



User Guide

Omada Gigabit VPN Gateway

CONTENTS

About This Guide

Intended Readers	1
Conventions.....	1
More Information	1

Accessing the Gateway

Determine the Management Method.....	3
Web Interface Access.....	4

Viewing Status Information

System Status.....	7
Traffic Statistics	8
Viewing the Interface Statistics.....	8
Viewing the IP Statistics.....	9

Quick Setup

Configuring Internet.....	12
Traffic Statistics	
Viewing the Interface Statistics.....	
Viewing the IP Statistics.....	

Configuring Network

Overview	15
Supported Features.....	15
WAN Configuration	16
Configuring the Number of WAN Ports.....	16
Configuring the WAN Connection	16
LAN Configuration	26
Configuring the IP Address of the LAN Port.....	26
Configuring the DHCP Server.....	27
Viewing the DHCP Client List.....	29
IPTV Configuration	31
Configuring the IPTV.....	31
MAC Configuration.....	33

Configuring MAC Address	33
Switch Configuration	34
Viewing the Statistics (only for certain devices).....	34
Configuring Port Mirror.....	35
Configuring Rate Control (only for certain devices)	36
Configuring Port Config	37
Viewing Port Status	38
VLAN Configuration	39
Creating a VLAN.....	39
Configuring the PVID of a Port.....	40
IPv6 Configuration.....	42
Configure IPv6 for WAN / SFP WAN port(s)	42
Configuring the WAN Connection	43
Configuring IPv6 for the LAN Port.....	48
USB Configuration	54
Configuring USB Modem	54

USB

Overview	60
USB Modem Configuration	61
Configuring USB Modem automatically.....	61
Configuring the USB Modem manually	63
USB Storage	65
Managing the USB Storage	65
Auto Backup	65
Firmware Upgrade via USB.....	66

Configuring Preferences

Overview	68
IP Group Configuration	69
Adding IP Address Entries.....	69
Grouping IP Address Entries.....	70
IPv6 Group Configuration	71
Adding IP Address Entries.....	71
Grouping IP Address Entries	72
Time Range Configuration.....	73
VPN IP Pool Configuration.....	75

Service Type Configuration.....	76
Configuring Transmission	
Transmission.....	80
Overview.....	80
Supported Features.....	80
NAT Configurations.....	82
Configuring the One-to-One NAT.....	82
Configuring the Virtual Servers.....	83
Configuring the Port Triggering.....	84
Configuring the NAT-DMZ.....	85
Configuring the ALG.....	85
Bandwidth Control Configuration.....	87
Quality of Services Configurations.....	89
Configuring Bandwidth Control.....	89
Configuring Class Rule.....	91
Configuring VoIP Prioritization.....	92
Configuring Tag Prioritization.....	92
Session Limit Configurations.....	93
Configuring Session Limit.....	93
Viewing the Session Limit Information.....	94
Load Balancing Configurations.....	95
Configuring the Load Balancing.....	95
Configuring the Link Backup.....	96
Configuring the Online Detection.....	97
Routing Configurations.....	98
Configuring the Static Routing.....	98
Configuring the Policy Routing.....	99
Viewing the Routing Table.....	100
Configuration Examples.....	101
Example for Configuring NAT.....	101
Network Requirements.....	101
Network Topology.....	101
Configuration Scheme.....	101
Configuration Procedure.....	102
Example for Configuring Load Balancing.....	103
Network Requirements.....	103

Network Topology.....	104
Configuration Scheme.....	104
Configuration Procedure.....	104
Example for Configuring Virtual Server.....	105
Network Requirements.....	105
Network Topology.....	105
Configuration Scheme.....	105
Configuration Procedure.....	105
Example for Configuring Policy Routing.....	106
Network Requirements.....	106
Network Topology.....	107
Configuration Scheme.....	107
Configuration Procedure.....	107

Configuring Firewall

Firewall.....	111
Overview.....	111
Supported Features.....	111
Firewall Configuration.....	113
Anti ARP Spoofing.....	113
Adding IP-MAC Binding Entries.....	113
Enable Anti ARP Spoofing.....	116
Configuring Attack Defense.....	118
Configuring MAC Filtering.....	119
Configuring Access Control.....	121
Configuration Examples.....	123
Example for Anti ARP Spoofing.....	123
Network Requirements.....	123
Configuration Scheme.....	123
Configuration Procedure.....	124
Example for Access Control.....	126
Network Requirements.....	126
Configuration Scheme.....	127
Configuration Procedure.....	127

Configuring Behavior Control

Behavior Control.....	133
-----------------------	-----

Overview.....	133
Supported Features.....	133
Behavior Control Configuration	134
Configuring Web Filtering	134
Configure Web Group Filtering.....	134
Configuring URL Filtering.....	137
Configuring Web Security.....	139
Configuration Examples.....	141
Example for Access Control	141
Network Requirements	141
Configuration Scheme.....	141
Configuration Procedure.....	142
Example for Web Security.....	145
Network Requirements	145
Configuration Scheme.....	145
Configuration Procedure.....	145

Configuring VPN

VPN.....	148
Overview.....	148
Supported Features.....	149
IPSec VPN Configuration.....	153
Configuring the IPSec Policy.....	153
Configuring the Basic Parameters	153
Configuring the Advanced Parameters.....	155
Configuring the Failover Group	157
Verifying the Connectivity of the IPSec VPN tunnel	159
GRE VPN Configuration	160
L2TP Configuration.....	162
Configuring the VPN IP Pool.....	162
Configuring L2TP Globally.....	163
Configuring the L2TP Server	163
Configuring the L2TP Client	164
(Optional) Configuring the L2TP Users.....	166
Verifying the Connectivity of L2TP VPN Tunnel.....	167
PPTP Configuration.....	168
Configuring the VPN IP Pool.....	168

Configuring PPTP Globally	169
Configuring the PPTP Server	169
Configuring the PPTP Client.....	170
(Optional) Configuring the PPTP Users	171
Verifying the Connectivity of PPTP VPN Tunnel	172
OpenVPN Configuration.....	174
Configuring the OpenVPN Server	174
Configuring the OpenVPN Client.....	176
Viewing the OpenVPN Tunnel	177
WireGuard VPN Configuration.....	178
Configuring the WireGuard VPN Server.....	178
Configuring the Peers Settings	179
Users Configuration.....	181

Configuring Authentication

Overview	185
Typical Topology	185
Portal Authentication Process	186
Supported Features	186
Supported Web Server	187
Supported Authentication Server.....	187
Guest Resources.....	187
Local Authentication Configuration.....	188
Configuring the Authentication Page.....	188
Configuring the Local User Account	190
Configuring the Local User Account.....	190
(Optional) Configuring the Backup of Local Users	193
Radius Authentication Configuration	194
Configuring Radius Authentication.....	194
Onekey Online Configuration.....	197
Configuring the Authentication Page.....	197
LDAP Configuration	199
Configuring the Authentication Page.....	199
Guest Resources Configuration.....	201
Configuring the Five Tuple Type	201
Configuring the URL Type.....	203
Configuring LDAP Profiles.....	205

Viewing the Authentication Status.....	207
Configuration Example	208
Network Requirements.....	208
Configuration Scheme	208
Configuration Procedures.....	209
Configuring the Authentication Page.....	209
Configuring Authentication Accounts for the Guests.....	210

Managing Services

Services.....	212
Overview.....	212
Support Features.....	212
Dynamic DNS Configurations	213
Configure and View Peanuthull DDNS.....	213
Configure and View Comexe DDNS	214
Configure and View DynDNS	215
Configure and View NO-IP DDNS.....	217
UPnP Configuration	219
Configuration Example for Dynamic DNS.....	220
Network Requirement	220
Configuration Scheme	220
Configuration Procedure.....	220
Specifying the IP Address of the Host.....	220
Configuring the DDNS function	220
mDNS Configuration.....	222
Reboot Schedule	224
DNS Proxy.....	225
DNSSEC.....	225
DOH.....	226
DOT	227

System Tools

System Tools.....	230
Overview.....	230
Support Features.....	230
Admin Setup	231
Admin Setup.....	231

Remote Management	232
System Setting	232
Controller Settings	234
Enable Cloud-Based Controller Management	234
Configure Controller Inform URL	235
Management.....	236
Factory Default Restore.....	236
Backup & Restore	236
Reboot	237
Firmware Upgrade.....	237
SNMP	238
Diagnostics	239
Diagnostics	239
Configuring Ping	239
Configuring Traceroute	240
Remote Assistance	241
Time Settings	242
Setting the System Time.....	242
Getting time from the Internet Automatically	242
Setting the System Time Manually.....	243
Setting the Daylight Saving Time.....	243
Predefined Mode.....	243
Recurring Mode	244
Date Mode	245
System Log	246

About This Guide

This User Guide provides information for managing Omada Gigabit VPN Gateway. Please read this guide carefully before operation.

Intended Readers

This Guide is intended for network managers familiar with IT concepts and network terminologies.


Conventions

When using this guide, notice that features available in SafeStream series products may vary by model and software version. Availability of SafeStream series products may also vary by region or ISP. All images, steps, and descriptions in this guide are only examples and may not reflect your actual experience.

Some models featured in this guide may be unavailable in your country or region. For local sales information, visit <https://www.tp-link.com>.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute the warranty of any kind, express or implied. Users must take full responsibility for their application of any products.

In this Guide, the following conventions are used:

- The symbol  stands for Note. Notes contain suggestions or references that helps you make better use of your device.
- **Menu Name > Submenu Name > Tab** page indicates the menu structure. **Status > Traffic Statistics > Interface Statistics** means the Interface Statistics page under the Traffic Statistics menu option that is located under the Status menu.
- **Bold** font indicates a button, toolbar icon, menu or menu item.

More Information

- The latest software and documentations can be found at Download Center at <https://www.tp-link.com/support>.
- The Installation Guide (IG) can be found where you find this guide or inside the package of the gateway.
- Specifications can be found on the product page at <https://www.tp-link.com>.
- To ask questions, find answers, and communicate with TP-Link users or engineers, please visit <https://community.tp-link.com> to join TP-Link Community.
- Our Technical Support contact information can be found at the Contact Technical Support page at <https://www.tp-link.com/support>.

Part 1

Accessing the Gateway

CHAPTERS

1. Determine the Management Method
2. Web Interface Access

1 Determine the Management Method

Before building your network, choose a proper method to manage your gateway based on your actual network situation. The gateway supports two configuration options: Standalone Mode or Controller Mode.

■ Controller Mode

If you want to configure and manage a large-scale network centrally, which consists of mass devices such as access points, switches, and gateways, Controller Mode is recommended. In Controller Mode, the gateway can be centrally configured and monitored via Omada SDN Controller.

To prepare the gateway for Omada SDN Controller Management, refer to Controller Settings. For detailed instructions about the network topology in such situations and how to use Omada SDN Controller, refer to the User Guide of Omada SDN Controller. The guide can be found on the download center of our official website: <https://www.tp-link.com/support/download/>.

■ Standalone Mode

If you have a relatively small-sized network and only one or just a small number of devices need to be managed, Standalone Mode is recommended. In Standalone Mode, you can access and manage the gateway using the GUI (Graphical User Interface, also called web interface in this text). The gateway uses two built-in web servers, HTTP server and HTTPS server, for user authentication.

This User Guide introduces how to configure and monitor the gateway in Standalone Mode.

Note:

The GUI is inaccessible while the gateway is managed by a controller. To turn the gateway back to Standalone Mode and access its GUI, you can forget the gateway on the controller or reset the gateway.

2 Web Interface Access

The following example shows how to log in via the web browser.

- 1) Connect a PC to a LAN port of the gateway with an RJ45 port properly. If your computer is configured with a fixed IP address, change it to "Obtain an IP address automatically".
- 2) Open a web browser and type the default management address `http://192.168.0.1` in the address field of the browser, then press the Enter key.

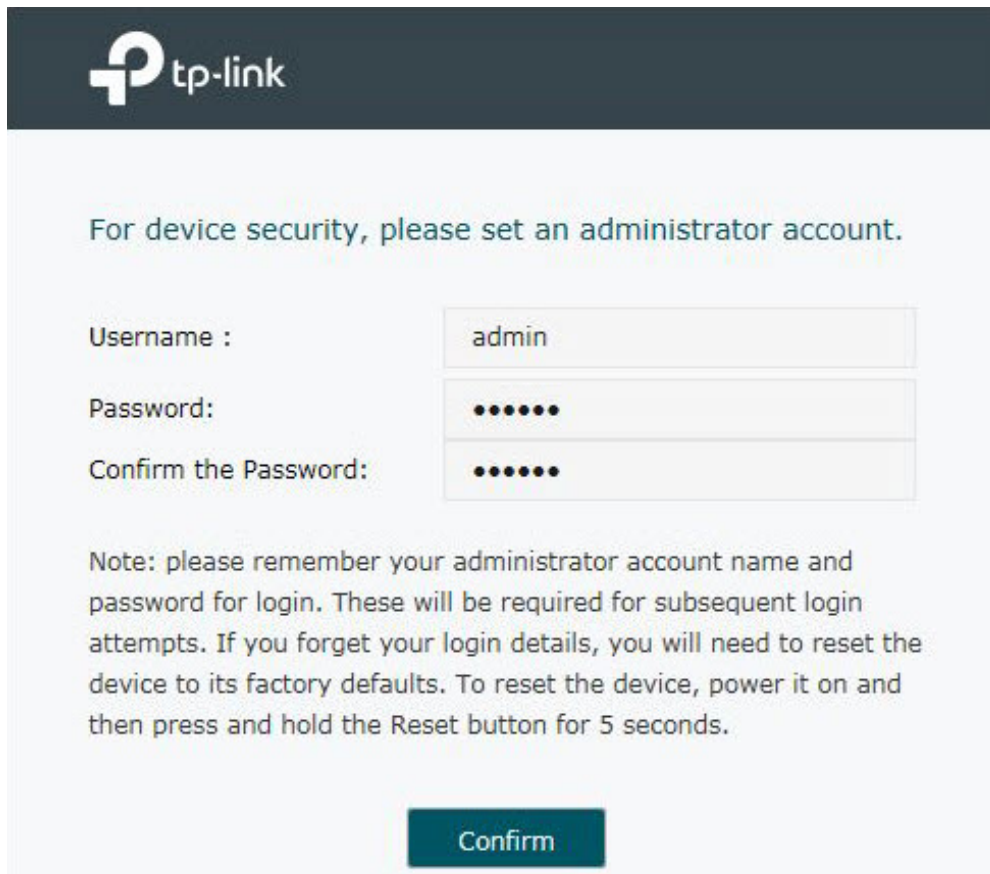
Figure 2-1 Enter the gateway's IP Address In the Browser



A screenshot of a web browser's address bar. On the left, there is a globe icon. To its right, the text "192.168.0.1" is entered in the address field.

