policy** page.
10. Click **Apply**.



View monitor information

1. From the left navigation pane, select **VPN** > **IPsec VPN**.
2. Click the **Monitor Info** tab.



Configure an L2TP server

About this feature

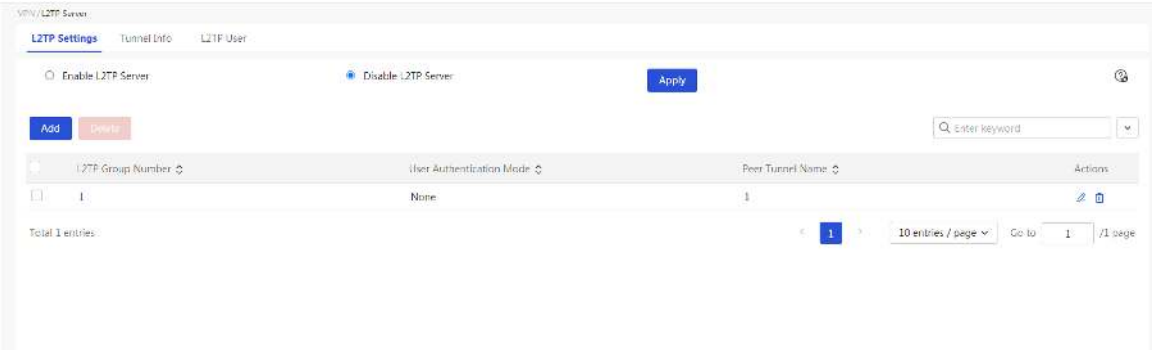
Perform this task to configure basic L2TP server parameters and enable L2TP.

To provide a secure, cost-effective solution for remote users (such as branches and travelers) of an enterprise to access resources in the internal network of the enterprise, configure an L2TP server.

An L2TP server is a device that can process PPP and L2TP protocol packets. Typically, an L2TP server is located at the edge of the internal network of an enterprise.

Configure L2TP settings

1. From the left navigation pane, select **VPN > L2TP Server**.
2. Click the **L2TP Settings** tab.



3. Select the **Enable L2TP Server** option, and click **Apply** to enable the L2TP service.
4. Click **Add**.
5. In the **L2TP Settings** area, configure L2TP tunnel parameters:
   a. Select the **Peer Tunnel Name** option as needed. If you select this option, enter the tunnel name of the L2TP client.
   b. In the **Local Tunnel Name** field, enter the tunnel name for the L2TP server.
   c. In the **Tunnel Authentication** field, select **On** or **Off** as needed.

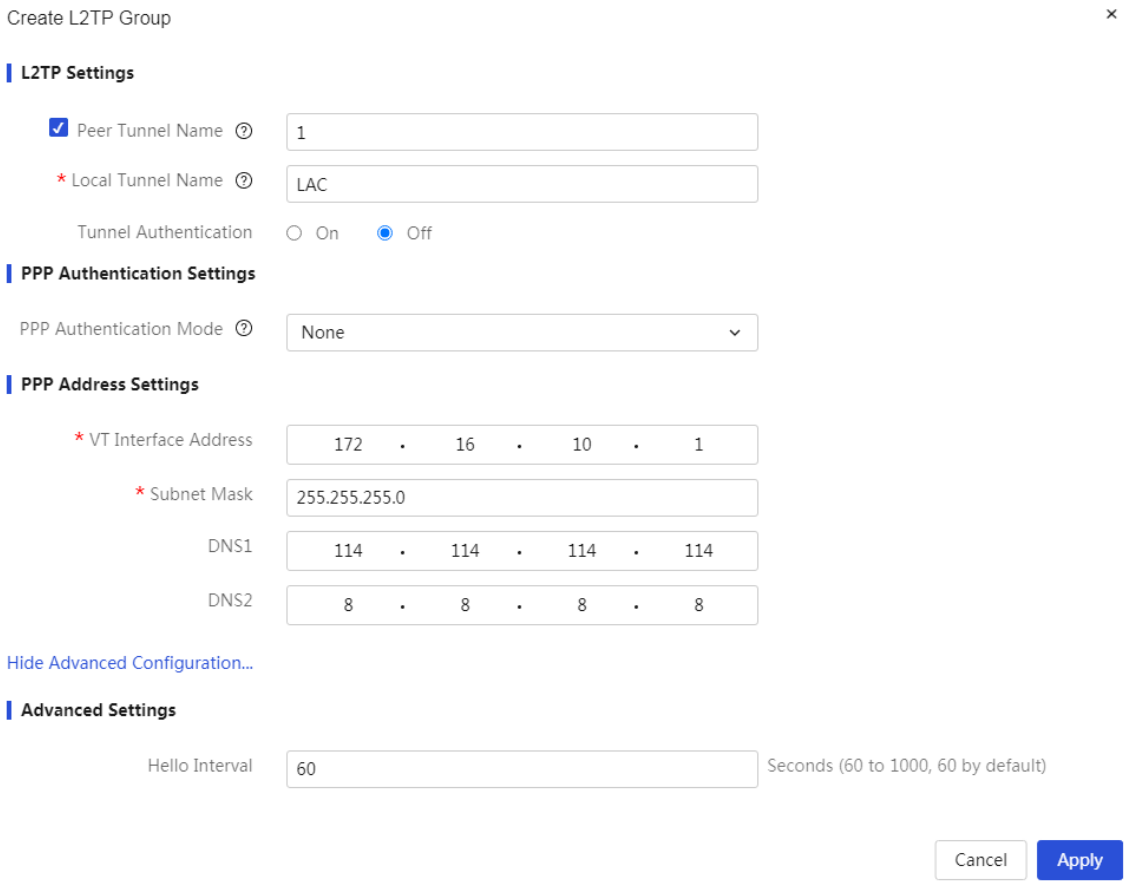
- If you select **On**, enter the authentication password in the **Tunnel Auth Password** field. The tunnel authentication feature enhances security. To use this feature, you must enable tunnel authentication on both the L2TP server and L2TP client and make sure the password are the same.
- If you select **Off**, authentication will not be performed for establishing a tunnel between the L2TP server and L2TP client.

6. From the **PPP Authentication Mode** list in the **PPP Authentication Settings** area, select **None**, **PAP**, or **CHAP** as needed.
   - If you select **None**, authentication will not be performed for users. Use this authentication method with caution because it is of the lowest security.
   - If you select **PAP**, a two-way handshake authentication will be performed for users. This authentication method is of medium security.
   - If you select **CHAP**, a three-way handshake authentication will be performed for users. This authentication method is of the highest security.
7. In the **PPP Address Settings** area, configure PPP address parameters:
   a. In the **VT Interface Address** field, enter the VT interface IP address to enable the L2TP server to allocate IP addresses to L2TP clients or users.
   b. In the **Subnet Mask** field, enter the subnet mask for the VT interface IP address.
   c. In the **DNS1** field, enter the primary DNS server address to be allocated to L2TP clients or users.
   d. In the **DNS2** field, enter the secondary DNS server address to be allocated to L2TP clients or users.

      DNS server 1 must be different from DNS server 2.
   e. In the **User Address Pool** field, enter the IP addresses to be allocated to L2TP clients or users.

      Make sure the user address pool does not contain the configured VT interface address.
8. Click **Show Advanced Configuration**.
9. In the **Hello Interval** field in the **Advanced Settings** area, enter the Hello interval.

   To check the connectivity of the tunnel between LAC and LNS, the LAC and LNS send Hello packets to each other periodically. The receiver will respond upon receiving a Hello packet. If the LAC or LNS does not receive a response from the peer within the specified time interval, it resends the Hello packet. If no response is received after five resends, the L2TP tunnel is considered disconnected and must be reestablished. The LNS side can configure a different Hello interval than the LAC side. By default, the Hello interval is 60 seconds.
10. Click **Apply**.

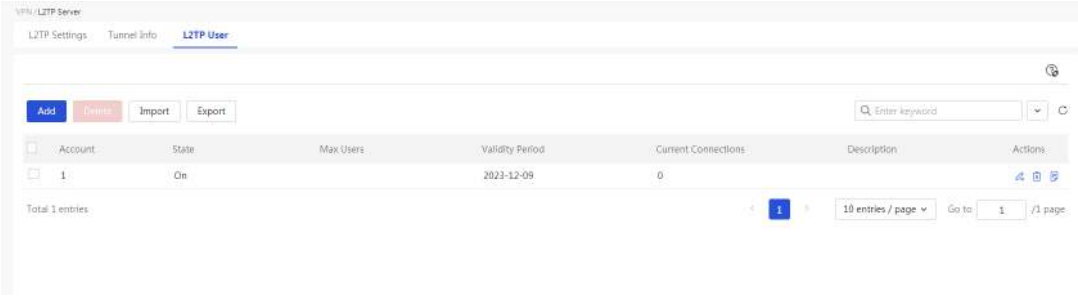


View tunnel information

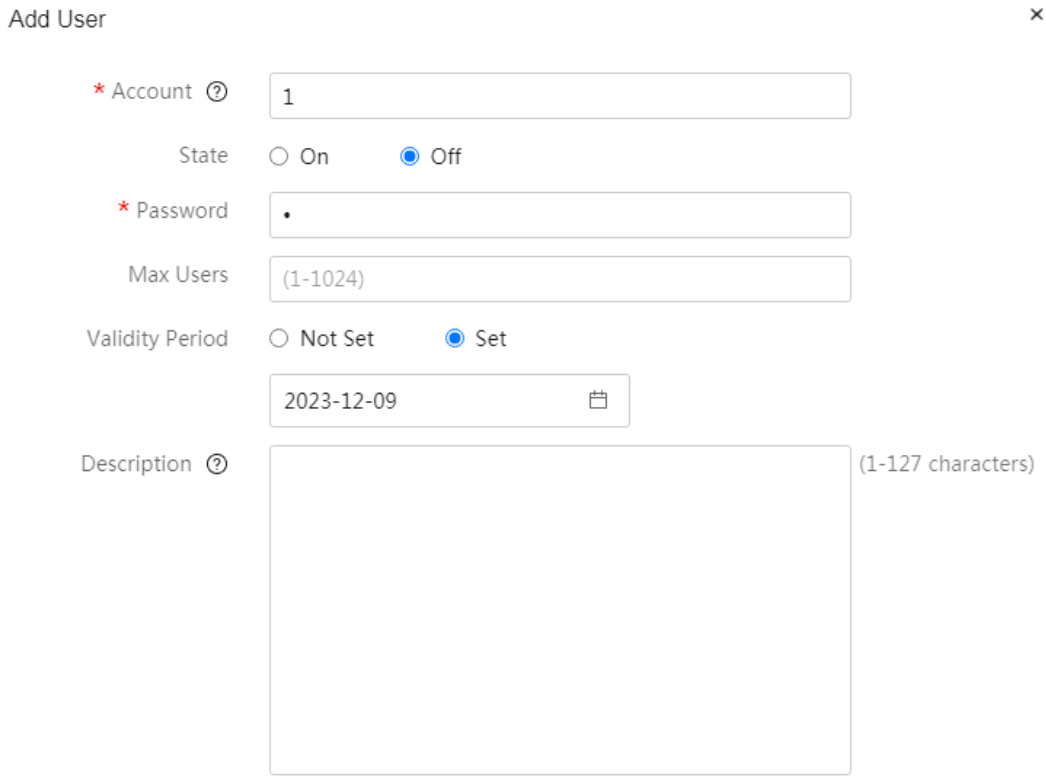
1. From the left navigation pane, select **VPN > L2TP Server**.
2. Click the **Tunnel Info** tab.

Configure L2TP users

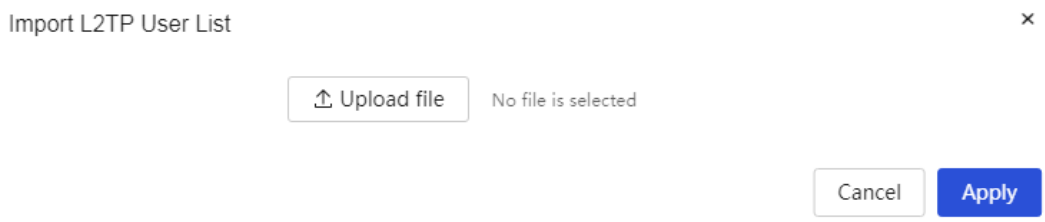
1. From the left navigation pane, select **VPN > L2TP Server**.
2. Click the **L2TP User** tab.



3. To add a single L2TP user, perform the following tasks:
   a. Click **Add**.
   b. In the **Account** field, enter the account name of the user.
   c. In the **State** field, select whether to enable the user.
   d. In the **Password** field, enter the password of the user.
   e. In the **Max Users** field, enter the maximum number of connections of the user.
   f. In the **Validity Period** field, select whether to set the expiration date of the user permissions. If you select the **Set** option, select the expiration date of the user permissions from the date selector.
   g. Click **Apply**.