- 3) Create a username and a password for subsequent login attempts.

Figure 2-2 Create a Username and a Password



The screenshot shows the TP-Link web interface. At the top left is the TP-Link logo. Below it, a message reads: "For device security, please set an administrator account." There are three input fields: "Username :" with the value "admin", "Password:" with six dots, and "Confirm the Password:" with six dots. Below these fields is a note: "Note: please remember your administrator account name and password for login. These will be required for subsequent login attempts. If you forget your login details, you will need to reset the device to its factory defaults. To reset the device, power it on and then press and hold the Reset button for 5 seconds." At the bottom center is a dark teal button labeled "Confirm".

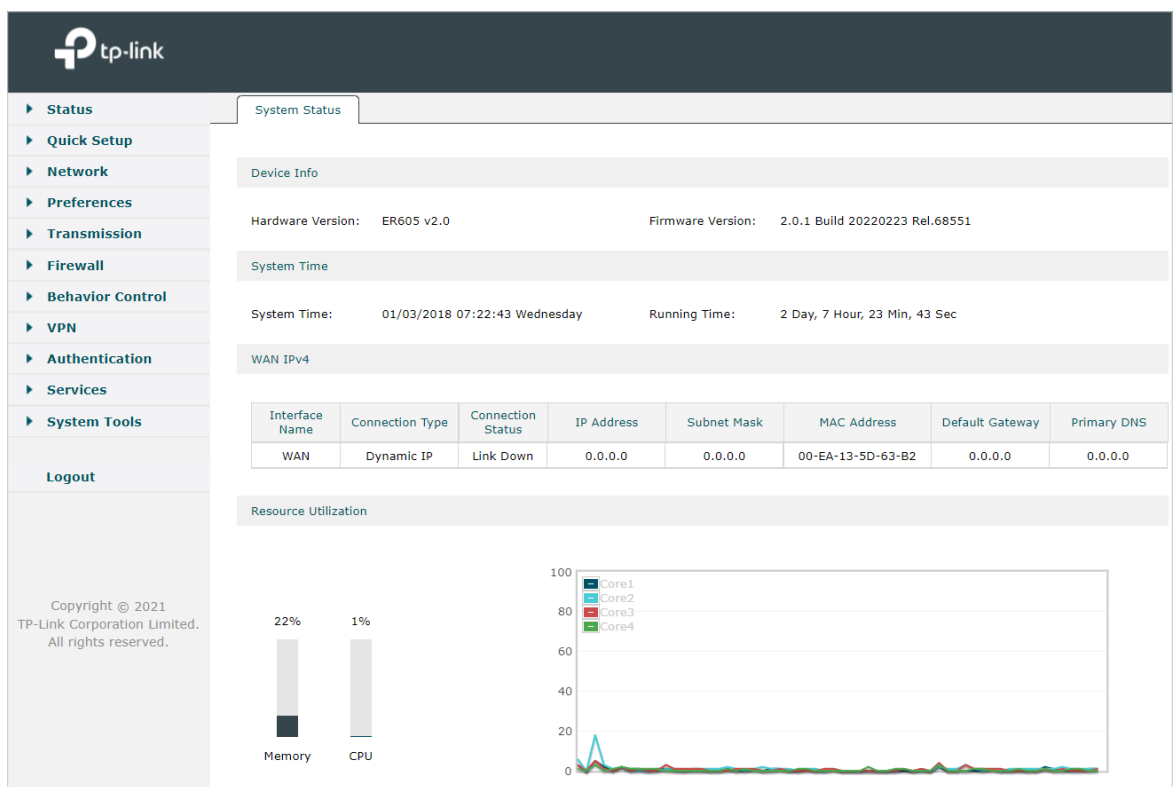
- 4) Use the username and password set above to log in to the webpage.

Figure 2-3 Login Authentication



- 5) After a successful login, the main page will appear as shown below, and you can configure the function by clicking the setup menu on the left side of the screen.

Figure 2-4 Web Interface



Part 2

Viewing Status Information

CHAPTERS

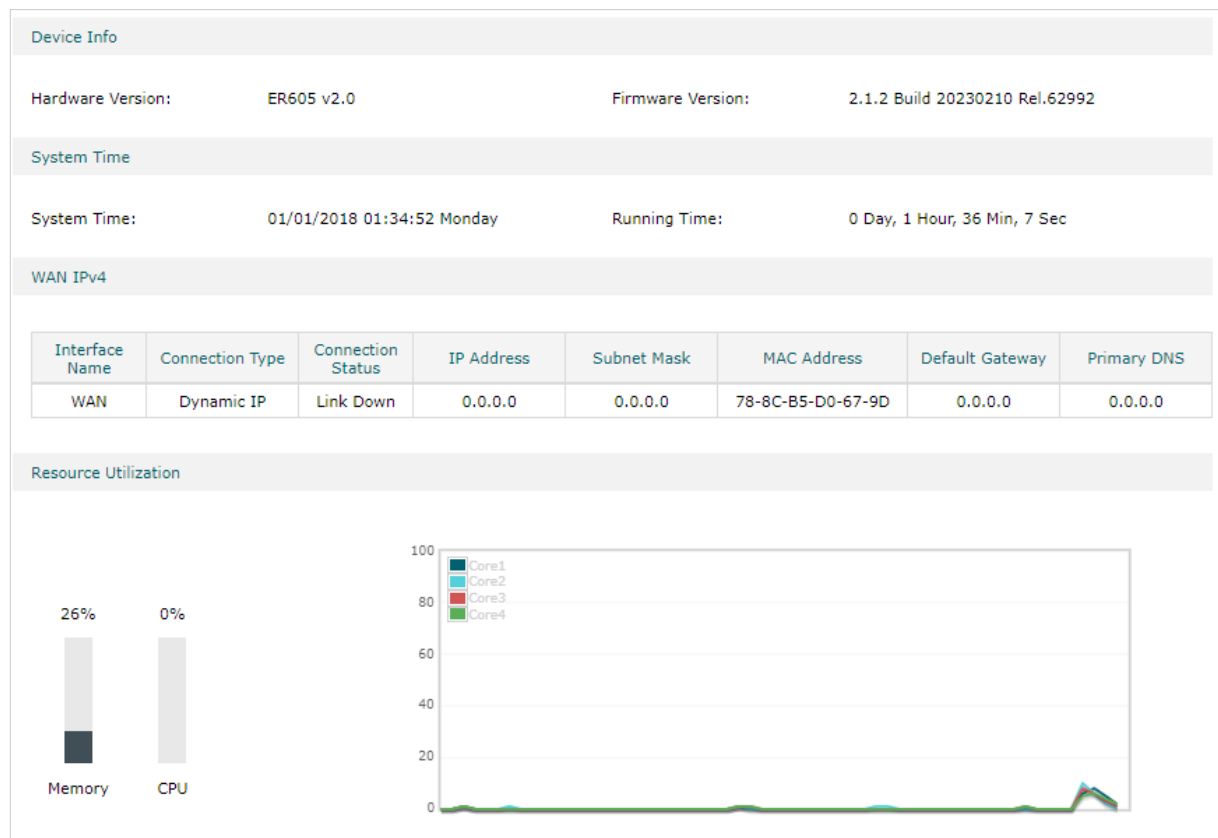
1. System Status
2. Traffic Statistics

1 System Status

The System Status page displays the basic system information (like the hardware version, firmware version and system time) and the running information (like the WAN interface status, memory utilization and CPU utilization).

Choose the menu **Status > System Status > System Status** to load the following page.

Figure 1-1 System Status



2 Traffic Statistics

Traffic Statistics displays detailed information relating to the data traffic of interfaces and IP addresses. You can monitor the traffic and locate faults according to this information.

With the Traffic Statistics function, you can:

- View the traffic statistics on each interface.
- Specify an IP address range, and view the traffic statistics of the IP addresses in this range.

2.1 Viewing the Interface Statistics

Choose the menu **Status > Traffic Statistics > Interface Statistics** to load the following page.

Figure 2-1 Interface Statistics

Statistics List								
Interface	TX Rate (KB/s)	RX Rate (KB/s)	TX Packet Rate (Pkt/s)	RX Packet Rate (Pkt/s)	Total TX Bytes	Total RX Bytes	Total TX Packets	Total RX Packets
LAN1	2	1	5	5	3.1M	253134	2613	2415
WAN	---	---	---	---	2802	---	11	---
WAN/LAN1	---	---	---	---	---	---	---	---
WAN/LAN2	---	---	---	---	---	---	---	---
WAN/LAN3	---	---	---	---	---	---	---	---

Clear Refresh Auto Refresh

View the detailed traffic information of each interface in the statistics list.

TX Rate (KB/s)	Displays the rate for transmitting data in kilobytes per second.
RX Rate (KB/s)	Displays the rate for receiving data in kilobytes per second.
TX Packet Rate (Pkt/s)	Displays the rate for transmitting data in packets per second.
RX Packet Rate (Pkt/s)	Displays the rate for receiving data in packets per second.
Total TX Bytes	Displays the bytes of packets transmitted on the interface.
Total RX Bytes	Displays the bytes of packets received on the interface.
Total TX Packets	Displays the number of packets transmitted on the interface.
Total RX Packets	Displays the number of packets received on the interface.

You can enable **Auto Refresh** or click **Refresh** to get the latest statistics information, or click **Clear** to clear the current statistics information.

2.2 Viewing the IP Statistics

Choose the menu **Status > Traffic Statistics > IP Statistics** to load the following page.

Figure 2-2 IP Statistics

Settings

Enable IP Statistics

IP Range : /

Statistics List

IP Address Number: 0 Auto Refresh

IP Address	TX Rate (KB/s)	RX Rate (KB/s)	TX Packet Rate (Pkt/s)	RX Packet Rate (Pkt/s)	Total TX Bytes	Total RX Bytes	Total TX Packets	Total RX Packets
--	--	--	--	--	--	--	--	--

Follow these steps to view the traffic statistics of the specific IP addresses:

- 1) In the **Settings** section, enable IP Statistics and specify an IP range to monitor.

Enable IP Statistics	Check the box to enable IP Statistics.
IP Range	Specify an IP range. The gateway will monitor the packets whose source IP addresses or destination IP addresses are in this range, and display the statistics information in Statistics List.

- 2) In the **Statistics List** section, view the detailed traffic information of the IP addresses.

IP Address Number	Displays the number of active users whose IP address is in the specified IP range.
TX Rate (KB/s)	Displays the rate for transmitting data in kilobytes per second.
RX Rate (KB/s)	Displays the rate for receiving data in kilobytes per second.
TX Packet Rate (Pkt/s)	Displays the rate for transmitting data in packets per second.
RX Packet Rate (Pkt/s)	Displays the rate for receiving data in packets per second.
Total TX Bytes	Displays the bytes of packets transmitted by the user who owns the IP address.
Total RX Bytes	Displays the bytes of packets received by the user who owns the IP address.

Total TX Packets	Displays the number of packets transmitted by the user who owns the IP address.
------------------	---

Total RX Packets	Displays the number of packets received by the user who owns the IP address.
------------------	--

You can enable **Auto Refresh** or click **Refresh** to get the latest statistics information, or click **Clear** to clear the current statistics information.

Part 3

Quick Setup

CHAPTERS

1. [Configuring Internet](#)

1 Configuring Internet

The quick setup will tell you how to configure the basic network parameters. To start quick setup, choose the menu **Quick Setup > Quick Setup** and click **Let's Get Started** to load the following page.

Figure 1-1 Quick Setup

In the **Quick Setup** section, enable and configure the desired WAN port(s) according to your needs. Then click **Next**.

Location	Automatically selects and displays the region when the USB modem and SIM card are successfully identified. If not, select the region from the drop-down menu.
Mobile ISP	Displays the ISP of the 3G/4G network. If not automatically detected, select the ISP from the drop-down menu.
Primary WAN	Specify the primary WAN port.
Dial Number, APN, Username and Password manually	Displays the rate for transmitting data in packets per second.

Connection Type	<p>The gateway supports five connection types: Static IP, Dynamic IP, PPPoE, L2TP, PPTP, you can choose one according to the service provided by your ISP.</p> <p>Static IP: Select this type if your ISP has offered you a fixed IP address.</p> <p>Dynamic IP: Select this type if your ISP automatically assigns the IP address.</p> <p>PPPoE: Select this type if your ISP provides you with a PPPoE account.</p> <p>L2TP: Select this type if your ISP provides you with an L2TP account.</p> <p>PPTP: Select this type if your ISP provides you with a PPTP account</p>
------------------------	---

 **Note:**

- Only WAN, WAN/LAN, SFP WAN (for certain devices) and USB Modem can function as WAN port.
 - If you change the WAN ports, the gateway will reboot after you complete the configuration. Please go to [Network > WAN](#) to check the connection status after reboot.
 - For more information about USB Modem configuration, refer to [USB Configuration](#).
 - For more information about WAN port configuration, refer to [Configuring the WAN Connection](#).
-

Part 4

Configuring Network

CHAPTERS

1. Overview
2. WAN Configuration
3. LAN Configuration
4. IPTV Configuration
5. MAC Configuration
6. Switch Configuration
7. VLAN Configuration
8. IPv6 Configuration

1 Overview

The Network module provides basic gateway functions, including WAN connection, DHCP service, VLAN and more.

1.1 Supported Features

WAN

WAN ports connect to the internet. You can configure multiple WAN ports for your network. Each WAN port has its own connection type and parameters, which you should configure according to the requirements of your ISP.

LAN

When the LAN ports of the gateway connect to your local network devices, the gateway functions as the gateway, which allows those devices to connect to the internet.

IPTV

Configure IPTV settings to enable Internet/IPTV/Phone service provided by your ISP (internet service provider).

MAC

You can change the default MAC address of the WAN port according to your needs.

Switch

The gateway supports some basic switch port management functions, like Port Mirror, Rate Control, Flow Control and Port Negotiation, to help you monitor the traffic and manage the network effectively.

VLAN

VLAN enables you to divide the LAN into multiple logical networks and control the traffic among them in a convenient and flexible way. The LAN can be logically segmented by departments, application, or types of users, without regard to geographic locations.

IPv6

IPv6 is the next-generation network protocol following IPv4. You can configure IPv6 network for the gateway if your ISP supports IPv6. IPv6 network won't cause conflict with your current IPv4 network..

2 WAN Configuration

You can configure multiple WAN ports for your network. Each WAN port can have its own WAN connection, providing link backup and load balancing.

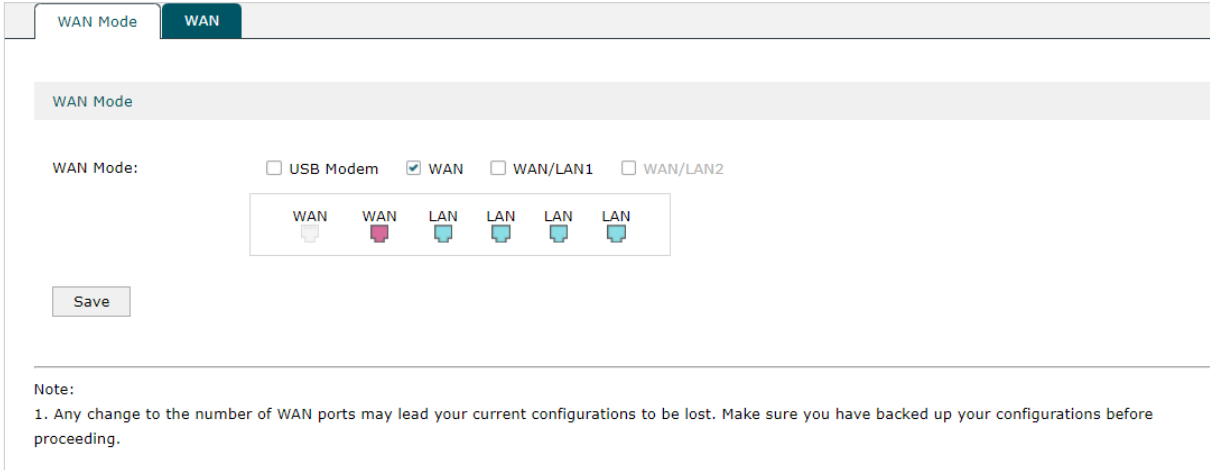
To complete WAN configuration, follow these steps:

- 1) Configure the number of WAN ports.
- 2) Configure the WAN connection.

2.1 Configuring the Number of WAN Ports

Choose the menu **Network > WAN > WAN Mode** to load the following page.

Figure 2-1 Configuring the WAN Mode



WAN Mode

Determine the number of WAN ports according to your needs. To enable a port as WAN port, check the box of the desired port. To configure multiple WAN ports, enable the ports one by one. Only WAN, WAN/LAN, SFP WAN (for certain devices) and USB Modem can function as WAN port.

Note:

Any change to the number of WAN ports may lead your current configurations to be lost. Make sure you have backed up your configurations before proceeding.

2.2 Configuring the WAN Connection

The gateway supports five connection types: **Static IP, Dynamic IP, PPPoE, L2TP, PPTP**, you can choose one according to the service provided by your ISP.

Static IP: If your ISP provides you with a fixed IP address and the corresponding parameters, choose Static IP.

Dynamic IP: If your ISP automatically assigns the IP address and the corresponding parameters, choose Dynamic IP.

PPPoE: If your ISP provides you with a PPPoE account, choose PPPoE.

L2TP: If your ISP provides you with an L2TP account, choose L2TP.

PPTP: If your ISP provides you with a PPTP account, choose PPTP.

Note:

The number of configurable WAN ports is decided by **WAN Mode**. To configure **Wan Mode**, refer to [Configuring the Number of WAN Ports](#).

■ Configuring the Dynamic IP

Choose the menu **Network > WAN > WAN** to load the following page.

Figure 2-2 Configuring the Dynamic IP

Connection Configuration		Connection Status	
Connection Type:	Dynamic IP	Connection Status	Disconnected
Host Name:	(Optional)	IP Address	0.0.0.0
Upstream Bandwidth:	1000000 Kbps (100-1000000)	Subnet Mask	0.0.0.0
Downstream Bandwidth:	1000000 Kbps (100-1000000)	Default Gateway	0.0.0.0
MTU:	1500 (576-1500)	Primary DNS	0.0.0.0
Primary DNS:	(Optional)	Secondary DNS	0.0.0.0
Secondary DNS:	(Optional)		
Vlan:	10		
<input type="checkbox"/> Get IP using Unicast DHCP			
<input type="button" value="Save"/> <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>			

In the **Connection Configuration** section, select the connection type as Dynamic IP. Enter the corresponding parameters and click **Save**.

Connection Type	Choose the connection type as Dynamic IP if your ISP automatically assigns the IP address.
Host Name	(Optional) Enter a name for the gateway. It is null by default.
Upstream Bandwidth	Specify the upstream bandwidth of the WAN port. The value configured here is the upper limit of the "Maximum Upstream Bandwidth" on Transmission > Bandwidth Control > Bandwidth Control page, to make "Bandwidth Control" take effect, please ensure this parameter is set correctly.
Downstream Bandwidth	Specify the downstream bandwidth of the WAN port. The value configured here is the upper limit of the "Maximum Downstream Bandwidth" on Transmission > Bandwidth Control > Bandwidth Control page, to make "Bandwidth Control" take effect, please ensure this parameter is set correctly.

MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When Dynamic IP is selected, MTU can be set in the range of 576-1500 bytes. The default value is 1500.
Primary/ Secondary DNS	(Optional) Enter the IP address of the DNS server provided by your ISP.
VLAN	Add the WAN port to a VLAN. Generally, you don't need to manually configure it unless required by your ISP. By default, the WAN port is automatically assigned to a VLAN, and the egress rule of the VLAN is UNTAG, so the packets are transmitted by the WAN port without VLAN tags. If you want the WAN port to transmit packets with VLAN tag, you need to create the corresponding VLAN first and configure its egress rule as TAG, then manually add the WAN port to that VLAN. To create VLANs, go to Network > VLAN > VLAN .
Get IP using Unicast DHCP	The broadcasting requirement may not be supported by a few ISPs. Select this option if you can not get the IP address from your ISP even with a normal network connection. This option is not required generally.
Connect/ Disconnect	Click the button to active/terminate the connection.

■ **Configuring the Static IP**

Choose the menu **Network > WAN > WAN** to load the following page.

Figure 2-3 Configuring the Static IP

Connection Configuration		Connection Status	
Connection Type:	Static IP ▼	Connection Status	Disconnected
IP Address:	<input type="text"/>	IP Address	0.0.0.0
Subnet Mask:	<input type="text"/>	Subnet Mask	0.0.0.0
Default Gateway:	<input type="text"/> (Optional)	Default Gateway	0.0.0.0
Upstream Bandwidth:	1000000 Kbps (100-1000000)	Primary DNS	0.0.0.0
Downstream Bandwidth:	1000000 Kbps (100-1000000)	Secondary DNS	0.0.0.0
MTU:	1500 (576-1500)		
Primary DNS:	<input type="text"/> (Optional)		
Secondary DNS:	<input type="text"/> (Optional)		
Vlan:	336 ▼		
<input type="button" value="Save"/>			

In **Connection Configuration** section, select the connection type as Static IP. Enter the corresponding parameters and click **Save**.

Connection Type	Choose the connection type as Static IP if your ISP has offered you a fixed IP address.
IP Address	Enter the IP address provided by your ISP.

Subnet Mask	Enter the subnet mask provided by your ISP.
Default Gateway	Enter the default gateway provided by your ISP.
Upstream Bandwidth	Specify the downstream bandwidth of the WAN port. The value configured here is the upper limit of the "Maximum Downstream Bandwidth" on Transmission > Bandwidth Control > Bandwidth Control page, to make "Bandwidth Control" take effect, please ensure this parameter is set correctly.
Downstream Bandwidth	Specify the downstream bandwidth of the WAN port. The value configured here is the upper limit of the "Maximum Downstream Bandwidth" on Transmission > Bandwidth Control > Bandwidth Control page, to make "Bandwidth Control" take effect, please ensure this parameter is set correctly.
MTU	<p>Specify the MTU (Maximum Transmission Unit) of the WAN port.</p> <p>MTU is the maximum data unit transmitted in the physical network. When Static IP is selected, MTU can be set in the range of 576-1500 bytes. The default value is 1500.</p>
Primary/ Secondary DNS	(Optional) Enter the IP address of the DNS server provided by your ISP.
VLAN	<p>Add the WAN port to a VLAN. Generally, you don't need to manually configure it unless required by your ISP.</p> <p>By default, the WAN port is automatically assigned to a VLAN, and the egress rule of the VLAN is UNTAG, so the packets are transmitted by the WAN port without VLAN tags. If you want the WAN port to transmit packets with VLAN tag, you need to create the corresponding VLAN first and configure its egress rule as TAG, then manually add the WAN port to that VLAN. To create VLANs, go to Network > VLAN > VLAN.</p>

■ **Configuring the PPPoE**

Choose the menu **Network > WAN > WAN** to load the following page.

Figure 2-4 Configuring the PPPoE

Connection Configuration		Connection Status	
Connection Type:	PPPoE	Connection Status	Disconnected
Username:		IP Address	0.0.0.0
Password:		Subnet Mask	0.0.0.0
Connection Mode:	Connect Automatically	Default Gateway	0.0.0.0
Upstream Bandwidth:	1000000 Kbps (100-1000000)	Primary DNS	0.0.0.0
Downstream Bandwidth:	1000000 Kbps (100-1000000)	Secondary DNS	0.0.0.0
MTU:	1492 (576-1492)	Secondary Connection	
Service Name:	(1-128 characters, optional)	IP Address	0.0.0.0
Primary DNS:	(Optional)	Subnet Mask	0.0.0.0
Secondary DNS:	(Optional)		
Vlan:	10		
Secondary Connection:	<input type="radio"/> None <input type="radio"/> Dynamic IP <input checked="" type="radio"/> Static IP		
IP Address:			
Subnet Mask:			
<input type="button" value="Save"/> <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>			

In the **Connection Configuration** section, select the connection type as PPPoE. Enter the corresponding parameters and click **Save**.

Connection Type	Choose the connection type as PPPoE if your ISP provides you with a PPPoE account.
Username	Enter the PPPoE username provided by your ISP.
Password	Enter the PPPoE password provided by your ISP.
Connection Mode	<p>Choose the connection mode, including Connect Automatically, Connect Manually and Time-Based.</p> <p>Connect Automatically: The gateway will activate the connection automatically when the gateway reboots or the connection is down.</p> <p>Connect Manually: You can manually activate or terminate the connection.</p> <p>Time-Based: During the specified period, the gateway will automatically activate the connection.</p>
Time	Choose the effective time range when the Connection Mode is chosen as Time-Based . To create the time range, go to Preferences > Time Range > Time Range .
Upstream Bandwidth	Specify the upstream bandwidth of the WAN port. The value configured here is the upper limit of the "Maximum Upstream Bandwidth" on Transmission > Bandwidth Control > Bandwidth Control page, to make "Bandwidth Control" take effect, please ensure this parameter is set correctly.