4. To bulk add L2TP users, perform the following tasks:
   a. Click **Export** to download the export template.
   b. Open the downloaded template, add L2TP users, and save the template locally.
   c. Click **Import**.
   d. Click **Select File** to select the edited template.
   e. Click **Apply**.



Configure an L2TP client

About this feature

Perform this task to configure basic L2TP client parameters and enable L2TP.

To provide a secure, cost-effective solution for branches of an enterprise to access resources in the internal network of the enterprise, configure an L2TP client.

An L2TP client is a device that can process PPP and L2TP protocol packets. Typically, an L2TP client is deployed on the egress of an enterprise branch.

Restrictions and guidelines

After completing the L2TP client configuration, add a static route to the L2TP server subnet.

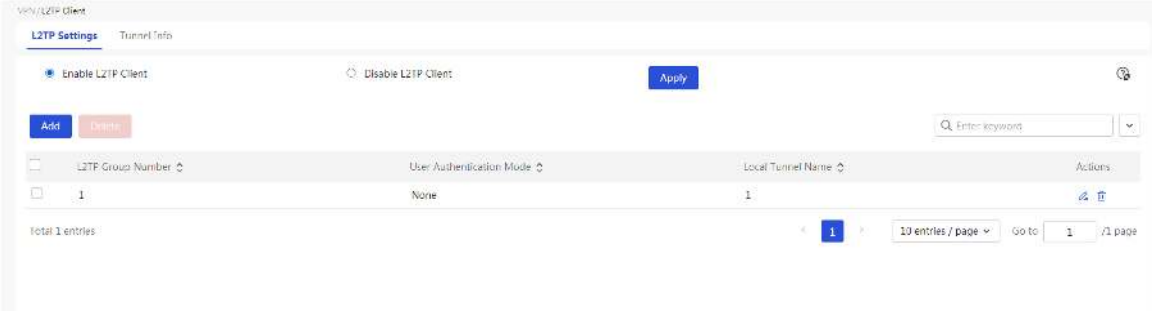
Configure L2TP settings

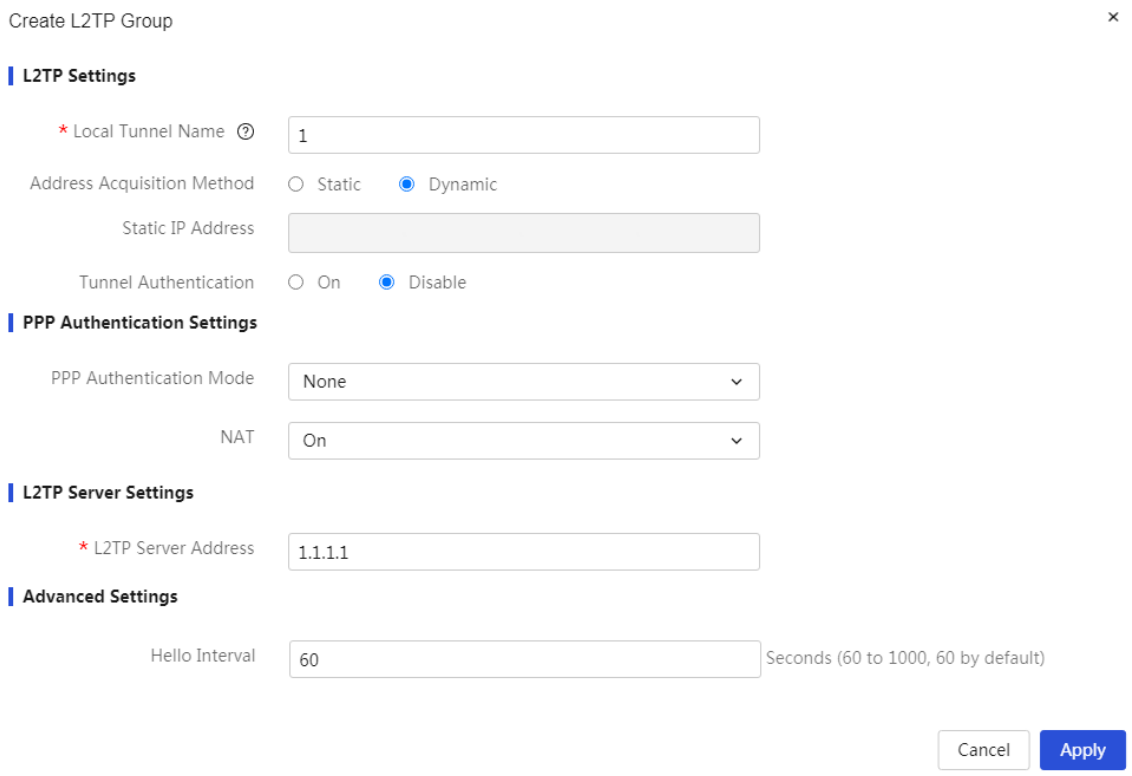
1. From the left navigation pane, select **VPN > L2TP Client**.
2. Click the **L2TP Settings** tab.
3. Select the **Enable L2TP Client** option, and click **Apply** to enable the L2TP service.
4. Click **Add**.
5. In the **L2TP Settings** area, configure L2TP tunnel parameters:
   a. In the **Local Tunnel Name** field, enter the tunnel name for the L2TP client.
   b. In the **Address Acquisition Method** field, select an IP address assignment method for the PPP interface after the LAC session is successfully established.
      – If you select the **Static** option, you must manually set an IP address (allocated by the LNS administrator on the peer end) on the LAC end.
      – If you select the **Dynamic** option, the IP address for the PPP interface is assigned by the LNS.
   c. In the **Tunnel Authentication** field, select **On** or **Off** as needed.
      – If you select **On**, enter the authentication password in the **Tunnel Auth Password** field. The tunnel authentication feature enhances security. To use this feature, you must enable tunnel authentication on both the L2TP server and L2TP client and make sure the password are the same.
      – If you select **Off**, authentication will not be performed for establishing a tunnel between the L2TP server and L2TP client.
6. From the **PPP Authentication Mode** list in the **PPP Authentication Settings** area, select **None**, **PAP**, or **CHAP** as needed.
   - If you select **None**, authentication will not be performed for users. Use this authentication method with caution because it is of the lowest security.

- If you select **PAP**, a two-way handshake authentication will be performed for users. This authentication method is of medium security. Enter a username and password.
- If you select **CHAP**, a three-way handshake authentication will be performed for users. This authentication method is of the highest security. Enter a username and password.

7. From the **NAT** list in the **PPP Authentication Settings** area, select **On** or **Off** as needed.
   - If you select **On**, you do not need to configure the route to the L2TP client on the L2TP server.
   - If you select **Off**, you must configure the route to the L2TP client on the L2TP server for the L2TP client to normally access resources on the server.
8. In the **L2TP Server Address** field in the **L2TP Server Settings** area, enter the IP address or domain name of the L2TP server.
9. In the **Hello Interval** field in the **Advanced Settings** area, enter the Hello interval.

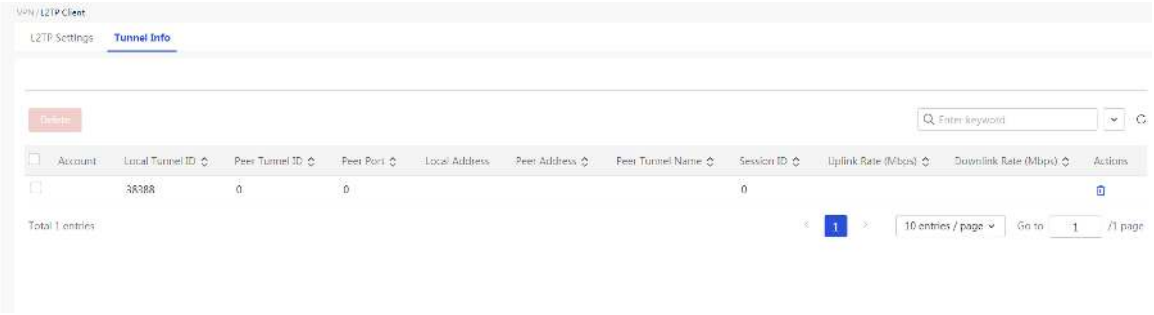
   To check the connectivity of the tunnel between LAC and LNS, the LAC and LNS send Hello packets to each other periodically. The receiver will respond upon receiving a Hello packet. If the LAC or LNS does not receive a response from the peer within the specified time interval, it resends the Hello packet. If no response is received after six resends, the L2TP tunnel is considered disconnected and must be reestablished. The LNS side can configure a different Hello interval than the LAC side. By default, the Hello interval is 60 seconds.
10. Click **Apply**.





View tunnel information

1. From the left navigation pane, select **VPN > L2TP Client**.
2. Click the **Tunnel Info** tab.



Configure advanced settings

Configuration tasks at a glance

Configure DDNS

You can configure DDNS for users to access services provided by a device's WAN interface through a fixed domain name. To configure DDNS, perform the following tasks:

Task	Remarks
(Required.) Register a domain name	Register a domain name on the DDNS service provider (such as PeanutHull).
(Required.) Configure DDNS	Bind the domain name registered on the DDNS server to the WAN interface on the device that provides the service.

Specify an output interface for packets with the specified destination IP address

You can configure a static route to specify an output interface for packets with the specified destination IP address. To configure a static route, perform the following tasks:

Task	Details
(Optional.) Configure VLANs	Add a VLAN for intercommunication on the device and assign the corresponding LAN ports into the VLAN. For more information, see VLAN configuration.
(Required.) Configure static routing	Add a static route for the subnet where the host resides.

Configure PBR

You can configure PBR to forward traffic from specific LAN hosts through designated WAN interfaces within a certain time period. To configure PBR, perform the following tasks:

Task	Details
(Required.) Add a time group	Set the time range for the PBR policy to take effect. For more information, see time group configuration.
(Required.) Configure PBR	Add a PBR policy as needed.

Manage application services

The application service allows you to configure Domain Name System (DNS) settings. DNS is a distributed database used by TCP/IP applications to translate domain names into IP addresses. The static DNS service, Dynamic Domain Name System (DDNS) service, and local DNS service are available.

The following rules apply when you configure the **Domain Name**, **Local Domain Name**, and **Server Address** fields:

- A domain name or server address is a string of 1 to 253 characters, and a local domain name is a string of 1 to 250 characters.
- A domain, server address, or local domain name can contain only letters, digits, hyphens (-), and dots (.)
- A domain, server address, or local domain name cannot start with or end with a dot (.) or hyphen (-), and cannot contain two or more consecutive dots (.) or hyphens (-).
- A domain name or server address must contain dots (.), and the characters following the last dot (.) cannot be all digits.

Configure static DNS

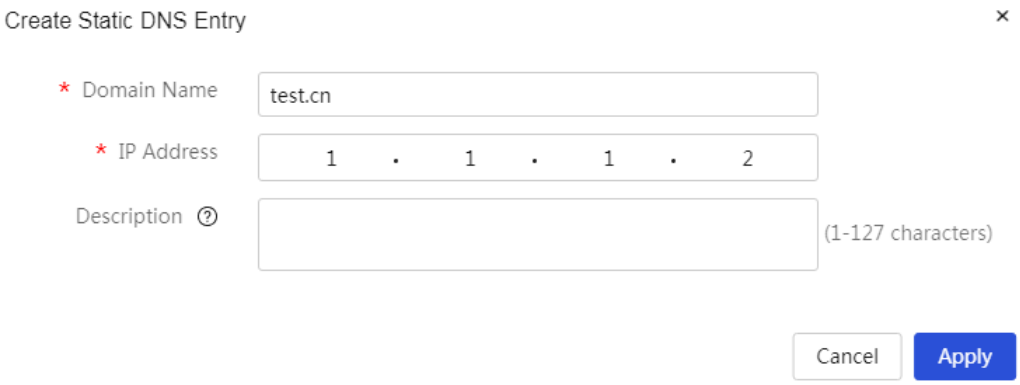
About this task

DNS provides only the static mappings between domain names and IP addresses. If you use a domain name to access services (such as Web, mail, or FTP) provided by the device, the system automatically checks the static name resolution table for an IP address.

Procedure

1. From the left navigation pane, select **Advanced Settings** > **App Services**.
2. Click the **Static DNS Entry Management** tab.

3. Click **Add**.
4. Specify a domain name assigned to the network device in the **Domain Name** field.
5. Enter the IP address of the network device in the **IP Address** field.
6. Click **Apply**.



Configure DDNS

About this task

Perform this task to configure DDNS for users to access services (such as Web, mail, or FTP) provided by a device's WAN interface through a fixed domain name when the WAN interface IP changes. For example, the WAN interface IP might change because of broadband dial-up.