Downstream Bandwidth	Specify the downstream bandwidth of the WAN port. The value configured here is the upper limit of the "Maximum Downstream Bandwidth" on Transmission > Bandwidth Control > Bandwidth Control page, to make "Bandwidth Control" take effect, please ensure this parameter is set correctly.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When PPPoE is selected, MTU can be set in the range of 576-1492 bytes. The default value is 1492.
Service Name	(Optional) Enter the service name. This parameter is not required unless provided by your ISP. It is null by default.
Primary/ Secondary DNS	(Optional) Enter the IP address of the DNS server provided by your ISP.
VLAN	Add the WAN port to a VLAN. Generally, you don't need to manually configure it unless required by your ISP. By default, the WAN port is automatically assigned to a VLAN, and the egress rule of the VLAN is UNTAG, so the packets are transmitted by the WAN port without VLAN tags. If you want the WAN port to transmit packets with VLAN tag, you need to create the corresponding VLAN first and configure its egress rule as TAG, then manually add the WAN port to that VLAN. To create VLANs, go to Network > VLAN > VLAN .
Secondary Connection	Secondary connection is required by some ISPs. Select the connection type required by your ISP. None: Select this if the secondary connection is not required by your ISP. Dynamic IP: Select this if your ISP automatically assigns the IP address and subnet mask for the secondary connection. Static IP: Select this if your ISP provides you with a fixed IP address and subnet mask for the secondary connection.
Connect/ Disconnect	Click the button to active/terminate the connection.

■ **Configuring the L2TP**

Choose the menu **Network > WAN > WAN** to load the following page.

Figure 2-5 Configuring the L2TP

Connection Configuration		Connection Status	
Connection Type:	L2TP	Connection Status	Disconnected
Username:		IP Address	0.0.0.0
Password:		Subnet Mask	0.0.0.0
Connection Mode:	Connect Automatically	Default Gateway	0.0.0.0
Upstream Bandwidth:	1000000 Kbps (100-1000000)	Primary DNS	0.0.0.0
Downstream Bandwidth:	1000000 Kbps (100-1000000)	Secondary DNS	0.0.0.0
MTU:	1460 (576-1460)	Secondary Connection	
Primary DNS:	(Optional)	IP Address	0.0.0.0
Secondary DNS:	(Optional)	Subnet Mask	0.0.0.0
Vlan:		Default Gateway	0.0.0.0
Secondary Connection:	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP	Primary DNS	0.0.0.0
VPN Server IP/Domain Name:		Secondary DNS	0.0.0.0
IP Address:			
Subnet Mask:			
Default Gateway:	(Optional)		
Primary DNS:	(Optional)		
Secondary DNS:	(Optional)		
<input type="button" value="Save"/> <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>			

In the **Connection Configuration** section, select the connection type as L2TP. Enter the corresponding parameters and click **Save**.

Connection Type	Choose the connection type as L2TP if your ISP provides you with an L2TP account.
Username	Enter the L2TP username provided by your ISP.
Password	Enter the L2TP password provided by your ISP.
Connection Mode	<p>Choose the connection mode, including Connect Automatically, Connect Manually and Time-Based.</p> <p>Connect Automatically: The gateway will activate the connection automatically when the gateway reboots or the connection is down.</p> <p>Connect Manually: You can manually activate or terminate the connection.</p> <p>Time-Based: During the specified period, the gateway will automatically activate the connection.</p>
Time	Choose the effective time range when the Connection Mode is chosen as Time-Based . To create the time range, go to Preferences > Time Range > Time Range .

Upstream Bandwidth	Specify the upstream bandwidth of the WAN port. The value configured here is the upper limit of the "Maximum Upstream Bandwidth" on Transmission > Bandwidth Control > Bandwidth Control page, to make "Bandwidth Control" take effect, please ensure this parameter is set correctly.
Downstream Bandwidth	Specify the downstream bandwidth of the WAN port. The value configured here is the upper limit of the "Maximum Downstream Bandwidth" on Transmission > Bandwidth Control > Bandwidth Control page, to make "Bandwidth Control" take effect, please ensure this parameter is set correctly.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When L2TP is selected, MTU can be set in the range of 576-1460 bytes. The default value is 1460.
Primary/Secondary DNS	(Optional) Enter the IP address of the DNS server provided by your ISP.
VLAN	Add the WAN port to a VLAN. Generally, you don't need to manually configure it unless required by your ISP. By default, the WAN port is automatically assigned to a VLAN, and the egress rule of the VLAN is UNTAG, so the packets are transmitted by the WAN port without VLAN tags. If you want the WAN port to transmit packets with VLAN tag, you need to create the corresponding VLAN first and configure its egress rule as TAG, then manually add the WAN port to that VLAN. To create VLANs, go to Network > VLAN > VLAN .
Secondary Connection	Select the secondary connection type provided by your ISP. If you select the secondary connection type as Static IP, you need to configure IP Address, Subnet Mask, Default Gateway, Primary/Second DNS. The secondary connection is required for L2TP connection. The gateway will get some necessary information after the secondary connection succeeded. These information will be used in the L2TP connection process.
VPN Server/Domain Name	Enter the VPN Server/Domain Name provided by your ISP.
IP Address	Enter the IP address provided by your ISP for the secondary connection.
Subnet Mask	Enter the subnet mask provided by your ISP for the secondary connection.
Default Gateway	Enter the default gateway provided by your ISP for the secondary connection.
Primary/Secondary DNS	Enter the primary/secondary DNS provided by your ISP for the secondary connection.
Connect/Disconnect	Click the button to active/terminate the connection.

■ **Configuring the PPTP**

Choose the menu **Network > WAN > WAN** to load the following page.

Figure 2-6 Configuring the PPTP

Connection Configuration		Connection Status	
Connection Type:	PPTP	Connection Status	Disconnected
Username:		IP Address	0.0.0.0
Password:		Subnet Mask	0.0.0.0
Connection Mode:	Connect Automatically	Default Gateway	0.0.0.0
Upstream Bandwidth:	1000000 Kbps (100-1000000)	Primary DNS	0.0.0.0
Downstream Bandwidth:	1000000 Kbps (100-1000000)	Secondary DNS	0.0.0.0
MTU:	1420 (576-1420)	Secondary Connection	
Primary DNS:	(Optional)	IP Address	0.0.0.0
Secondary DNS:	(Optional)	Subnet Mask	0.0.0.0
Vlan:		Default Gateway	0.0.0.0
Secondary Connection:	<input checked="" type="radio"/> Dynamic IP <input type="radio"/> Static IP	Primary DNS	0.0.0.0
VPN Server IP/Domain Name:		Secondary DNS	0.0.0.0
IP Address:			
Subnet Mask:			
Default Gateway:	(Optional)		
Primary DNS:	(Optional)		
Secondary DNS:	(Optional)		
<input type="button" value="Save"/> <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>			

In **Connection Configuration** section, select the connection type as PPTP. Enter the corresponding parameters and click **Save**.

Connection Type	Choose the connection type as PPTP if your ISP provides you with a PPTP account.
Username	Enter the PPTP username provided by your ISP.
Password	Enter the PPTP password provided by your ISP.
Connection Mode	<p>Choose the connection mode, including Connect Automatically, Connect Manually and Time-Based.</p> <p>Connect Automatically: The gateway will activate the connection automatically when the gateway reboots or the connection is down.</p> <p>Connect Manually: You can manually activate or terminate the connection.</p> <p>Time-Based: During the specified period, the gateway will automatically activate the connection.</p>
Time	Choose the effective time range when the Connection Mode is chosen as Time-Based . To create the time range, go to Preferences > Time Range > Time Range .

Upstream Bandwidth	Specify the upstream bandwidth of the WAN port. The value configured here is the upper limit of the "Maximum Upstream Bandwidth" on Transmission > Bandwidth Control > Bandwidth Control page, to make "Bandwidth Control" take effect, please ensure this parameter is set correctly.
Downstream Bandwidth	Specify the downstream bandwidth of the WAN port. The value configured here is the upper limit of the "Maximum Downstream Bandwidth" on Transmission > Bandwidth Control > Bandwidth Control page, to make "Bandwidth Control" take effect, please ensure this parameter is set correctly.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port. MTU is the maximum data unit transmitted in the physical network. When PPTP is selected, MTU can be set in the range of 576-1420 bytes. The default value is 1420.
Primary/Secondary DNS	(Optional) Enter the IP address of the DNS server provided by your ISP.
VLAN	Add the WAN port to a VLAN. Generally, you don't need to manually configure it unless required by your ISP. By default, the WAN port is automatically assigned to a VLAN by default, and the egress rule of the VLAN is UNTAG, so the packets are transmitted by the WAN port without VLAN tags. If you want the WAN port to transmit packets with VLAN tag, you need to create the corresponding VLAN first and configure its egress rule as TAG, then manually add the WAN port to that VLAN. To create VLANs, go to Network > VLAN > VLAN .
Secondary Connection	Select the secondary connection type provided by your ISP. If you select the secondary connection type as Static IP, you need to configure IP Address, Subnet Mask, Default Gateway, Primary/Second DNS. The secondary connection is required for PPTP connection. The gateway will get some necessary information after the secondary connection succeeded. These information will be used in the PPTP connection process.
VPN Server/Domain Name	Enter the VPN Server/Domain Name provided by your ISP.
IP Address	Enter the IP address provided by your ISP for the secondary connection.
Subnet Mask	Enter the subnet mask provided by your ISP for the secondary connection.
Default Gateway	Enter the default gateway provided by your ISP for the secondary connection.
Primary/Secondary DNS	Enter the primary/secondary DNS provided by your ISP for the secondary connection.
Connect/Disconnect	Click the button to active/terminate the connection.

3 LAN Configuration

The LAN port is used to connect to the LAN clients, and works as the default gateway for these clients. You can configure the DHCP server for the LAN clients, and clients will automatically be assigned to IP addresses if the method of obtaining IP addresses is set as "Obtain IP address automatically".

For LAN configuration, you can:

- Configure the IP address of the LAN port.
- Configure the DHCP server.

3.1 Configuring the IP Address of the LAN Port

Choose the menu **Network > LAN > LAN** to load the following page.

Figure 3-1 Configuring the LAN IP Address

The screenshot shows the configuration page for LAN1. The fields are as follows:

LAN1	
IP Address:	192.168.0.1
Subnet Mask:	255.255.255.0
Vlan:	1 (1-4086)
IGMP Proxy:	<input checked="" type="checkbox"/> Enable
IGMP Version:	V2 ▼
<input type="button" value="Save"/>	

Enter the IP address of the LAN port, and click **Save**.

IP Address

Enter the IP address of the LAN port.

This IP address is the default gateway of the LAN clients, and the IP addresses of all the LAN clients should be in the same subnet with this LAN IP address.

Subnet Mask

Enter the subnet mask of the LAN port.

Vlan	Specify the VLAN of the LAN port, only the clients in the specified VLAN can access and manage the gateway.
IGMP Proxy	Check the box to enable IGMP Proxy. IGMP Proxy sends IGMP querier packets to the LAN ports to detect if there is any multicast member connected to the LAN ports.
IGMP Version	Choose the IGMP version as V2 or V3. The default is IGMP V2.

 **Note:**

- Changing the IP address of LAN port will automatically redirect the browser to the new management page. If the redirecting failed, please try to reconnect your PC to the gateway to automatically get a new IP address, or configure a proper static IP address manually.
 - Changing the IP address of the LAN port may affect some related functions, like the IP pool of the DHCP server.
-

3.2 Configuring the DHCP Server

You can configure an IP address pool for the DHCP server to assign IP addresses. When clients send requests to the DHCP server, the server will automatically assign IP addresses and the corresponding parameters to the clients. Moreover, if you want to reserve an IP address for a certain client, you can use **Address Reservation** to bind the IP address with the client's MAC address, and the bound IP address will always be assigned to that client.

Figure 3-2 cConfiguring the DHCP Server

DHCP Settings

Starting IP Address:	<input type="text" value="192.168.0.100"/>	
Ending IP Address:	<input type="text" value="192.168.0.199"/>	
Lease Time:	<input type="text" value="120"/>	minutes. (1-2880. The default value is 120)
Default Gateway:	<input type="text"/>	(Optional)
Default Domain:	<input type="text"/>	(Optional)
Primary DNS:	<input type="text"/>	(Optional)
Secondary DNS:	<input type="text"/>	(Optional)
Option60:	<input type="text"/>	(Optional)
Option138:	<input type="text"/>	(Optional)
Status:	<input checked="" type="checkbox"/> Enable	

Configure the parameters of the DHCP server, then click **Save**.

Starting/Ending IP Address	Enter the starting IP address and ending IP address of the DHCP server's IP pool. The IP pool defines the IP range that can be assigned to the clients in the LAN. Note: The starting IP address and ending IP address should be in the same subnet with the IP address of the LAN port.
Lease Time	Specify the lease time for DHCP clients. Lease time defines how long the clients can use the IP address assigned by the DHCP server. Generally, the client will automatically request the DHCP server for extending the lease time before the lease expired. If the request failed, the client will have to stop using that IP address when the lease finally expired, and try to get a new IP address from the other DHCP servers.
Default Gateway	(Optional) It is recommended to enter the IP address of the LAN port.
Default Domain	(Optional) Enter the domain name of your network.
Primary/Secondary DNS	(Optional) Enter the DNS server address provided by your ISP. If you are not clear, please consult your ISP.

Option 60	<p>(Optional) Specify the option 60 for device identification. Mostly it is used under the scenario where the clients apply for different IP addresses from different servers according to the needs. By default, it is TP-LINK.</p> <p>If a client requests option 60, the server will respond a packet containing the option 60 configured here. And then the client will compare the received option 60 with its own. If they are the same, the client will accept the IP address assigned by the server, otherwise the assigned IP address will not be accepted.</p>
Option 138	<p>(Optional) Specify the option 138, which can be configured as the management IP address of an Omada controller. If the APs in the local network request this option, the server will respond a packet containing this option to inform the APs of the controller's IP address.</p>
Status	Check the box to enable the DHCP server.

■ **Configuring the Address Reservation**

Choose the menu **Network > LAN > Address Reservation** and click **Add** to load the following page.