Before you configure DDNS on the WAN interface, make sure you have registered an account on the DDNS service provider (such as PeanutHull). Then, if the WAN interface IP address of the device changes, the device will automatically notify the DDNS server to update the mapping between the IP address and the fixed domain name.

Restrictions and guidelines

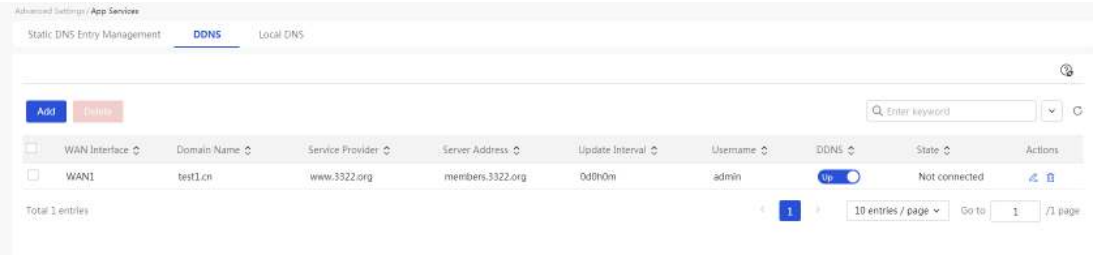
For a device to apply for a domain from the DDNS server, make sure the WAN interface on the device is an IP address on the public network.

Prerequisites

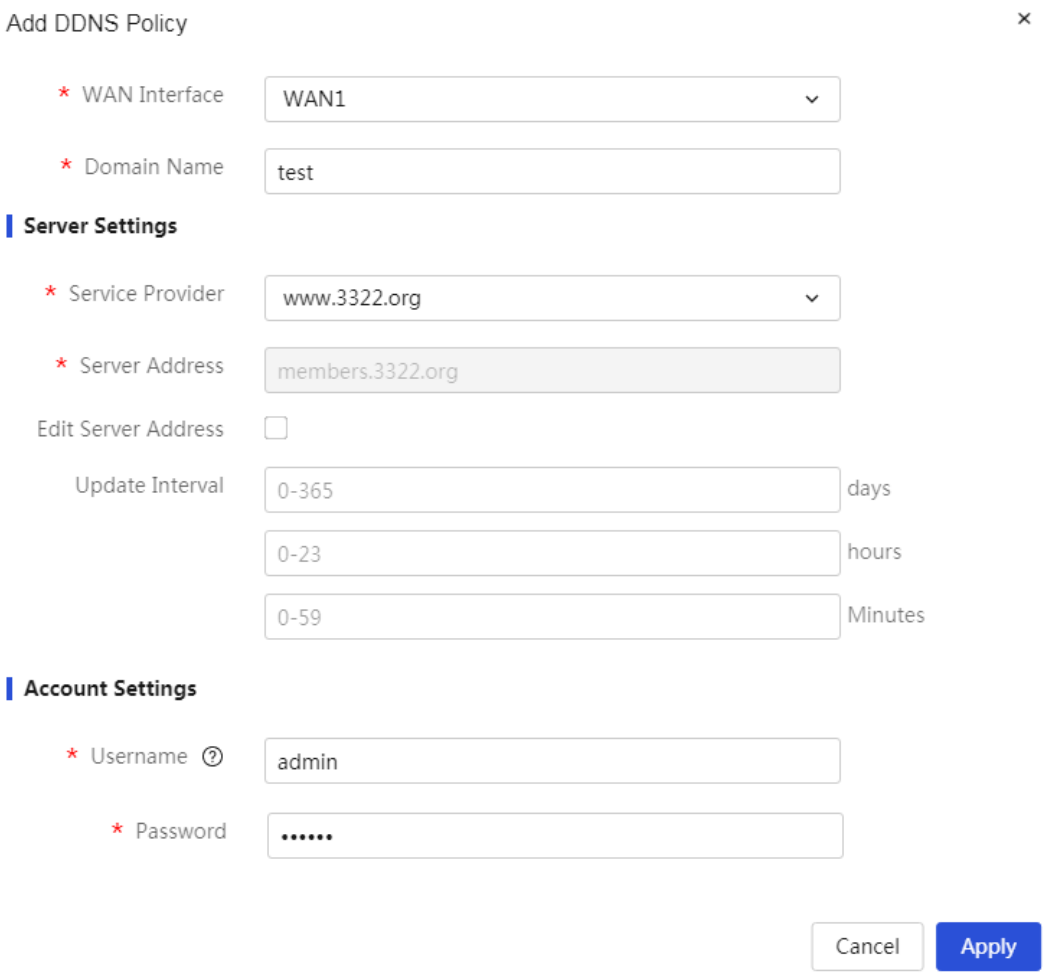
Register an account and password on the DDNS server (a DDNS service provider), for example, PeanutHull.

Procedure

1. From the left navigation pane, select **Advanced Settings** > **App Services**.
2. Click the **DDNS** tab.



3. Click **Add**.
4. In the **WAN Interface** field, select a WAN interface that provides Web, mail, or FTP services on the device.
5. Specify a domain name for the device in the **Domain Name** field.
6. In the **Server Settings** area, configure DDNS server parameters:
   - **Service Provider**: Select a DDNS service provider, for example, ORAY (PeanutHull).
   - **Server Address**: Specify the server address of the service provider. To edit the DDNS server address, select **Edit Server Address**, and then edit the server address in the **Server Address** field.
   - **Update Interval**: Specify the interval at which the device sends update requests to the server. You must specify the number of days, hours, and minutes. If you set the interval to 0, the device will send update requests only when the WAN interface IP address changes or the state of the WAN interface changes from down to up.
7. In the **Account Settings** area, enter the username and password registered at the DDNS service provider.
8. Click **Apply**.



Configure the local DNS service

About this task

Endpoints in the internal network can access the Web management interface of the device by using the local domain name.

Restrictions and guidelines

Make sure the local domain name does not conflict with registered domain names in the Internet.

Procedure

1. From the left navigation pane, select **Advanced Settings** > **App Services**.
2. Click the **Local DNS** tab.
3. Select **Enable** for **Local DNS**.
4. Enter a local domain name address in the **Local Domain Name** field.
5. Click **Apply**.

UPnP

About this task

Universal Plug and Play (UPnP) is a set of protocols for devices to communicate with each other. As a UPnP gateway, the device provides automatic port mapping. To achieve automatic port mapping via UPnP, make sure the following conditions are met:

- UPnP is enabled on the device.
- The operating systems of the hosts on the internal network support and are enabled with UPnP.
- The applications, for example, Thunder, BitComet, eMule, and MSN support and are enabled with UPnP.

With UPnP enabled, the device can automatically add port mapping for applications that support UPnP, which accelerates point-to-point transmission, and solve the issue that traditional services (such as MSN) cannot traverse NAT. However, with UPnP enabled, the device might also establish mapping for illegitimate applications that support UPnP, which poses security risks.

Restrictions and guidelines

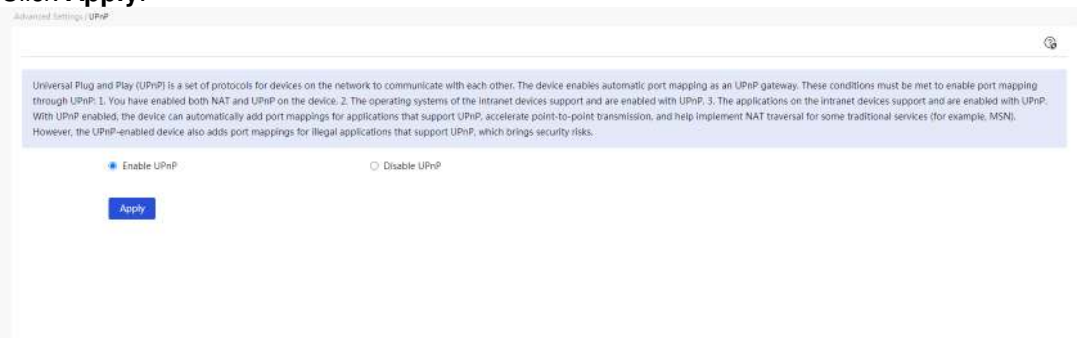
If your operating system or application does not support UPnP, you can manually configure port mapping by configuring the virtual server or port triggering.

The possible reasons for UPnP mapping failure include:

- SSDP service (used to discover UPnP devices) is disabled in the system. To use UPnP, you must enable SSDP in the system.
- The SP1 network in the operating system is enabled to connect the firewall, which conflicts with UPnP device discovery. SP2 fixes this issue, but you need to add an exception of UPnP framework to the firewall.
- The application or device does not support UPnP.

Procedure

1. From the left navigation pane, select **Advanced Settings** > **UPnP**.
2. Select **Enable UPnP**.
3. Click **Apply**.



Configure static routing

About this task

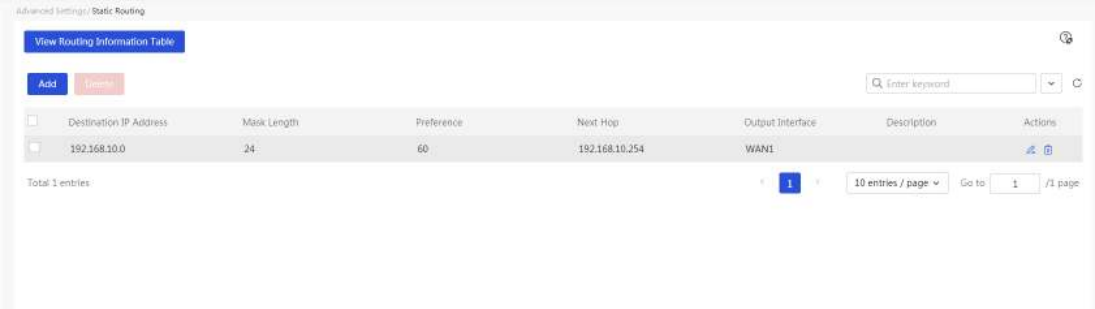
- Static routes are manually configured. If a network's topology is simple and stable, you only need to configure static routes for the network to work correctly. For example, you can configure a static route based on the network egress interface and the gateway IP address for correct communication.
- If multiple static routes are available to reach the same destination, you can assign different preference values to the static routes. The lower the preference value of a static route, the higher the priority of the route.

Restrictions and guidelines

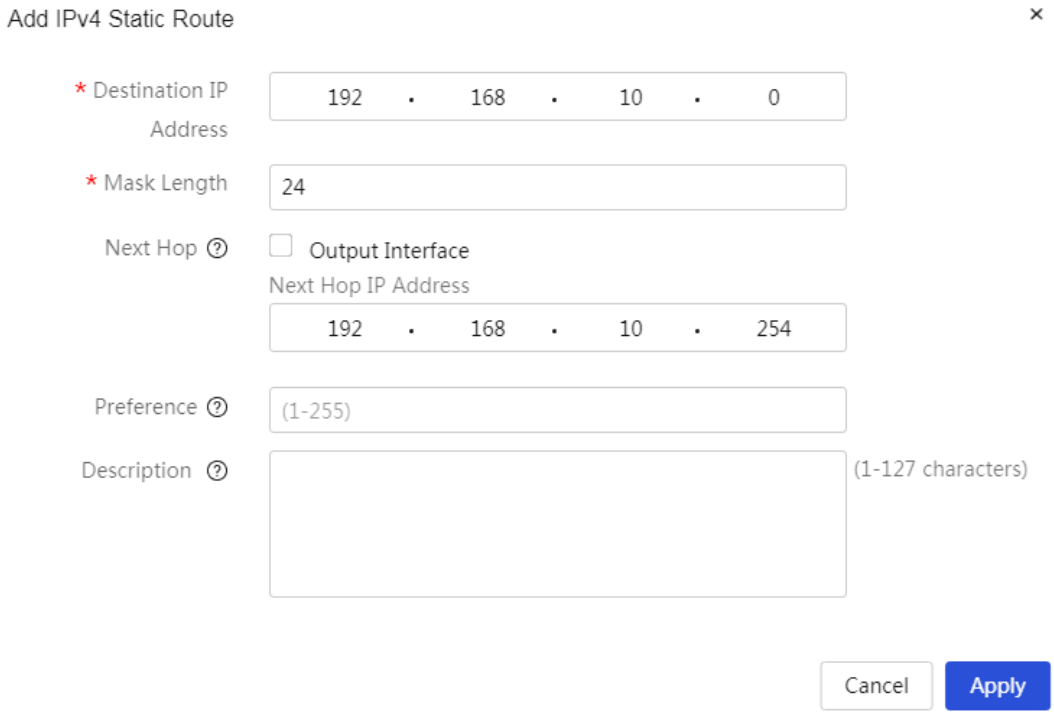
If the interface associated with the next hop in a static route becomes invalid, the static route will not be deleted from the local device. To resolve this issue, you need to check your network environment and edit the static route settings.