Figure 3-3 Configuring the Address Reservation

<input type="checkbox"/>	ID	MAC Address	IP Address	Description	Status	Operation
--	--	--	--	--	--	--

MAC Address:

IP Address:

Description: (Optional)

Export to IP-MAC Binding: Enable

Status: Enable


Enter the MAC address of the client and the IP address to be reserved, then click **OK**.

MAC Address	Enter the MAC address of the client.
IP Address	Enter the IP address to be reserved.
Description	(Optional) Enter a brief description for the entry. Up to 32 characters can be entered.
Export to IP-MAC Binding	(Optional) Check the box to export this binding entry to IP-MAC Binding List on Firewall > Anti ARP Spoofing > IP-MAC Binding page.
Status	Check the box to enable this entry.

3.3 Viewing the DHCP Client List

Choose the menu **Network > LAN > DHCP Client List** to load the following page.

Figure 3-4 Viewing the DHCP Client List

DHCP Client List					
Total Clients: 0					 Refresh
ID	Client Name	MAC Address	Assigned IP Address	Lease Time	Operation
--	--	--	--	--	--

Here you can view the DHCP client list.

Client Name	Displays the name of the client.
MAC Address	Displays the MAC address of the client.
Assigned IP Address	Displays the IP address assigned to the client.
Lease Time	Displays the remaining lease time of the assigned IP address. After the lease expires, the IP address will be re-assigned.

4 IPTV Configuration

Configure IPTV settings to enable Internet/IPTV/Phone service provided by your ISP (internet service provider).

To complete IPTV configuration, follow these steps:

- 1) Configure the number of WAN ports.
- 2) Chose the Wan Port according to your ISP.
- 3) Chose the Wan Port according to your ISP.
- 4) Select the Port Mode to determine which port is used to support IPTV service, IP-Phone service, or internet service.
- 5) Click **Save**.

4.1 Configuring the IPTV

Choose the menu **Network > IPTV > IPTV** to load the following page.

Figure 4-1 Configuring the IPTV

The screenshot shows the IPTV configuration page. At the top, there is a tab labeled 'IPTV'. Below it is a 'Settings' section. The configuration options are as follows:

IPTV:	<input type="checkbox"/> Enable IPTV
Wan Port:	WAN
Mode:	Bridge
WAN/LAN1:	Internet
WAN/LAN2:	Internet
LAN1:	Internet
LAN2:	Internet

At the bottom of the settings section, there is a 'Save' button.

Note:

To configure Internet VLAN ID, please go to Network -> WAN and configure on the corresponding WAN port.

Enable IPTV and configure corresponding parameters, then click **Save**.

IPTV	Enable IPTV globally.
Wan Port	Select the Wan Port according to your ISP.
Mode	Select the appropriate Mode according to your ISP. Bridge: Select this mode if your ISP requires no other parameters. Custom: Select this mode if your ISP provides necessary parameters, and configure the parameters according to the requirements of your ISP.
Port Mode	Select the appropriate Port Mode of the LAN ports to determine which port is used to support Internet service, IPTV service, or IP-Phone service.

 **Note:**

To configure Internet VLAN ID, please go to [WAN Configuration](#) and configure on the corresponding WAN port.

5 MAC Configuration

Generally, the MAC address does not need to be changed. However, in the following situations, you may need to change the MAC address of the WAN port.

In the condition that your ISP has bound your account to the MAC address of the dial-up device, if you want to replace the dial-up device with this gateway, you can just set the MAC address of this gateway's WAN port the same as that of the previous dial-up device for a normal internet connection.

5.1 Configuring MAC Address

Choose the menu **Network > MAC > MAC** to load the following page.

Figure 5-1 Configuring MAC Address

MAC		
Interface Name	Current MAC Address	MAC Clone
WAN1	<input type="text" value="00-0A-EB-61-20-11"/>	<input type="button" value="Restore Factory MAC"/> <input type="button" value="Clone Current PC's MAC"/>
WAN2	<input type="text" value="00-0A-EB-61-20-12"/>	<input type="button" value="Restore Factory MAC"/> <input type="button" value="Clone Current PC's MAC"/>
LAN	<input type="text" value="00-0A-EB-61-20-10"/>	<input type="button" value="Restore Factory MAC"/>

Configure the MAC address of the WAN port or LAN port according to your need, then click **Save**.

Interface Name	Displays the WAN port and LAN port.
Current MAC Address	Configure the MAC address of the WAN port.
MAC Clone	<p>Restore Factory MAC: Click this button to restore the MAC address to the factory default value.</p> <p>Clone Current PC's MAC: Click this button to clone the MAC address of the PC you are currently using to configure the gateway. It's only available for the WAN ports.</p>

Note:

When cloning current management host's MAC on the WAN port, the management PC should be connected to the LAN port.

If the connection type on the WAN port is PPPoE, L2TP or PPTP, changing the MAC address of the WAN port may cause the connection to be terminated or re-established.

6 Switch Configuration

The gateway provides some basic switch port management function, including **Statistics**, **Port Mirror**, **Rate Control**, **Port Config** and **Port Status**. **Statistics** and **Rate Control** are available only for certain devices.

6.1 Viewing the Statistics (only for certain devices)

Choose the menu **Network > Switch > Statistics** to load the following page.

Figure 6-1 Viewing the Statistics

Statistics List						
Packet Type		Port1	Port2	Port3	Port4	Port5
Received	Unicast	0	0	0	0	20562
	Broadcast	0	0	0	0	7517
	Pause	0	0	0	0	0
	Multicast	0	0	0	0	42499
	Total	0 B	0 B	0 B	0 B	16.9 MB
	Undersize	0	0	0	0	0
	Normal	0	0	0	0	70578
	Oversize	0	0	0	0	0
Transmitted	Unicast	0	0	0	0	28841
	Broadcast	0	0	0	0	0
	Pause	0	0	0	0	0
	Multicast	0	0	0	0	1865
	Total	0 B	0 B	0 B	0 B	19.0 MB

Refresh Clear

Statistics displays the detailed traffic information of each port, which allows you to monitor the traffic and locate faults promptly.

Unicast Displays the number of normal unicast packets received or transmitted on the port.

Broadcast Displays the number of normal broadcast packets received or transmitted on the port.

Pause Displays the number of flow control frames received or transmitted on the port.

Multicast Displays the number of normal multicast packets received or transmitted on the port.

Total	Displays the total bytes of the received or transmitted packets (including error frames).
Undersize	Displays the number of received packets which have a length less than 64 bytes (including error frames).
Normal	Displays the number of received packets which have length between 64 bytes and the maximum frame length (including error frames).
Oversize	Displays the number of received packets that have a length greater than the maximum frame length (including error frames).

 **Note:**

Error Frame: The frames that have a false checksum.

Maximum frame length: The maximum frame length supported by the gateway. For untagged frames, it's 1518 bytes long; for tagged packets, it's 1522 bytes long.

6.2 Configuring Port Mirror

Port Mirror function allows the gateway to forward packet copies of the monitored port(s) to a specific monitoring port. Then you can analyze the copied packets to monitor network traffic and troubleshoot network problems.

Choose the menu **Network > Switch > Mirror** to load the following page.

Figure 6-2 Configuring Port Mirror

Settings

Enable Port Mirror

Mirror Mode: Ingress and Egress

Monitor List

Mirroring Port	Mirrored Port
<input type="radio"/> Port1	<input checked="" type="checkbox"/> Port1
<input type="radio"/> Port2	<input type="checkbox"/> Port2
<input type="radio"/> Port3	<input type="checkbox"/> Port3
<input type="radio"/> Port4	<input type="checkbox"/> Port4
<input checked="" type="radio"/> Port5	<input type="checkbox"/> Port5

Save

Follow these steps to configure Port Mirror:

- 1) In **Settings** section, enable Port Mirror function, and choose the mirror mode.

Enable Port Mirror	Check the box to enable Port Mirror function.
Mirror Mode	Choose the mirror mode which includes Ingress , Egress and Ingress and Egress . Ingress: The packets received by the mirrored port will be copied to the mirroring port. Egress: The packets sent by the mirrored port will be copied to the mirroring port. Ingress and Egress: Both the incoming and outgoing packets through the mirrored port will be copied to the mirroring port.

2) In the **Monitor List** section, set the mirroring port and the mirrored port(s), then click **Save**.

Mirroring Port	The packets through the mirrored port will be copied to this port. Usually, the mirroring port is connected to a data diagnose device, which is used to analyze the mirrored packets for monitoring and troubleshooting the network.
Mirrored Port	The packets through this port will be copied to the mirroring port. Usually, the mirrored ports are the ports to be monitored.

6.3 Configuring Rate Control (only for certain devices)

Rate Control enables you to control the traffic rate for the specific packets on each port to manage your network.

Choose the menu **Network > Switch > Rate Control** to load the following page.

Figure 6-3 Configuring Rate Control

Settings					
Port	Ingress Limit	Ingress Frame Type	Ingress Rate(Mbps)	Egress Limit	Egress Rate(Mbps)
Port1	<input type="checkbox"/> Enable	All Frames ▼	1000	<input type="checkbox"/> Enable	1000
Port2	<input type="checkbox"/> Enable	All Frames ▼	1000	<input type="checkbox"/> Enable	1000
Port3	<input type="checkbox"/> Enable	All Frames ▼	1000	<input type="checkbox"/> Enable	1000
Port4	<input type="checkbox"/> Enable	All Frames ▼	1000	<input type="checkbox"/> Enable	1000
Port5	<input type="checkbox"/> Enable	All Frames ▼	1000	<input type="checkbox"/> Enable	1000

Save

Choose the port and configure the ingress frames or egress frames limitation, then click **Save**.

Ingress Limit	Check the box to enable the Ingress Limit feature.
----------------------	--

Ingress Frame Type	Specify the ingress frame type to be limited. It is All Frames by default. All Frames: The ingress rate of all frames is limited. Broadcast: The ingress rate of broadcast frames is limited.
Ingress Rate (Mbps)	Specify the limit rate for the ingress packets.
Egress Limit	Check the box to enable Egress Limit feature.
Egress Rate (Mbps)	Specify the limit rate for the egress packets.

6.4 Configuring Port Config

You can configure the flow control and negotiation mode for the port.

Choose the menu **Network > Switch > Port Config** to load the following page.

Figure 6-4 Configuring Flow Control and Negotiation

Port	Flow Control	Negotiation Mode
Port1	<input type="checkbox"/> Enable	Auto
Port2	<input type="checkbox"/> Enable	Auto
Port3	<input type="checkbox"/> Enable	Auto
Port4	<input type="checkbox"/> Enable	Auto
Port5	<input type="checkbox"/> Enable	Auto

Save

Configure the flow control and negotiation mode for a port.

Flow Control	Check the box to enable the flow control function. Flow Control is the process of managing the data transmission of the sender to avoid the receiver getting overloaded.
Negotiation Mode	Select the negotiation mode for the port. You can set the mode as Auto , or manually set the speed and duplex mode for the port. It is recommended to configure both devices of a link to work in Auto-Negotiation mode or manually configure them to work in the same speed and duplex mode. If the two devices at both sides work in Auto mode, they will advertise their speed and duplex abilities to each other, and negotiate the optimal speed and duplex mode. If the local device works in Auto mode while the peer device does not, the local device will automatically detect and match the speed with the peer device. The local device will work in half-duplex mode, no matter what duplex mode the peer device is in.

6.5 Viewing Port Status

Choose the menu **Network > Switch > Port Status** to load the following page.

Figure 6-5 Viewing Port Status

Status List				
Port	Status	Speed(Mbps)	Duplex Mode	Flow Control
Port1	Link Down	---	---	---
Port2	Link Down	---	---	---
Port3	Link Down	---	---	---
Port4	Link Down	---	---	---
Port5	Link Up	1000M	Full-duplex	Disabled

Status	Displays the port status. Link Down: The port is not connected. Link Up: The port is working normally.
Speed (Mbps)	Displays the port speed.
Duplex Mode	Displays the duplex mode of the port.
Flow Control	Displays if the Flow Control is enabled.

7 VLAN Configuration

The gateway supports 802.1Q VLAN, which can divide a LAN into multiple logical LANs. Each logical LAN is a VLAN. Hosts in the same VLAN can communicate with each other. However, hosts in different VLANs cannot communicate directly. Therefore, broadcast packets can be limited to within the VLAN.

7.1 Creating a VLAN

Choose the menu **Network > VLAN > VLAN** and click **Add** to load the following page.

Figure 7-1 Creating a VLAN

Create a VLAN and add the port(s) to the VLAN, then click **OK**.

VLAN ID	Enter a VLAN ID. The value ranges from 1 to 4094.
Name	Specify the name of the VLAN for easy identification.
Ports	<p>Check the box to select the port and specify the port type in the specified VLAN. The port can be divided into two types: TAG or UNTAG.</p> <p>TAG: The egress rule of the packets transmitted by the port is Tagged.</p> <p>UNTAG: The egress rule of the packets transmitted by the port is Untagged.</p>
Description	(Optional) Enter a brief description for easy management and searching.

VLAN List						
<input type="checkbox"/>	ID	VLAN ID	Name	Ports	Description	Operation
<input type="checkbox"/>	1	20	vlan20	2(UNTAG)	Default Vlan For WAN2	
--	2	100	vlan100	1(UNTAG)		
--	3	300	vlan300	1(TAG)		
--	4	336	vlan336	4(UNTAG)		
<input type="checkbox"/>	5	1445	vlan1445	3(UNTAG)		
<input type="checkbox"/>	6	2988	vlan2988	5(UNTAG)		

In the VLAN list you can view all the VLANs existing in the gateway.