Procedure

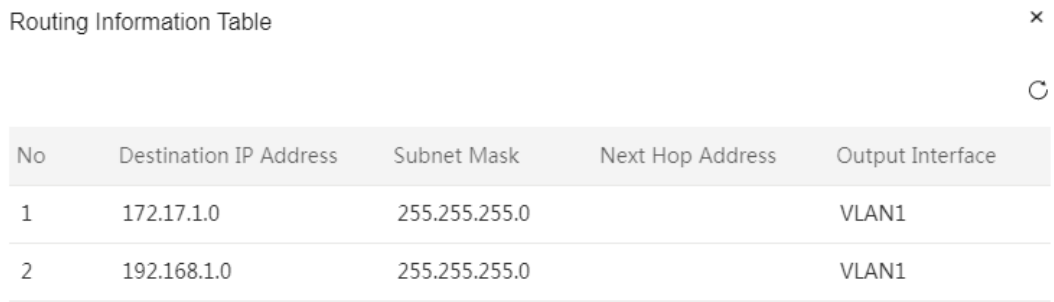
1. From the left navigation pane, select **Advanced Settings** > **Static Routing**.



2. Click **Add**.
3. In the **Destination IP address** field, enter the destination network IP address of the static route.
4. In the **Mask length** field, enter the mask length of the destination network.
5. In the **Next Hop** field, specify an output interface and a next hop IP address for the static route.
   - Select the **Output Interface** option. If you cannot determine the output interface, do not select the **Output Interface** option. The device will select an appropriate output interface based on the specified next hop IP address.
   - Enter a next hop IP address.
6. In the **Preference** field, enter a preference for the static route.
7. In the **Description** field, enter a description for the static route.
8. Click **Apply**.



9. To view the device routing information, click **View Routing Information Table**.



No	Destination IP Address	Subnet Mask	Next Hop Address	Output Interface
1	172.17.1.0	255.255.255.0		VLAN1
2	192.168.1.0	255.255.255.0		VLAN1

Configure PBR

About this task

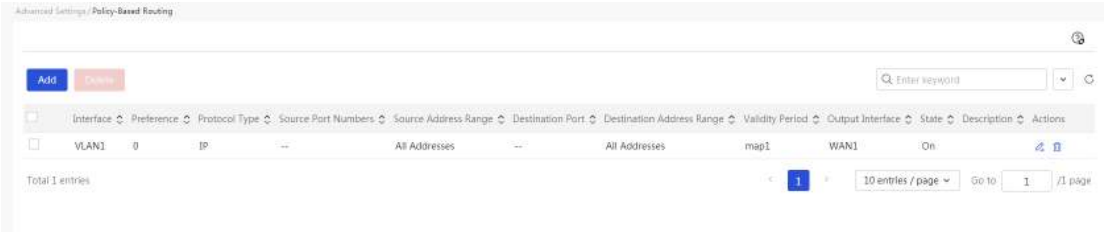
Policy-based routing (PBR) enables you to forward packets flexibly based on packet characteristics by configuring a policy that contains a set of packet matching criteria and actions. For example, you can configure a PBR policy to forward packets with the specified source or destination IP address to the specified next hop or out of the specified interface.

The PBR policies take effect in the order they are configured. The PBR policy configured first take preference over the PBR policy configured later.

You can customize the priorities for PBR policies. The smaller the value, the higher the priority.

Procedure

1. From the left navigation pane, select **Advanced Settings** > **Policy-Based Routing**.
2. Click **Add**.



3. Configure the match rule parameters:
   - In the **Interface** field, select an interface for the PBR policy.
   - Select a protocol type for the **Protocol Type** field. If you select **Protocol Number**, you must enter the protocol number.

     If you select **TCP** or **UDP**, you must enter the source and destination port numbers of the packets to match.
   - In the **Source address range** and **Destination address range** fields, enter the source and destination IP address ranges. To specify an address range, separate the start and end IP addresses with a hyphen (-), for example, 1.1.1.1-1.1.1.2. To specify only one IP address, enter that IP address as both start and end IP addresses, for example, 1.1.1.1-1.1.1.1. To negate the address range rule, add an exclamation mark before the address range, for example, !1.1.1.1-1.1.1.10. This setting represents all IP addresses not in the specified address range.
   - In the **Source Port** and **Destination Port** fields, enter the source and destination ports. To negate the port number rule, add an exclamation mark before the port number range, for example, !1-5000. This setting represents all port numbers not in the specified port number range.
   - In the **Validity Period** section, specify the time range for the PBR policy to take effect.
   - In the **Preference** field, set the priority for the PBR policy. If you select **Custom**, you need to manually specify a priority for this PBR policy.
   - In the **Output Interface** field, set the output interface for matching packets.
   - You can use the **Apply Policy on Disconnection** option to control whether the PBR policy can take effect when the associated WAN interface is disconnected from the external network.
     - If you select the **Apply Policy on Disconnection** option, the PBR policy can take effect to forward data when the associated WAN interface is disconnected from the external network.
     - If you do not select the **Apply Policy on Disconnection** option, the PBR policy does not take effect when the associated WAN interface is disconnected from the external network.
   - Specify whether or not to enable the PBR policy in the **Status** field.
   - Enter a description for the PBR policy in the **Description** field to facilitate usage.
4. Click **Apply**.

Add PBR Policy ⓘ ×

PBR Policy

* Interface ⓘ: VLAN1

* Protocol Type: IP

0

Source Address Range: 0.0.0.0-255.255.255.255

Destination Address Range: 0.0.0.0-255.255.255.255

Source Port: 1-65535
(Enter a list of port numbers or port number ranges separated by commas (,), for example, 1,3,4,10-20. Each port number is in the range of 1 to 65535.)

Destination Port: 1-65535
(Enter a list of port numbers or port number ranges separated by commas (,), for example, 1,3,4,10-20. Each port number is in the range of 1 to 65535.)

Validity Period ⓘ: map1 × View

Preference ⓘ: ◉ Auto ○ Custom (0-65534)

Output Interface: WAN1 ☐ Apply Policy on Disconnection

Status: ◉ On ○ Disable

Description ⓘ: (1-127 characters)

Cancel Apply

Use system tools

Configure system settings

About this feature

Use this feature to configure device information and set the system time. Device information includes device name, device location, and contact information of the administrator. The information helps the administrator manage and locate the device. The system time settings include date, time, and time zone. To facilitate device management and ensure correct coordination with other network devices, you must configure the system time accurately for the device.

You can use the following methods to obtain the system time:

- **Manually set the date and time**—The manually specified date and time become the current system time. After you specify the date and time, the device will use its internal clock signal for timing. The system time will restore to the factory default after the device restarts.
- **Automatic date and time synchronization**—The device uses the time obtained from the NTP server as the current system time and periodically synchronizes the time with the NTP server. The device can resynchronize the system time of the NTP server after it restarts. As a best practice, use automatic date and time synchronization if an NTP server is available in your network to provide more accurate time.

Configure device information

1. From the left navigation pane, select **System Tools** > **System Settings**.
2. Click the **Device Info** tab.
3. In the **Device Name** field, enter a device name. For example, enter a device name in the format of *device model*. The device name is a string of 1 to 31 characters. Only letters, digits, Chinese characters, and special characters !#$%&()*+,-./:;<=>?@[]^_{|}~ are supported. A Chinese character is three characters long.
4. In the **Device Location** field, enter the location information of the device. The value is a string of 1 to 255 characters. The string cannot contain Chinese characters.
5. In the **Contact Info** field, enter the contact information of the administrator. The value is a string of 1 to 255 characters. The string cannot contain Chinese characters.
6. Click **Apply**.

Manually set the date and time

Prerequisites

Obtain the time zone of the device. Configure the time zone of the device as the time zone of the geographical area where the device is located. For example, if the device is in China, select **Beijing**, **Chongqing**, **Hong Kong SAR**, **Urumqi (GMT+08:00)**. If the device is in the United States, select **Central Time (US & Canada) (GMT-06:00)**.

Restrictions and guidelines

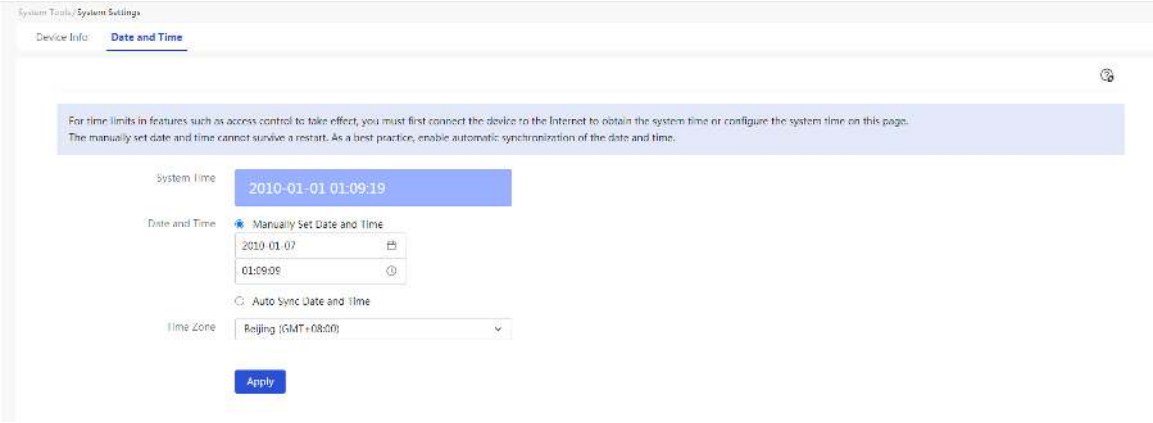
The system time will restore to the factory default after the device restarts.

Procedure

1. From the left navigation pane, select **System Tools** > **System Settings**.
2. Click the **Date and Time** tab.

3. Select the **Manually Set Date and Time** option.
4. Set the system time to the current time of the geographical region where the device is located.
   a. Pick the year, month, and day.
   b. Pick hours, minutes, and seconds.
5. Set the time zone to the time zone of the physical location where the device resides.
6. Click **Apply**.

Figure 11 Manually setting the date and time



Configure automatic date and time synchronization

Prerequisites

Obtain the time zone of the device. Configure the time zone of the device as the time zone of the geographical area where the device is located. For example, if the device is in China, select **Beijing**, **Chongqing**, **Hong Kong SAR**, **Urumqi (GMT+08:00)**. If the device is in the United States, select **Central Time (US & Canada) (GMT-06:00)**.

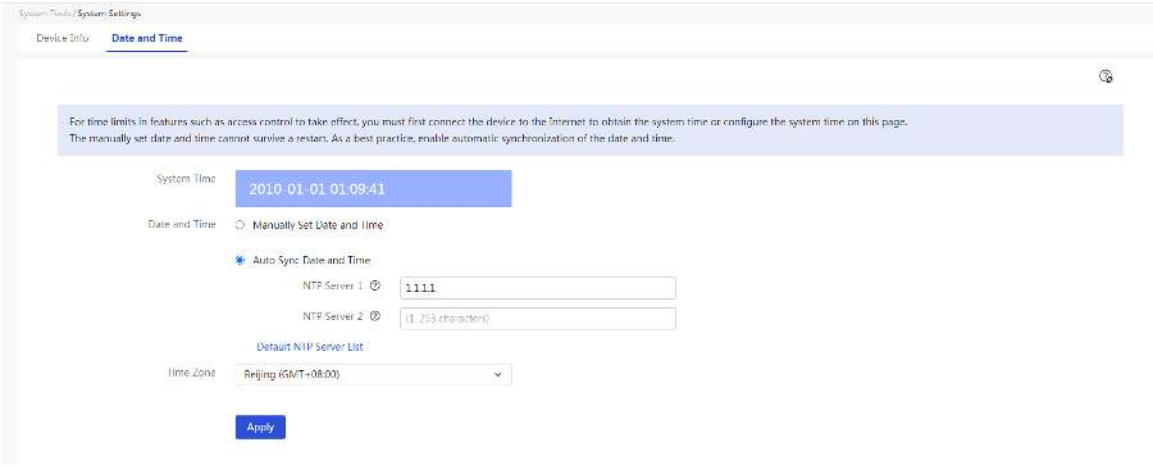
Restrictions and guidelines

For time consistency between the device and the NTP server, make sure the device uses the same time zone as that configured on the NTP server.

Procedure

1. From the left navigation pane, select **System Tools** > **System Settings**.
2. Click the **Date and Time** tab.
3. Select the **Auto Sync Date and Time** option.
4. In the **NTP Server 1** field, enter the IP address or domain name of NTP server 1.
5. In the **NTP Server 2** field, enter the IP address or domain name of NTP server 2. The device selects an NTP server automatically for time synchronization. If the preferred server fails, the system time of the device will automatically be replaced with the system time of another NTP server. If both NTP servers fail, the device will use the internal clock signal for timing. When an NTP server recovers, the device will synchronize its system time with the system time of the NTP server.
6. Click the **Default NTP Server List** link. In the dialog box that opens, view information about the built-in NTP servers on the device, and click **Close** to close the dialog box.
7. Set the time zone to the time zone of the physical location where the device resides.
8. Click **Apply**.