VLAN ID	Displays the VLAN ID.
Name	Displays the VLAN name.
Ports	Displays the ports which belongs to the corresponding VLAN.
Description	Displays the description of the VLAN.

Note:

The VLAN list contains all the VLANs existing in the gateway. Some of them are manually created by the user, and can be edited or deleted. Some are automatically created and referenced by the gateway for some special scenarios like management VLAN, and you cannot edit or delete these VLANs.

7.2 Configuring the PVID of a Port

Choose the menu **Network > VLAN > Port** to load the following page.

Figure 7-2 Configuring the PVID

Port	PVID	VLAN
Port1	34	10(UNTAG) 34(TAG)
Port2	20	20(UNTAG)
Port3	1	1(UNTAG)
Port4	1	1(UNTAG)
Port5	1	1(UNTAG)

Configure the PVID of the port, then click **Save**.

Port	Displays the port.
PVID	Specify the PVID for the port. PVID indicates the default VLAN for the corresponding port.
VLAN	Displays the VLAN(s) the port belongs to.

8 IPv6 Configuration

IPv6 is the next-generation network protocol after IPv4. You can configure IPv6 network for the gateway if your ISP supports IPv6. IPv6 network won't cause conflict with your current IPv4 network.

To configure the IPv6 network, follow the guidelines:

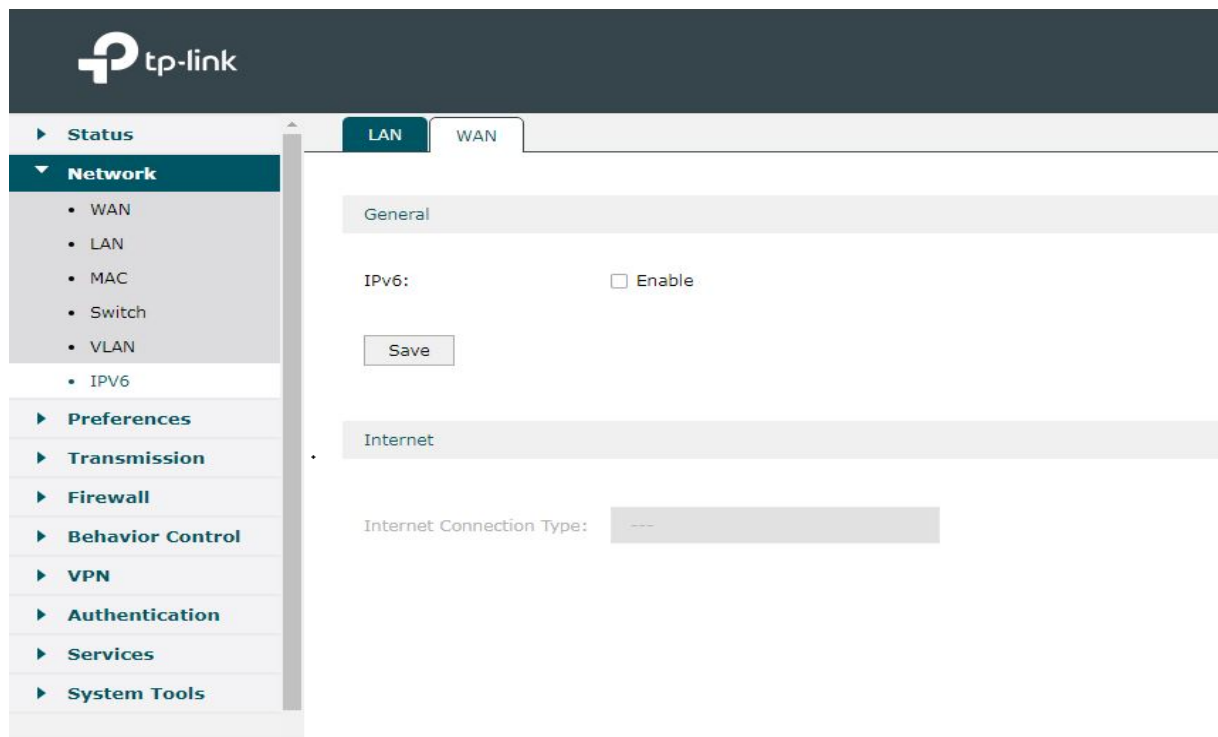
- Configure IPv6 for the WAN / SFP WAN port(s). You can configure IPv6 for multiple WANs one by one, and each WAN port has its own Internet Connection Type and parameters.
- Configure IPv6 for the LAN port.

8.1 Configure IPv6 for WAN / SFP WAN port(s)

Choose the menu **Network > IPv6 > WAN** to load the following page.

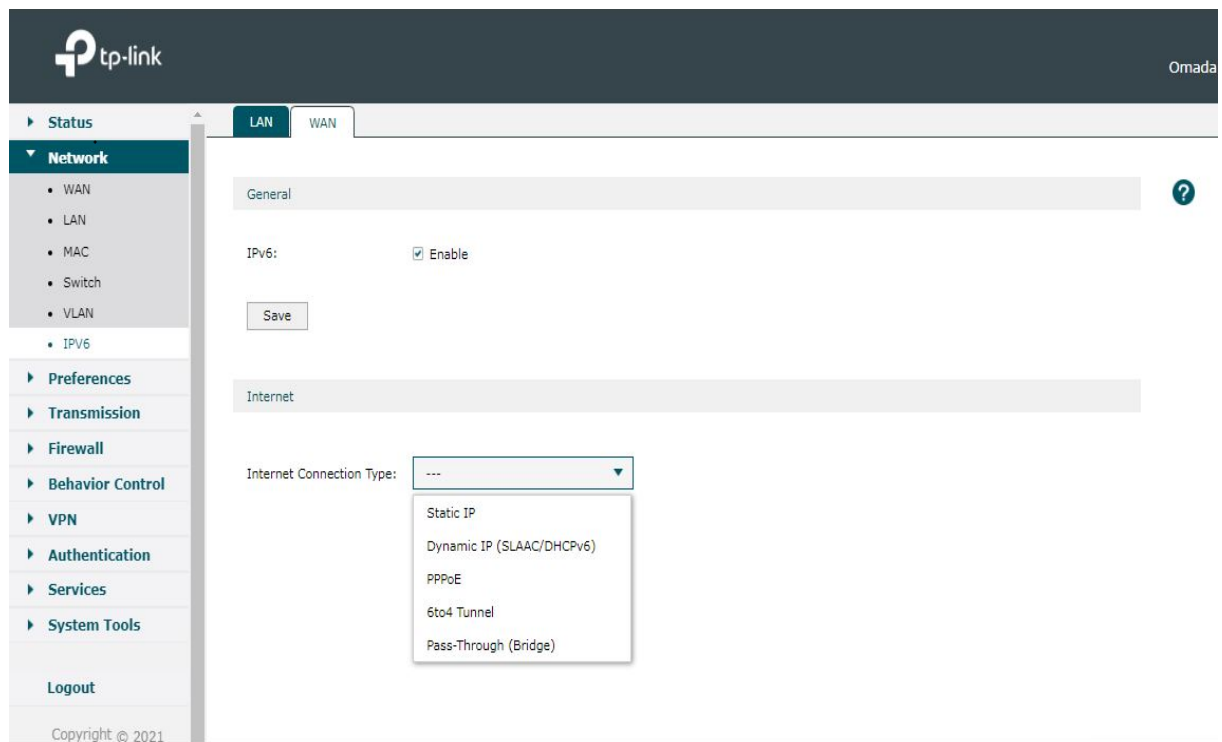
Choose a WAN / SFP WAN port, and click the corresponding tab.

Figure 8-1 Enable IPv6



In the **General** section, enable IPv6 and click **Save**.

Figure 8-2 Select Internet Connection Type



In the **Internet** section, select the proper Internet Connection Type and configure the parameters according to the requirements of your ISP. Then click **Save**.

<p>Internet Connection Type</p>	<p>Choose the proper Internet Connection Type according to the requirements of your ISP.</p>
--	--

8.2 Configuring the WAN Connection

The gateway supports five connection types: **Static IP**, **Dynamic IP (SLAAC/DHCPv6)**, **PPPoE**, **6to4 Tunnel**, **PPTP**, you can choose one according to the service provided by your ISP.

Static IP: If your ISP provides you with a fixed IP address and the corresponding parameters, choose Static IP.

Dynamic IP (SLAAC/DHCPv6): If your ISP automatically assigns the IP address and the corresponding parameters, choose Dynamic IP.

PPPoE: If your ISP provides you with a PPPoE account, choose PPPoE.

6to4 Tunnel: Select this type if your ISP uses 6to4 deployment for assigning address.

Pass-Through (Bridge): Select this type if your ISP uses Pass-Through (Bridge) network deployment.

 **Note:**

If Internet Connection Type of WAN / SFP WAN is selected as Pass-Through (Bridge), the IPv6 parameters of the LAN port and the other WAN ports cannot be configured.

■ **Configuring the Static IP**

Choose the menu **Network > IPv6 > WAN** to load the following page.

Figure 8-3 Configuring the Static IP

Connection Configuration		Connection Status	
Connection Type:	Static IP	Connection Status	Disconnected
IP Address:		IP Address	0.0.0.0
Subnet Mask:		Subnet Mask	0.0.0.0
Default Gateway:		Default Gateway	0.0.0.0
Upstream Bandwidth:	1000000	Primary DNS	0.0.0.0
Downstream Bandwidth:	1000000	Secondary DNS	0.0.0.0
MTU:	1500		
Primary DNS:			
Secondary DNS:			
Vlan:	336		
<input type="button" value="Save"/>			

In **Internet** section, select the connection type as Static IP. Enter the corresponding parameters and click **Save**.

IPv6 Address/
Default Gateway/
Primary DNS/
Secondary DNS

Enter these parameters as provided by the ISP.

■ **Configuring the Dynamic IP (SLAAC/DHCPv6)**

Choose the menu **Network > IPv6 > WAN** to load the following page.

Figure 8-4 Configuring the Dynamic IP (SLAAC/DHCPv6)

Connection Configuration		Connection Status	
Connection Type:	Dynamic IP	Connection Status	Disconnected
Host Name:	<input type="text"/>	IP Address	0.0.0.0
Upstream Bandwidth:	1000000 Kbps (100-1000000)	Subnet Mask	0.0.0.0
Downstream Bandwidth:	1000000 Kbps (100-1000000)	Default Gateway	0.0.0.0
MTU:	1500 (576-1500)	Primary DNS	0.0.0.0
Primary DNS:	<input type="text"/> (Optional)	Secondary DNS	0.0.0.0
Secondary DNS:	<input type="text"/> (Optional)		
Vlan:	10		
<input type="checkbox"/> Get IP using Unicast DHCP			
<input type="button" value="Save"/> <input type="button" value="Connect"/> <input type="button" value="Disconnect"/>			

In **Internet** section, select the connection type as Dynamic IP (SLAAC/DHCPv6). Enter the corresponding parameters and click **Save**.

IPv6 Address/ Primary DNS/ Secondary DNS	These parameters are automatically assigned by your ISP.
Renew	Click this button to get new IPv6 parameters assigned by your ISP.
Release	Click this button to release all IPv6 addresses assigned by your ISP.
Get IPv6 Address	Select the proper method whereby your ISP assigns IPv6 address to your gateway.
DHCPv6	Your ISP assigns an IPv6 address and other parameters including the DNS server address to your gateway using DHCPv6.
SLAAC+Stateless DHCP	Your ISP assigns the IPv6 address prefix to your gateway and your gateway automatically generates its own IPv6 address. Also, your ISP assigns other parameters including the DNS server address to your gateway using DHCPv6.
Prefix Delegation	Select Enable to get an address prefix for your LAN port from your ISP, or Disable to designate an address prefix for your LAN port manually. Clients in LAN will get an IPv6 address with this prefix.
DNS Address	Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually.
Get dynamically from ISP	Your ISP assigns a DNS address to your gateway dynamically.
Use the following DNS Addresses	You should manually enter the DNS address provided by your ISP.

Primary DNS/ Secondary DNS Enter the DNS address manually or display the DNS address which is assigned by your ISP.

■ **Configuring the PPPoE**

Choose the menu **Network > IPv6 > WAN** to load the following page.

Figure 8-5 Configuring the PPPoE

Connection Configuration		Connection Status	
Connection Type:	PPPoE	Connection Status	Disconnected
Username:		IP Address	0.0.0.0
Password:		Subnet Mask	0.0.0.0
Connection Mode:	Connect Automatically	Default Gateway	0.0.0.0
Upstream Bandwidth:	1000000 Kbps (100-1000000)	Primary DNS	0.0.0.0
Downstream Bandwidth:	1000000 Kbps (100-1000000)	Secondary DNS	0.0.0.0
MTU:	1492 (576-1492)	Secondary Connection	
Service Name:	(1-128 characters, optional)	IP Address	0.0.0.0
Primary DNS:	(Optional)	Subnet Mask	0.0.0.0
Secondary DNS:	(Optional)		
Vlan:	10		
Secondary Connection:	<input type="radio"/> None <input type="radio"/> Dynamic IP <input checked="" type="radio"/> Static IP		
IP Address:			

In **Internet** section, select the connection type as PPPoE. Enter the corresponding parameters and click **Save**.

PPPoE same session with IPv4 connection If this option is enabled, IPv6 uses the same PPPoE session as IPv4.

Username/ Password: Enter these parameters as provided by your ISP.

IPv6 Address This address will be automatically assigned by your ISP after you enter the username and password and click **Connect**.

Connect Click this button to connect to the internet.

Disconnect Click this button to disconnect from the internet.

Get IPv6 Address Select the proper method whereby your ISP assigns IPv6 address to your gateway according to the requirements of your ISP

DHCPv6 Your ISP assigns an IPv6 address and other parameters including the DNS server address to your gateway using DHCPv6.

SLAAC+Stateless DHCP Your ISP assigns the IPv6 address prefix to your gateway and your gateway automatically generates its own IPv6 address. Also, your ISP assigns other parameters including the DNS server address to your gateway using DHCPv6.

Specified by ISP You should manually enter the IPv6 address provided by your ISP.

Prefix Delegation	Select Enable to get an address prefix for your LAN port from your ISP, or Disable to designate an address prefix for your LAN port manually. Clients in LAN will get an IPv6 address with this prefix.
DNS Address	Select whether to get the DNS address dynamically from your ISP or designate the DNS address manually.
Get dynamically from ISP	Your ISP assigns an DNS address and to your gateway dynamically.
Use the following DNS Addresses	You should manually enter the DNS address provided by your ISP.
Primary DNS/ Secondary DNS	Enter the DNS address manually or display the DNS address which is assigned by your ISP.

■ **Configuring the 6to4 Tunnel**

Choose the menu **Network > IPv6 > WAN** to load the following page.

Figure 8-6 Configuring the 6to4 Tunnel

The screenshot shows a configuration page with two main sections: 'General' and 'Internet'. In the 'General' section, the 'IPv6' checkbox is checked and labeled 'Enable', with a 'Save' button below it. The 'Internet' section shows 'Internet Connection Type' set to '6to4 Tunnel' in a dropdown menu. Below this, the 'IPv4 Address', 'IPv4 Subnet Mask', and 'IPv4 Default Gateway' are all set to '0.0.0.0'. The 'Tunnel Address' is set to '::'. At the bottom of the 'Internet' section, there is an 'Advanced' toggle button.

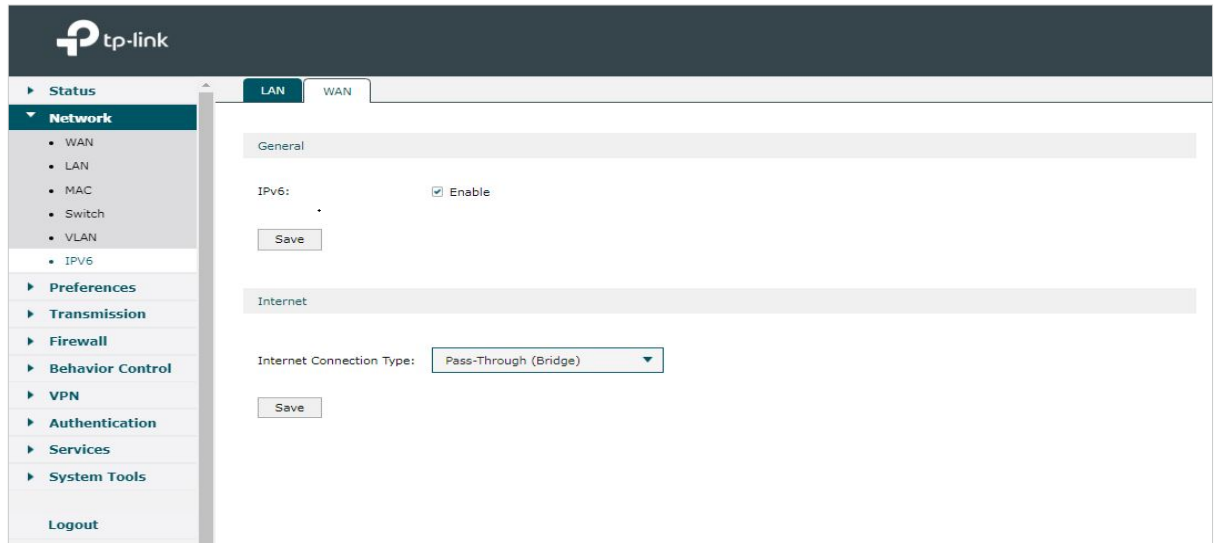
In **Internet** section, select the connection type as 6to4 Tunnel. Enter the corresponding parameters and click **Save**.

IPv4 Address/ IPv4 Subnet Mask/IPv4 Default Gateway/ Tunnel Address	These parameters will be dynamically generated by the IPv4 information of WAN port after you click Connect .
Use the following DNS Server	Check the box to manually enter the primary DNS and/or secondary DNS as provided by your ISP.
Connect	Click this button to connect to the internet.
Disconnect	Click this button to disconnect from the internet.

■ Configuring the Pass-Through (Bridge)

Choose the menu **Network > IPv6 > WAN** to load the following page.

Figure 8-7 Configuring the Pass-Through (Bridge)

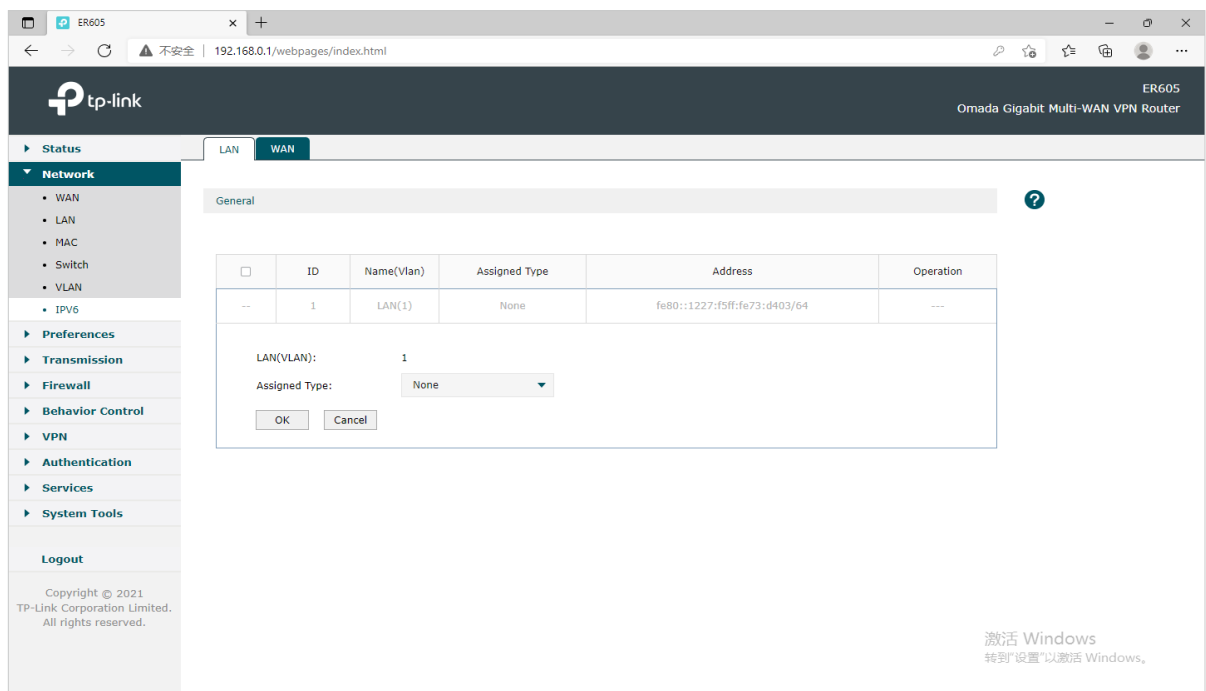


In **Internet** section, select the connection type as Pass-Through (Bridge). No configuration is required for this type of connection.

8.3 Configuring IPv6 for the LAN Port

Choose the menu **Network > IPv6 > LAN > Operation** to load the following page.

Figure 8-8 Select Assigned Type



In the **General** section, select the proper Assigned Type, which is determined by the compatibility of clients in your local network, and configure the parameters according to the requirements of your ISP. Then click **OK**.

Assigned Type Determines the method whereby the gateway assigns IPv6 addresses to the clients in your local network. Some clients may support only a few of these assigned types, so you should choose it according to the compatibility of clients in your local network.

 **Note:**

- If Internet Connection Type of WAN / SFP WAN is selected as Pass-Through (Bridge), the IPv6 parameters of the LAN port and the other WAN ports cannot be configured.
- If Prefix Delegation of WAN / SFP WAN is enabled, the Address Prefix of LAN is automatically assigned by your ISP and you cannot designate an address prefix manually.

■ **Configuring the DHCPv6**

Choose the menu **Network > IPv6 > LAN** to load the following page.

Figure 8-9 Configuring the DHCPv6

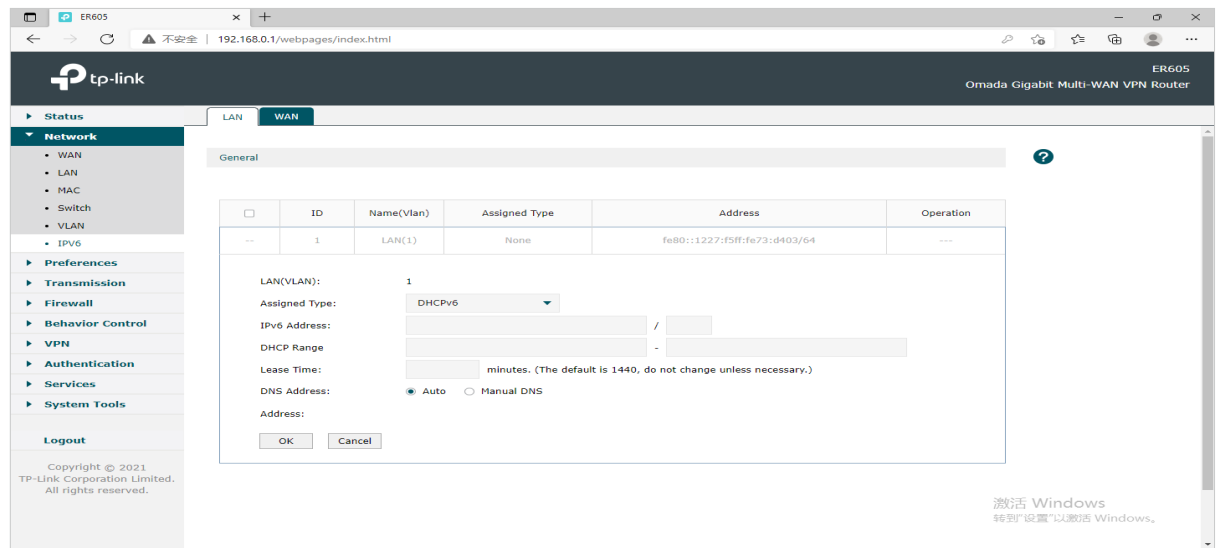
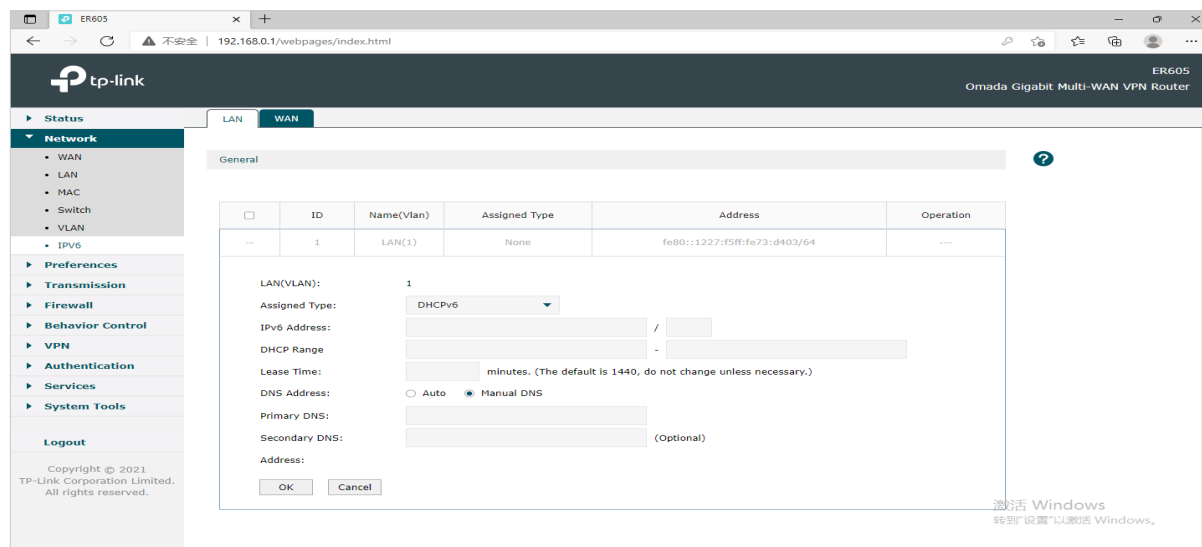


Figure 8-10 Configuring the SLAAC+Stateless DHCP



In **Assigned Type** section, select the connection type as DHCPv6. Enter the corresponding parameters and click **OK**.

DHCPv6	The gateway assigns an IPv6 address and other parameters including the DNS server address to each client using DHCPv6.
Lease Time	Determines how long the assigned IPv6 address remains valid. Either keep the default 86400 seconds or change it if required by your ISP. Lease Time is only available when the Assigned Type is configured as DHCPv6.
Address	Displays the IPv6 address of the LAN port.

■ **Configuring the SLAAC+Stateless DHCP**

Choose the menu **Network > IPv6 > LAN** to load the following page.