Figure 12 Configuring automatic date and time synchronization



Perform network diagnosis

About this feature

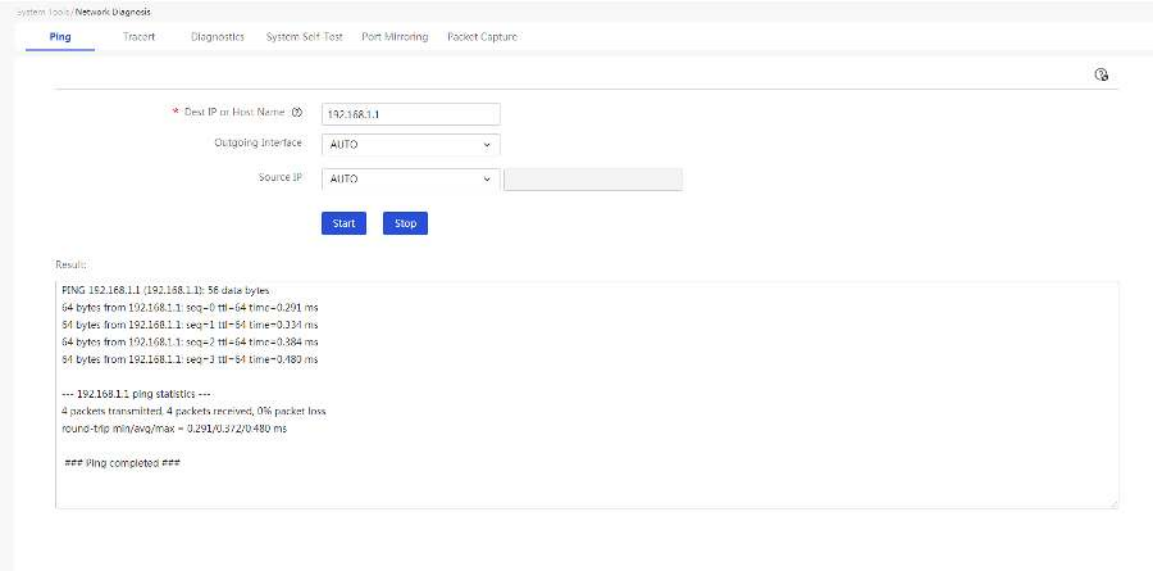
Perform this task to diagnose network issues. The device provides the following network diagnostic utilities:

- **Ping**—Tests the reachability of the destination IP address.
- **Tracert**—Traces the path that the packets traverse from source to destination.
- **System self-test**—Checks the running and configuration information for the device.
- **Diagnostics**—Collects running information for each module for you to locate issues. The device saves the information as a zip file to your endpoint automatically.
- **Port mirroring**—Copies the packets passing through a port to a port that connects to a data monitoring device for traffic monitoring, performance analysis, and fault diagnostics.
- **Packet capture**—Captures data packets for fault analysis. After packet capture finishes, the system automatically exports the **capture-******.pcap** file. You can save the file to your device.

Configure ping

1. From the left navigation pane, select **System Tools** > **Info Collector**.
2. Click the **Ping** tab.
3. In the **Dest IP or Host Name** field, enter the destination IP address or host name to be pinged. The value cannot contain a Chinese character, space, back slash (\), apostrophe ('), quotation mark ("), left angle bracket (<), right angle bracket (>), semi-colon (;), ampersand sign (&), back quote (`), or pound sign (#).
4. In the **Outgoing Interface** field, select an outgoing interface for packets to the destination IP address or host name. For the device to automatically select an interface to forward ping packets, select **AUTO**.
5. In the **Source IP** field, select the source IP address for the ping operation. For the device to automatically select a source IP address for the ping operation, select **AUTO**. To manually enter an IP address as the source IP address for the ping operation, select **Source IP**.
6. Click **Start**. The system displays the test process and result on this page, including packet sending information and average RTT to the specified host.

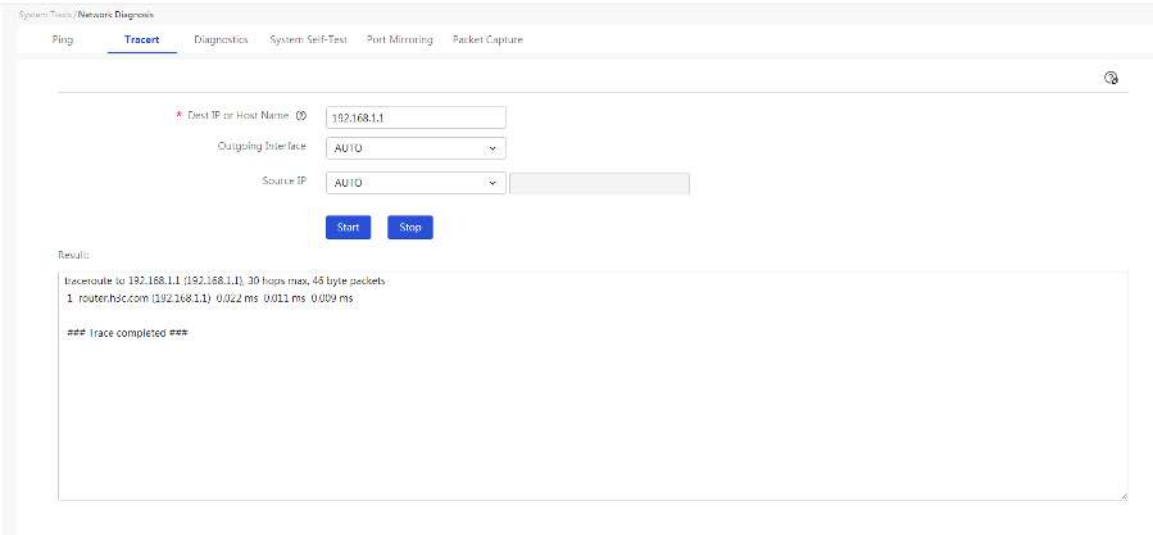
Figure 13 Configuring ping



Configure tracert

1. From the left navigation pane, select **System Tools** > **Info Collector**.
2. Click the **Tracert** tab.
3. In the **Dest IP or Host Name** field, enter the destination IP address or host name to be traced.
4. In the **Outgoing Interface** field, select an outgoing interface for packets to the destination IP address or host name. For the device to automatically select an interface to forward tracert packets, select **AUTO**.
5. In the **Source IP** field, select the source IP address for the tracert operation. For the device to automatically select a source IP address for the tracert operation, select **AUTO**. To manually enter an IP address as the source IP for the tracert operation, select **Source IP**.
6. Click **Start**. The system displays the test process and result on this page.

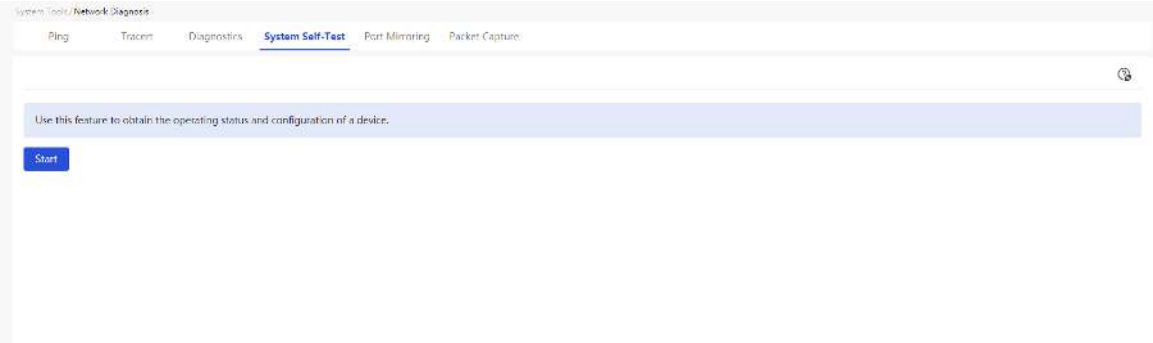
Figure 14 Configuring tracert



Perform a system self-test

1. From the left navigation pane, select **System Tools** > **Info Collector**.
2. Click the **System Self-Test** tab.
3. Click **Start**. The system displays the self-test result on the page.

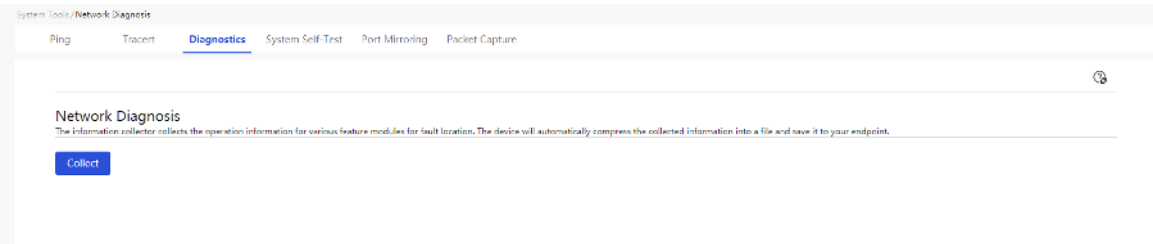
Figure 15 Performing a system self-test



Collect diagnostic information

1. From the left navigation pane, select **System Tools** > **Info Collector**.
2. Click the **Diagnostics** tab.
3. Click **Collect**.

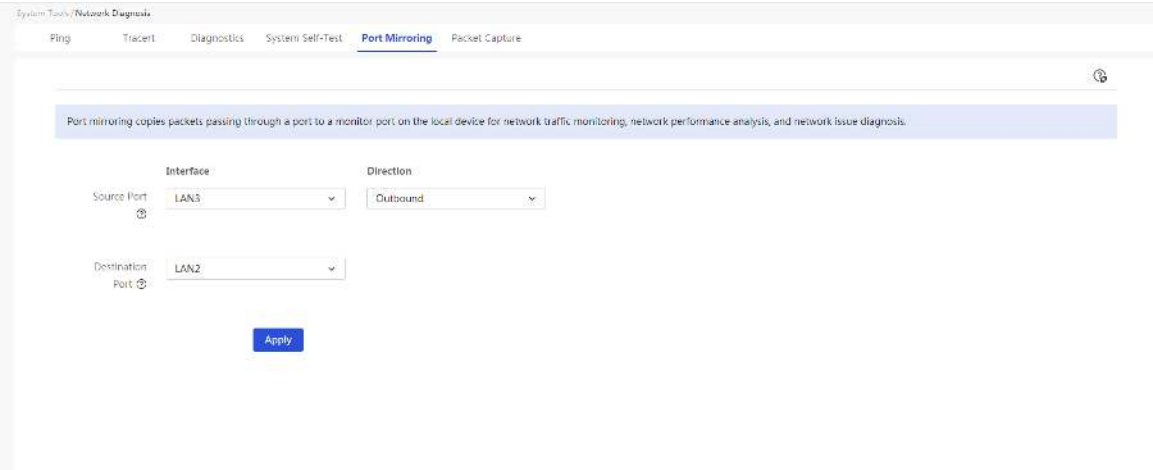
Figure 16 Collecting diagnostic information



Configure port mirroring

1. From the left navigation pane, select **System Tools** > **Info Collector**.
2. Click the **Port Mirroring** tab.
3. In the **Source Port** field, select a mirroring source port, which is the port connected to the data monitoring device.
4. In the **Direction** field, select the direction of the traffic that is copied on a mirroring source.
   - To copy only packets received by the mirroring source, select **Inbound**.
   - To copy only packets sent from the mirroring source, select **Outbound**.
   - To copy packets received by and sent from the mirroring source, select **Bidirectional**.
5. In the **Destination Port** field, select the mirroring destination port, which is the port connected to the data monitoring device.
6. Click **Apply**.

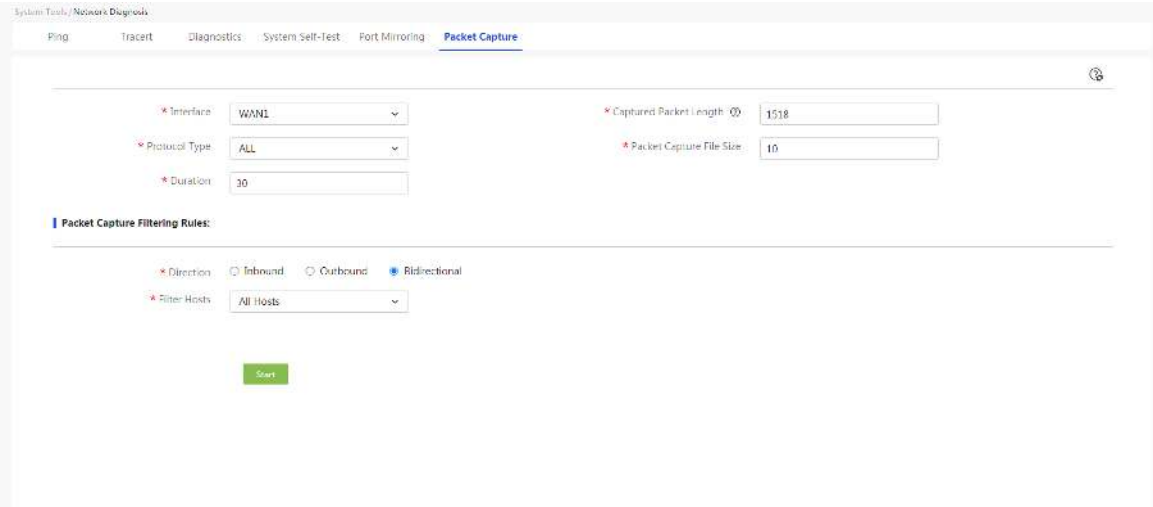
Figure 17 Configuring port mirroring



Capture packets

1. From the left navigation pane, select **System Tools** > **Info Collector**.
2. Click the **Packet Capture** tab.
3. In the **Interface** field, select an interface on which packets will be captured. Options include all WAN and VLAN interfaces on the device.
4. In the **Captured Packet Length** field, enter the length of the packets to be captured, in bytes. If the length of a packet is greater than this value, the packet will be truncated. Using a longer captured packet length will increase packet processing time and decrease the number of captured packets, which leads to packet loss. On the premise of being able to capture the desired packets, the smaller the captured packet length, the better.
5. In the **Protocol Type** field, select the protocol type of the packets. To capture all packets on the selected interface, select **ALL**.
6. In the **Packet Capture File Size** field, enter the size of the packets to be captured, in MB.
7. In the **Duration** field, enter the duration of the packet capture process, in seconds.
8. In the **Direction** field, select a packet capture direction. Options include:
   - **Inbound**—Captures received packets.
   - **Outbound**—Captures sent packets.
   - **Bidirectional**—Captures both received and sent packets. The default option is **Bidirectional**.
9. In the **Source Host**, **Destination Host**, and **Filter Hosts** fields, filter source and destination hosts for packet capture.
   - **All Hosts**—Captures packets from or destined for all hosts.
   - **Filter by IP Address**—Captures packets from or destined for the specified IP address.
   - **Filter by MAC Address**—Captures packets from or destined for the specified MAC address.
10. Click **Start**. The system displays the packet capture process and the current number of captured packets on this page. During the packet capture process, you can click **Cancel** to terminate the current operation and export the captured file **capture-******.pacp**.

Figure 18 Capturing packets



Configure remote management

About this feature

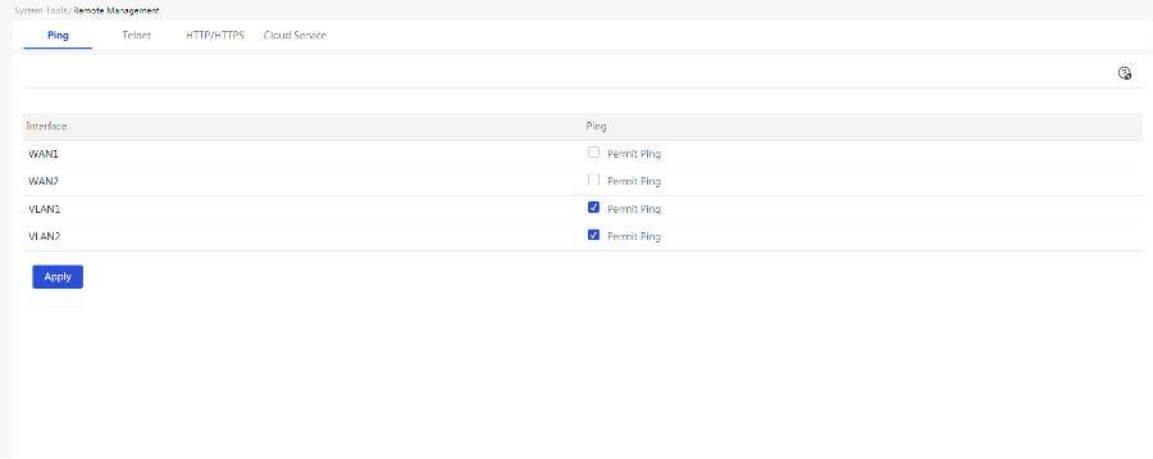
Use remote management to configure parameters for network connectivity detection or device remote login and management. Remote management provides the following functionalities:

- **Ping**—Tests the network connectivity to obtain network situations.
- **Telnet**—A remote login protocol. You can Telnet to the device from a PC to remotely manage the device.
- **HTTP/HTTPS**—Web login can use HTTP or HTTPS. HTTPS login is more secure than HTTP login. You can use HTTP or HTTPS to log in to the Web interface of the device from a PC for intuitively configuring and managing the device.
- **Cloud**—The device can be managed on the Cloudnet platform.

Permit ping on an interface

1. From the left navigation pane, select **System Tools** > **Remote Management**.
2. Click the **Ping** tab.
3. Select **Permit Ping** for an interface to permit the interface to respond to ping packets.
4. Click **Apply**.

Figure 19 Permitting ping on an interface



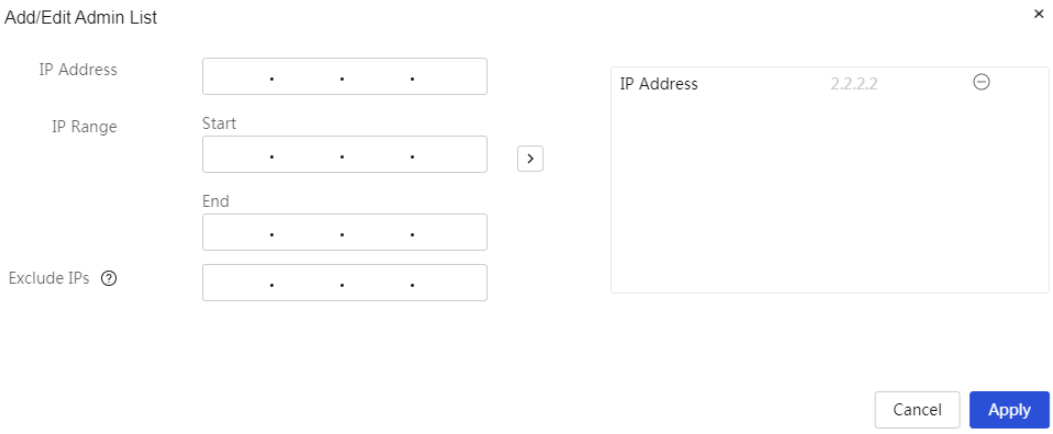
Configure Telnet login

1. From the left navigation pane, select **System Tools** > **Remote Management**.
2. Click the **Telnet** tab.
3. Click the button next to the **Telnet** field to enable the Telnet service. When the Telnet service is in **ON** state, the service is enabled.
4. In the **IPv4 Port** field, enter the port number used for accessing and managing the device over Telnet. External users can Telnet to the device for management through this port.

   Figure 20 Configuring Telnet login

5. In the **Admin List** area, click **Add/Edit**.
   a. In the **IP Address** field, enter an IP address for accessing the device over Telnet.
   b. In the **IP Range** field, enter the start and end IP addresses to specify an administrator IP address range for accessing the device over Telnet.
   c. In the **Exclude IPs** field, enter an IP address not allowed to access the device over Telnet.
   d. Click the **>** icon to submit the configuration.
   e. Repeat steps a, b, c, and d to add multiple IP addresses, IP ranges, or excluded IP addresses.
6. Click **Apply**.

Figure 21 Adding and editing the admin list



Configure HTTP/HTTPS login

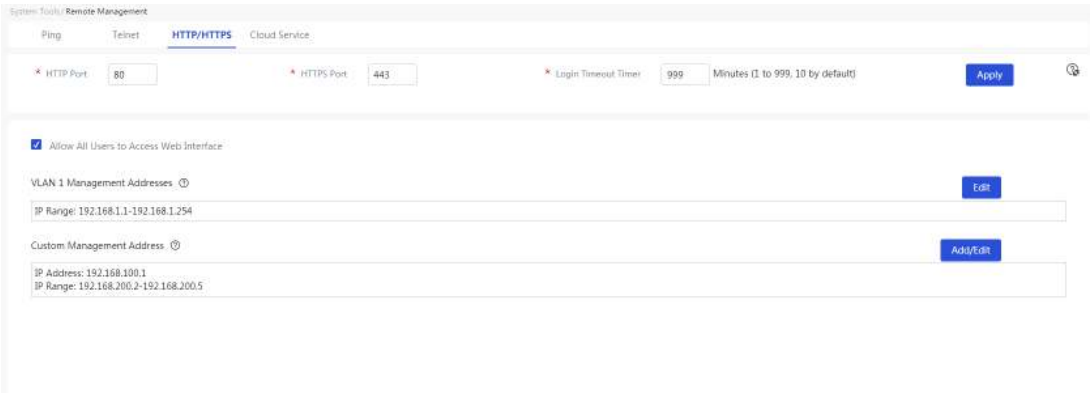
Restrictions and guidelines

When the administrator changes the VLAN1 network segment, the VLAN1 management address range will automatically change accordingly.

Procedure

1. From the left navigation pane, select **System Tools** > **Remote Management**.
2. Click the **HTTP/HTTPS** tab.

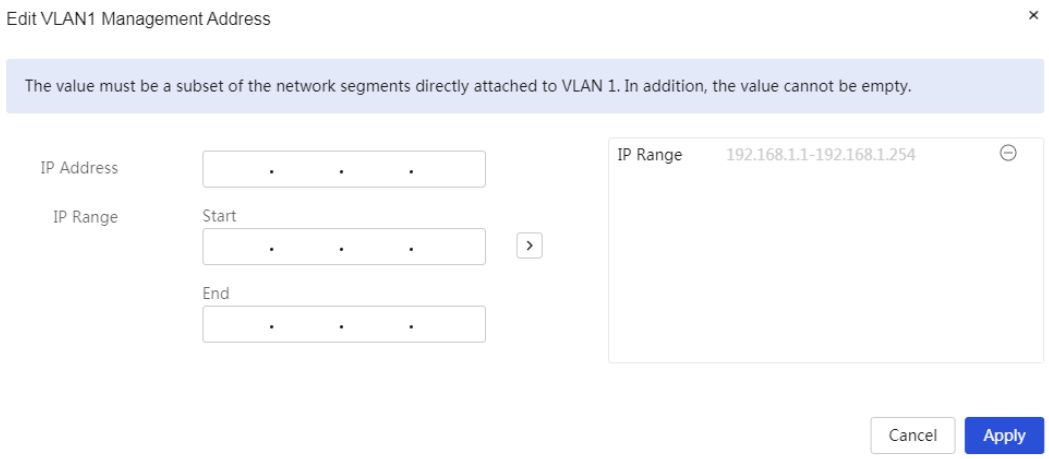
   Figure 22 Configuring HTTP/HTTPS login



3. In the **HTTP Port** field, enter a port number for HTTP login. As a best practice, use a port number greater than 10000 for HTTP login.
4. In the **HTTPS Port** field, enter a port number for HTTPS login. As a best practice, use a port number greater than 10000 for HTTPS login.
5. In the **Login Timeout Timer** field, enter the idle timeout timer for the Web interface. By default, the value is 10 minutes. When the idle time exceeds the idle timeout timer after an administrator logs in to the Web interface, the system automatically logs out that administrator. This parameter takes effect on the next login of the administrator after it is configured.
6. To allow all users to access the Web interface over HTTP/HTTPS, select **Allow All Users to Access Web Interface**.

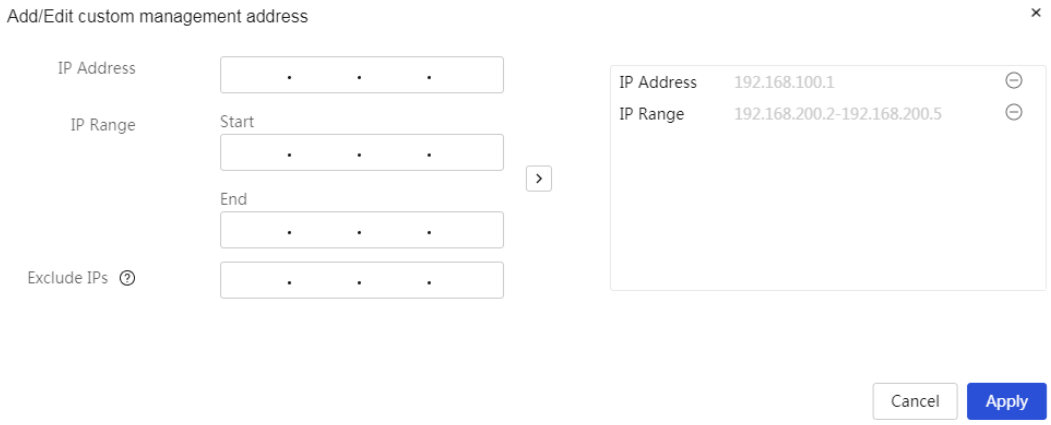
7. In the **VLAN 1 Management Addresses** area, click **Edit** to add administrator IP addresses or ranges allowed to access the Web interface. In the dialog box that opens, you can perform the following operations:
   a. In the **IP Address** field, enter an IP address allowed to access the device through HTTP or HTTPS.
   b. In the **IP Range** field, enter a start IP address and an end IP address to specify an IP range allowed to access the device through HTTP or HTTPS.
   c. Click the **>** icon to submit the configuration.
   d. Repeat steps a, b, and c to add multiple IP addresses or ranges.
   e. Click **Apply**.

Figure 23 Editing VLAN 1 management addresses



8. In the **Custom Management Address** area, click **Add**/**Edit** to add administrator IP addresses or ranges allowed to access the Web interface. In the dialog box that opens, you can perform the following operations:
   a. In the **IP Address** field, enter an IP address allowed to access the device through HTTP or HTTPS.
   b. In the **IP Range** field, enter a start IP address and an end IP address to specify an IP range allowed to access the device through HTTP or HTTPS.
   c. In the **Exclude IPs** field, enter an IP address that is not allowed to access the device through HTTP or HTTPS.
   d. Click the **>** icon to submit the configuration.
   e. Repeat steps a, b, c, and d to add multiple IP addresses, IP ranges, or excluded IP addresses.
   f. Click **Apply**.

Figure 24 Adding and editing custom management addresses



Use the cloud service

1. From the left navigation pane, select **System Tools** > **Remote Management**.
2. Click the **Cloud** tab.
3. Select whether to enable the cloud service.
4. Use the Hik-Connect or Hik-ProConnect app the scan the QR code and onboard the device.

Manage configuration

About this feature

Use configuration management to manage the configuration files on the device. A configuration file saves device settings.

With configuration management, you can perform the following tasks:

- **Restore the factory defaults**—This task restores the configuration to the factory defaults. If the device does not have a startup configuration file or the startup configuration file is corrupt, perform this task so that the device can start up at the next startup.
- **Restore the configuration from a backup file**—This task replaces the running configuration with the configuration from a backup file. Perform this task if the running configuration contains incorrect or undesirable settings.
- **Export the running configuration**—This task exports the running configuration to a configuration file. Perform this task to back up the running configuration for future use.
- **Fast back up the running configuration to a USB drive**—This task backs up the running configuration to a USB drive.
- **Fast restore the device configuration from a USB drive**—This task restores the device configuration from the configuration file on a USB drive.

Support for USB depends on the device model.

Restore the factory defaults

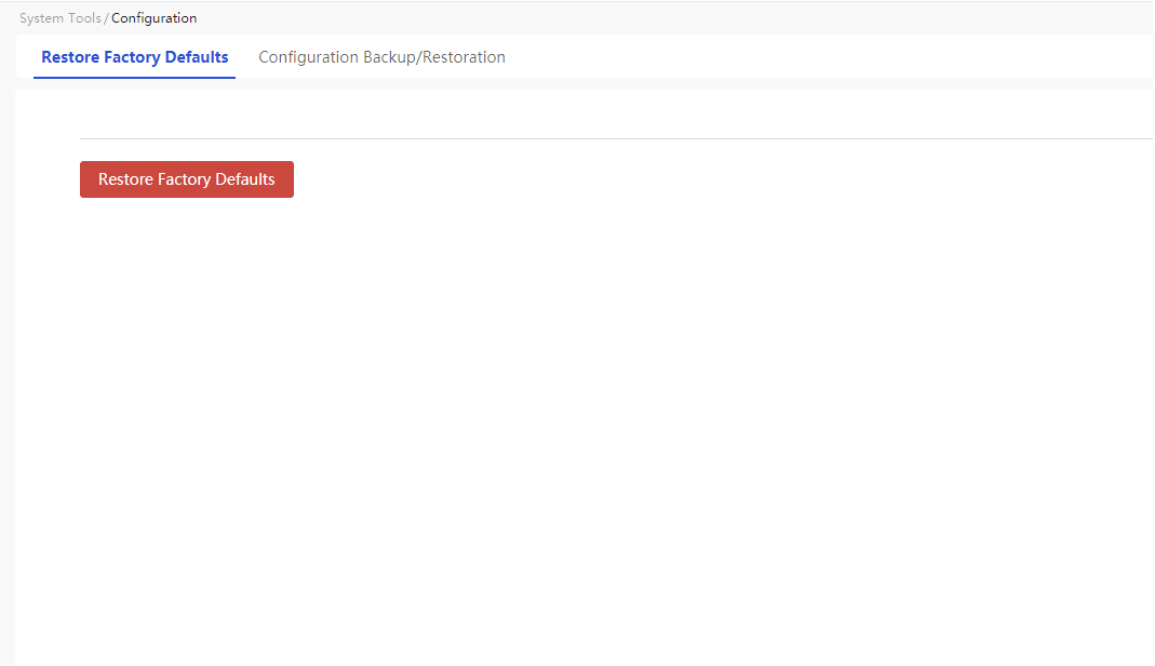
Restrictions and guidelines

The device running configuration will be lost after a factory restore. If you do not want to lose the running configuration, back up the configuration before restoring the factory defaults. After restoring to factory defaults, the device will restart, during which you must ensure that no power outage will occur.

Procedure

1. From the left navigation pane, select **System Tools** > **Configuration**.
2. Click the **Restore Factory Defaults** tab.
3. Click **Restore Factory Defaults**.
4. To reboot the device immediately after restoring it to the factory defaults, select **Reboot Device**.
5. Click **Apply**.

Figure 25 Restoring the factory defaults



Restore configuration from a backup file

Restrictions and guidelines

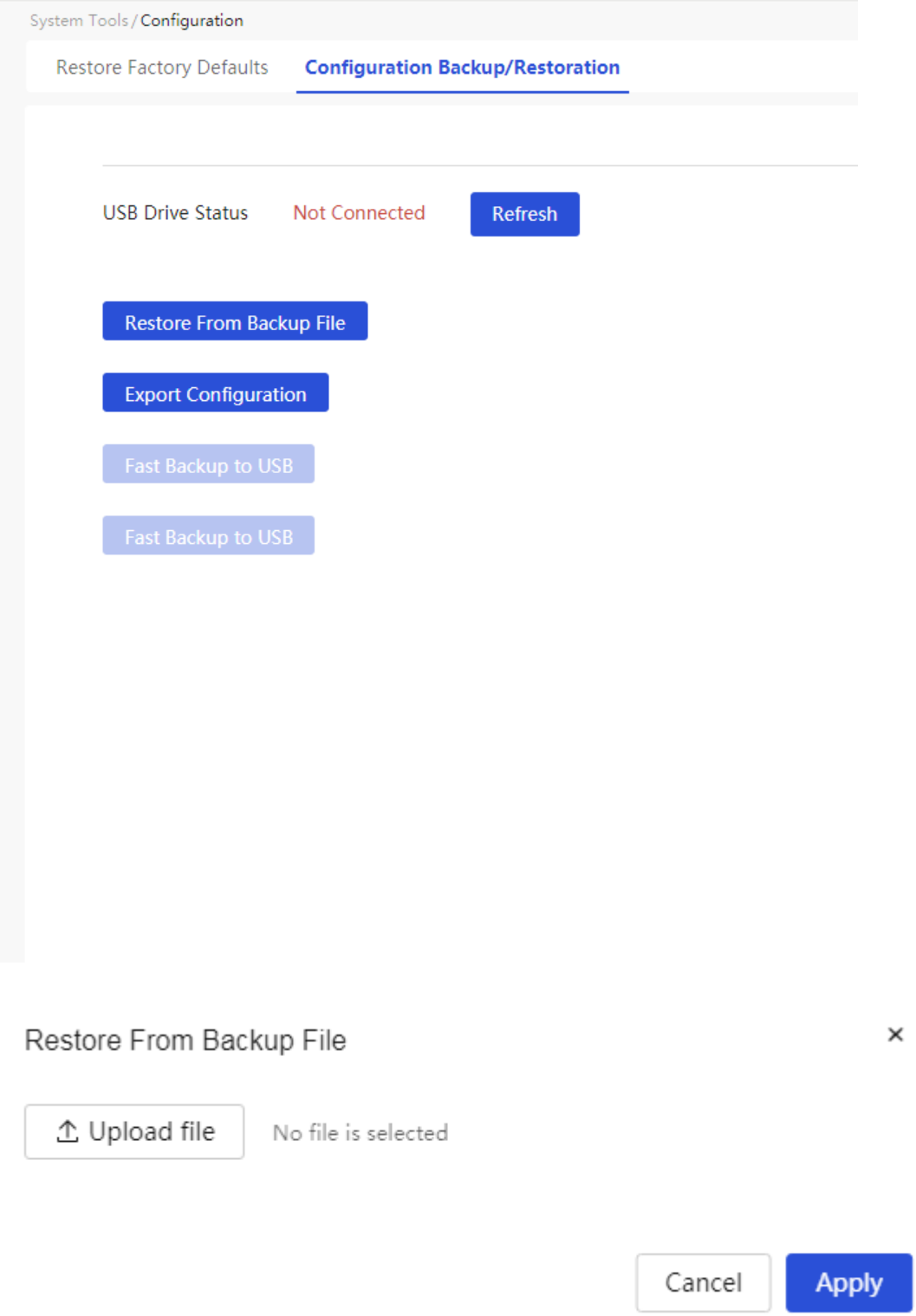
- You can restore the device configuration only from a .rar backup file.
- Ensure stable and normal power supply during device configuration restoration.
- After completing configuration restoration, the device will restart with the new configuration automatically.

Procedure

1. From the left navigation pane, select **System Tools** > **Configuration**.
2. Click the **Configuration Backup/Restoration** tab.
3. Click **Restore From Backup File**.

4. In the dialog box that opens, click **Upload file** to select a backup configuration file.
5. Click **Apply**.
6. In the dialog box that opens, click **Apply**.

Figure 26 Restoring configuration from a backup file



Export the running configuration

1. From the left navigation pane, select **System Tools** > **Configuration**.
2. Click the **Configuration Backup**/**Restoration** tab.
3. Click **Export Configuration** and select the save path. You can export the running configuration to your local PC.

Fast back up the running configuration to a USB drive

Prerequisites

- You can only use a USB drive in FAT32 format.
- Before backing up the running configuration to a USB drive, first insert the USB drive into the device.

Restrictions and guidelines

- If the USB drive has multiple partitions, the backup configuration file will be saved in the first partition.
- The backed up configuration file is named **backup.data**. If you perform the operations multiple times, the system will overwrite the previous configuration file with the new one, and only one **backup.data** configuration file will exist on the USB drive.

Procedure

1. From the left navigation pane, select **System Tools** > **Configuration**.
2. Click the **Configuration Backup**/**Restoration** tab.
3. Click **Fast Backup to USB**.
4. In the dialog box that opens after the backup operation is complete, click **Apply**.

Fast restore the device configuration from a USB drive

Prerequisites

- You can only use a USB drive in FAT32 format.
- To fast restore the device configuration from a USB drive, make sure the USB drive contains a device configuration file named **backup. data** and insert the USB drive into the device. The device will restore its configuration from the **backup. data** configuration file.
- If the USB drive has multiple partitions, the **backup. data** configuration file must be in the first partition.

Restrictions and guidelines

- Ensure stable and normal power supply during device configuration restoration.
- After the device configuration is restored, the device will restart with the new configuration automatically.

Procedure

1. From the left navigation pane, select **System Tools** > **Configuration**.
2. Click the **Configuration Backup**/**Restoration** tab.
3. Click **Fast Restore from USB**.
4. In the dialog box that opens after the restoration operation is complete, click **Apply**.

Upgrade the system

About this feature

Use this feature to upgrade the device software for resolving issues or updating applications.

Restrictions and guidelines

- Save the configuration on the device before you upgrade the software. You use the configuration to restore the system when an issue occurs during the upgrade process.
- After you upload the software image, the device upgrades the software automatically and then restarts.
- For the device to operate correctly, do not power off the device during the upgrade process.
- As a best practice to avoid incompatibility issues, do not use an image file with a lower version or released earlier than the current software.

Manually upgrade the software

Restrictions and guidelines

Before manual upgrade, access the **Security** > **DDoS Attack Prevention** > **Abnormal Traffic Prevention** page to identify whether abnormal traffic prevention is enabled. If it is enabled, disable it, and then perform a manual upgrade.

Procedure

1. From the left navigation pane, select **System Tools** > **System Upgrade**.
2. Click the **Manual Upgrade** tab.
3. Click **Manual Upgrade**.
4. Click **Upload file** to select the file in the specified path.
5. Select whether to restore the factory default configuration after software upgrade.
6. Click **Apply**.

Use a USB drive to restore the system software

When the device has abnormalities during its operation, such as power interruption during the upgrade process or device malfunction, you can use a USB drive to restore the system software.

CAUTION:

Use this feature with caution. After the system software is restored from a USB drive, the device will restore the factory defaults.

The restoration procedure is as follows:

1. Prepare a USB drive with the FAT32 file format and either a USB 2.0 interface or USB 3.0 interface (which is also compatible with USB 2.0).
2. Power off the device, and then insert the USB drive into the USB port of the device.
3. Power on the device and wait for about 10 minutes. After the device starts up correctly, you can log in to it again.

Reboot the device

About this feature

Use this feature to reboot the device immediately or configure scheduled device reboot.

Reboot the device immediately

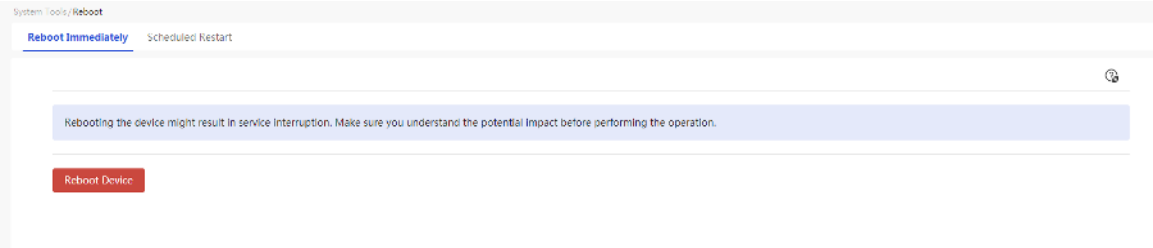
Restrictions and guidelines

A device reboot might result in service interruption. Perform this task with caution.

Procedure

1. From the left navigation pane, select **System Tools** > **Reboot**.
2. On the **Reboot Immediately** tab, click **Reboot Device**. In the dialog that opens, click **Apply**.

Figure 27 Rebooting the device immediately



Configure scheduled reboot

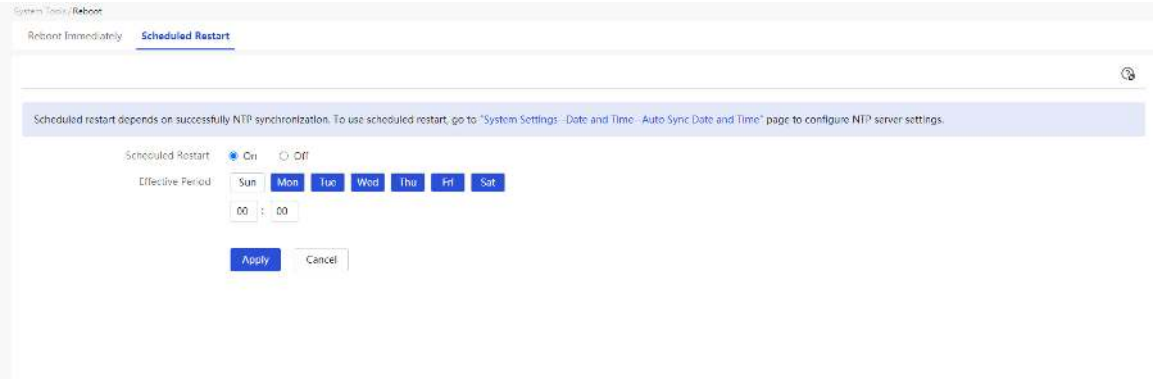
Restrictions and guidelines

Scheduled reboot depends on successful NTP synchronization. To use scheduled reboot, first navigate to the **System Tools** > **System Settings** > **Date and Time** page, select **Auto Sync Date and Time**, and specify an NTP server.

Procedure

1. From the left navigation pane, select **System Tools** > **Reboot**.
2. Click the Scheduled Restart tab.
3. In the **Scheduled Restart** field, enable scheduled reboot. If you enable this feature, the device will reboot as scheduled.
4. In the **Effective Period** field, set the weekday and time at which the device reboots.
5. Click **Apply**.

Figure 28 Configuring scheduled reboot



Manage system logs

About this feature

During operation, the device generates system logs to record the configuration performed by the administrator, device state changes, and important events occurred on the device. Based on the logs, you can monitor device performance and troubleshoot network issues.

You can send logs to log servers for centralized management or view logs directly on the Web page.

Logs are classified into five severity levels from 0 through 4 in descending order of severity. Understanding log severity levels helps you quickly filter out important logs.

Table 1 Log severity

Severity value	Level	Description
0	Error(0)	Error condition.
1	Warning(1)	Warning condition.
2	Notification(2)	Normal but significant condition.
3	Informational(3)	Informational message.
4	Debugging(4)	Debugging message.

Send system logs to a log server

Prerequisites

Make sure the device and the log server can reach each other.

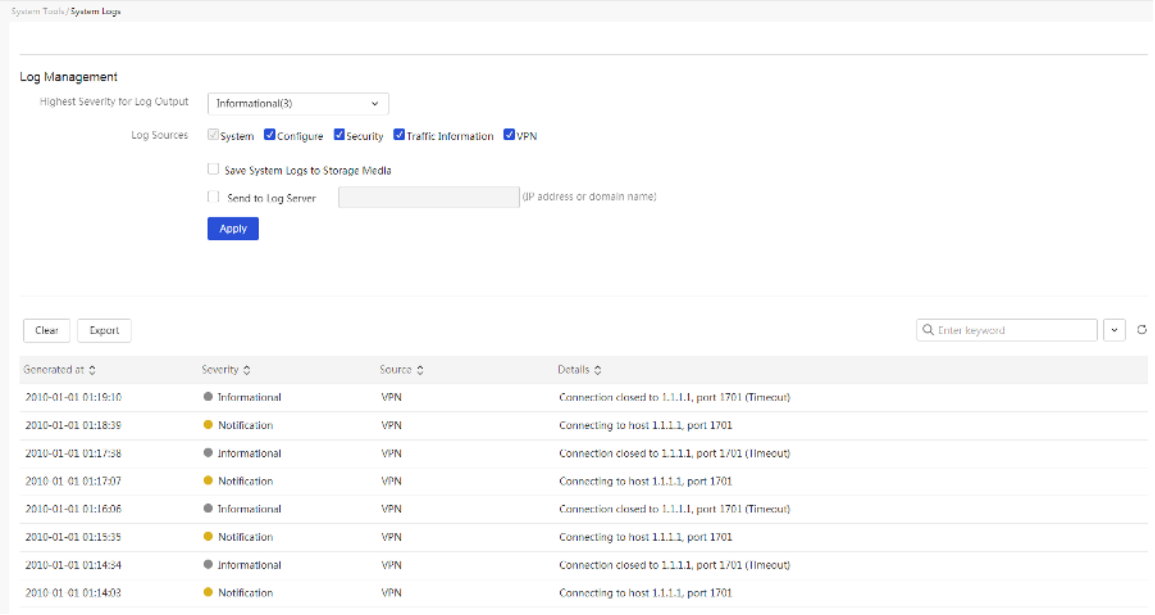
Procedure

1. From the left navigation pane, select **System Tools** > **System Logs**.
2. In the **Highest Severity for Log Output** field, specify the highest severity for log output.
3. In the **Log Sources** field, select log source modules to filter logs. Options include:
   - **System**: Records running status information of some modules during device operation. This parameter is selected by default and cannot be canceled.
   - **Configure**: Records information about changes in device configuration.

- **Security**: Records relevant information about device attack prevention, message filtering, and firewall.
- **Traffic Information**: Records traffic information by IP and port.
- **VPN**: Records VPN-related information.

4. Select the **Save System Logs to Storage Media** option as needed.
5. Select the **Send to Log Server** option and enter the IP address or domain name of the log server.
6. Click **Apply**.

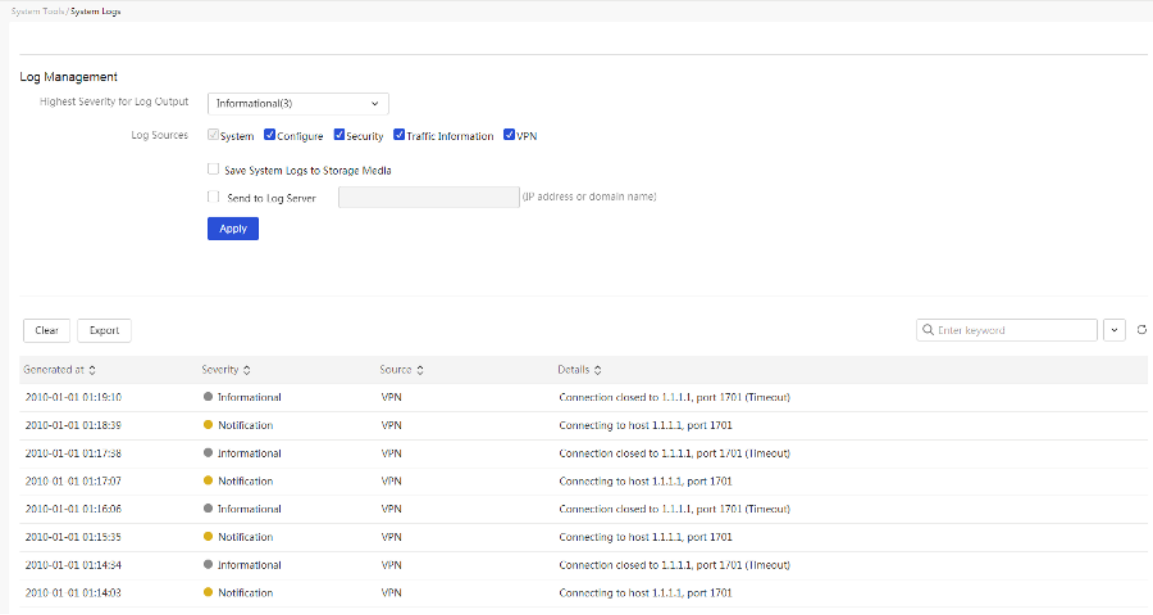
Figure 29 Sending system logs to a log server



View system logs on the Web page

1. From the left navigation pane, select **System Tools** > **System Logs**. The page that opens displays the generation time, severity, and details of each log.
2. You can use the advanced search function to search for system logs by any combination of the filter criteria including generation time, severity, source, and details.
3. Click **Export** to export all existing logs on the device to your PC.

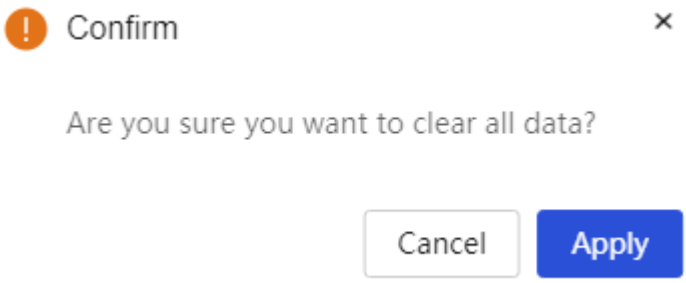
Figure 30 Viewing system logs on the Web page



Clear system logs

1. From the left navigation pane, select **System Tools** > **System Logs**.
2. Click **Clear**.

Figure 31 Clearing system logs



Manage the admin account

About this feature

Use this feature to manage the admin account for the system.

Edit the admin account

Restrictions and guidelines

The system has only one admin account.

You can edit only the password for the admin account but cannot delete the admin account.

Procedure

1. Click the icon of the admin account on the top right corner of the page, and then select **Settings**.
2. To change the password of the current admin account:
   a. In the **Old Password** field, enter the current password.
   b. In the **New Password** field, enter a new password. Make sure the password meets the following requirements:
      – The new password must be a string of 8 to 16 characters. Only uppercase letters, lowercase letters, digits, spaces, and special characters ~`!@#$%^&*()_+-={}|[]\:;'<>,./ are supported. The password string must contain a minimum of two character types (excluding spaces).
      – The new password cannot contain the following strings or characters: String **123**, four consecutive digits, four consecutive identical characters (case sensitive), string **admin** or **nimda** (case insensitive), string **hik**, **hkws**, or **hikvision** (case insensitive) as a separate word. The new password cannot be **1qaz2wsx**, **1qaz@WSX**, **!@#$QWER**, **p@ssword**, **passw0rd**, or **p@ssw0rd** (case sensitive).
   c. In the **Confirm Password** field, confirm the new password by entering the password again.
3. In the **Password hint** field, enter a hint for remembering the password.
4. Click **Apply**.