Figure 8-11 Configuring the SLAAC+Stateless DHCP

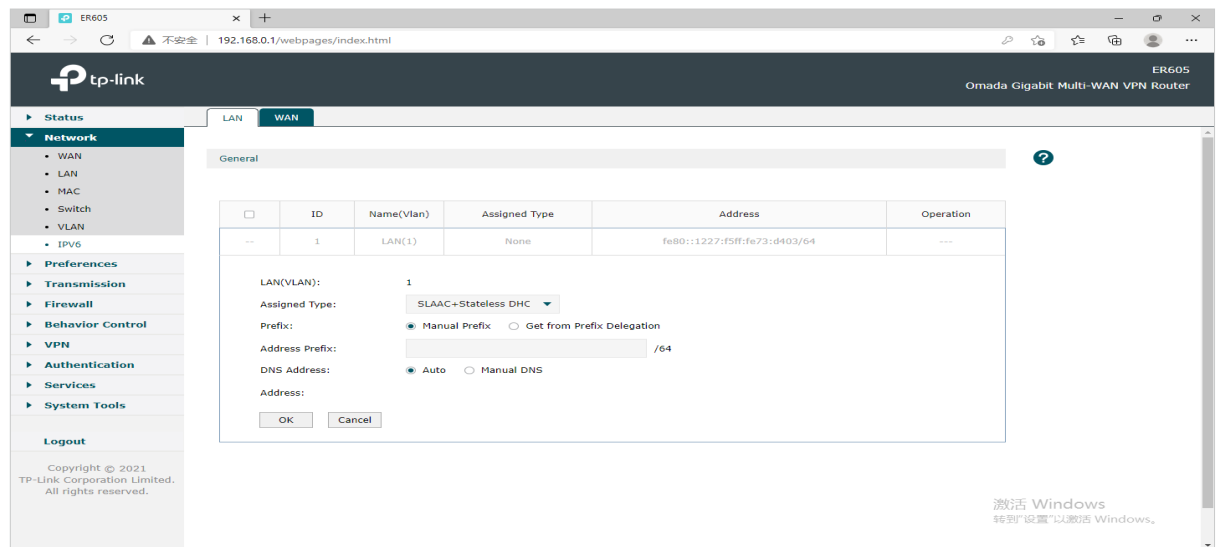
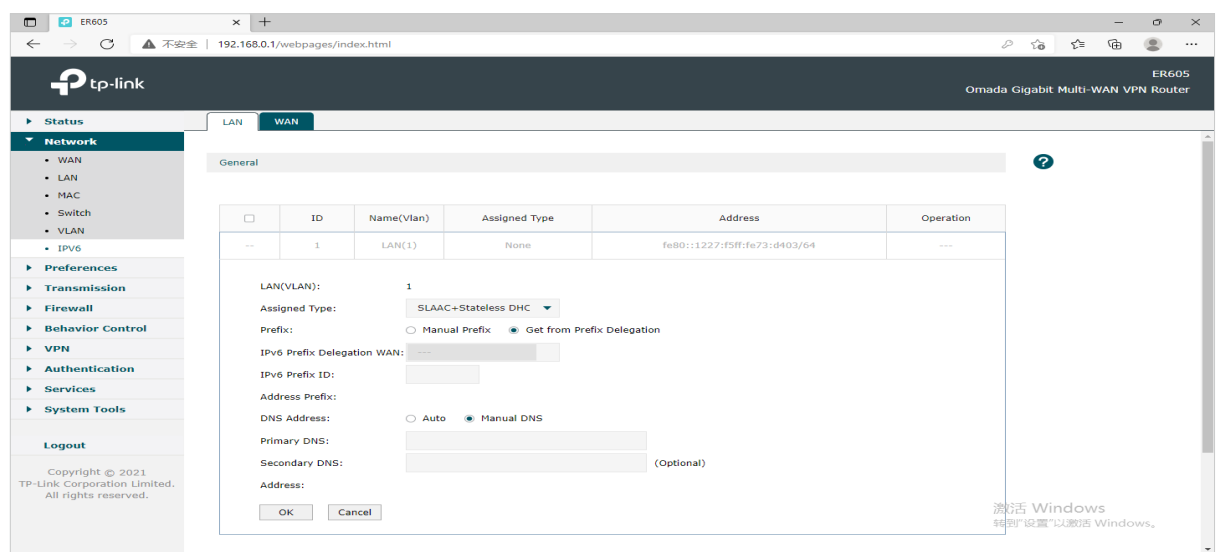


Figure 8-12 Configuring the SLAAC+Stateless DHCP



In **Assigned Type** section, select the connection type as SLAAC+Stateless DHCP. Enter the corresponding parameters and click **OK**.

SLAAC+Stateless DHCP	The gateway assigns the IPv6 address prefix to each client and the client automatically generates its own IPv6 address. Also, the gateway assigns other parameters including the DNS server address to each client using DHCPv6.
Address Prefix	Enter the address prefix according to the requirements of your ISP.
Address	Displays the IPv6 address of the LAN port.

■ Configuring the SLAAC+RDNSS

Choose the menu **Network > IPv6 > LAN** to load the following page.

Figure 8-13 Configuring the SLAAC+RDNSS

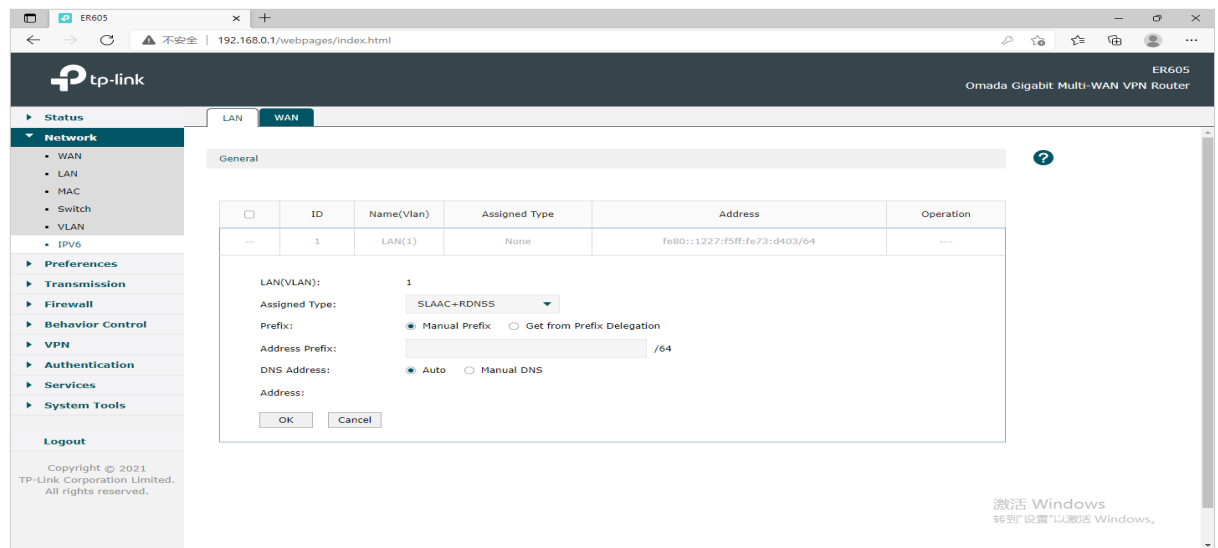
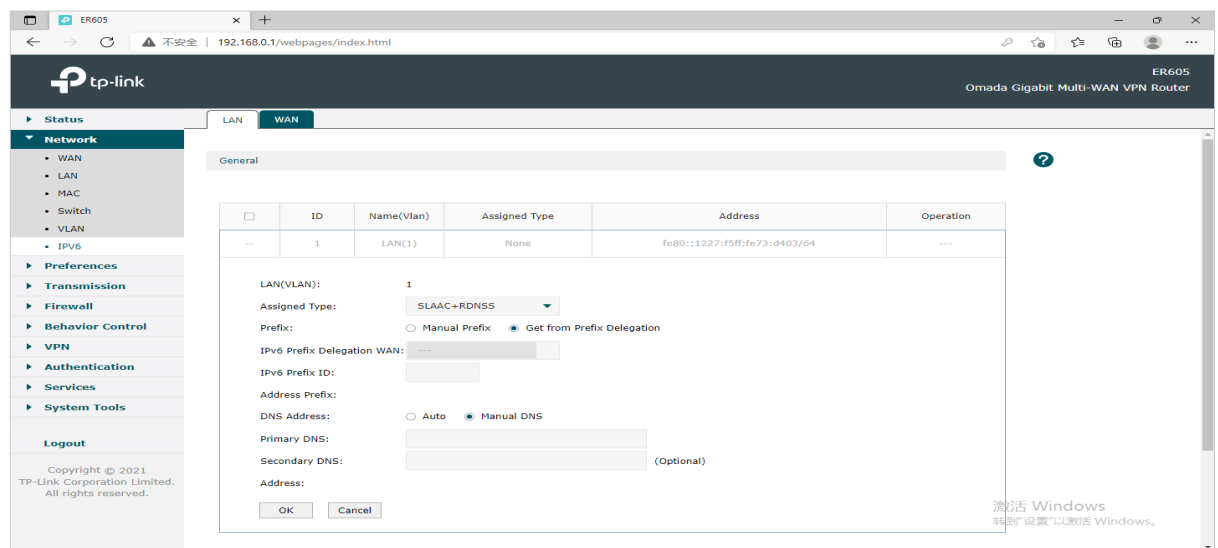


Figure 8-14 Configuring the SLAAC+RDNSS



In **Assigned Type** section, select the connection type as SLAAC+RDNSS. Enter the corresponding parameters and click **OK**.

SLAAC+RDNSS The gateway assigns the IPv6 address prefix to each client and the client automatically generates its own IPv6 address. Also, the gateway assigns other parameters including the DNS server address to each client using the RDNSS option in RA (Gateway Advertisement).

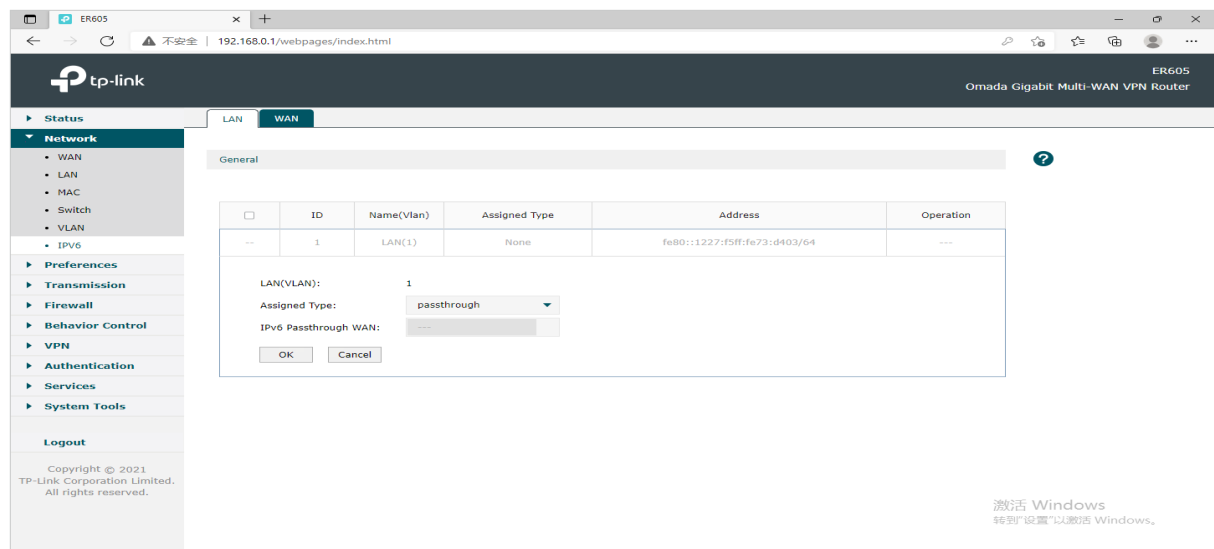
Address Prefix Enter the address prefix according to the requirements of your ISP.

Address Displays the IPv6 address of the LAN port.

■ Configuring the pass-through

Choose the menu **Network > IPv6 > LAN** to load the following page.

Figure 8-15 Configuring the pass-through



In **Assigned Type** section, select the connection type as pass-through. Enter the corresponding parameters and click **OK**.

👉 Note:

- If Internet Connection Type of WAN / SFP WAN is selected as Pass-Through (Bridge), the IPv6 parameters of the LAN port and the other WAN ports cannot be configured.
- If Prefix Delegation of WAN / SFP WAN is enabled, the Address Prefix of LAN is automatically assigned by your ISP and you cannot designate an address prefix manually.

9 USB Configuration

The USB Modem function is used to connect to the 3G/4G network of the ISP (Internet Service Provider) as the WAN connection, after you connect the 3G/4G USB modem to the USB port.

To configure the USB Modem, you should:

- Confirm that the USB modem is connected to the USB port properly.
- Specify the ISP information. You can specify the location and ISP, or you can set the Dial Number, APN, Username and Password manually, which depends on the Config Type you select.

9.1 Configuring USB Modem

■ Configuring the USB Modem automatically

Choose the menu **Network > USB > USB Modem** to load the following page.

Figure 9-1 Configuring the USB Modem automatically

The screenshot shows the configuration page for the USB Modem. The sidebar on the left includes sections for Status, Quick Setup, Network (with sub-items WAN, LAN, IPTV, MAC, Switch, VLAN, IPV6, USB), Preferences, Transmission, Firewall, Behavior Control, VPN, Authentication, Services, and System Tools. The main content area is titled 'USB Modem' and '3G/4G'. It shows the status 'No USB modem connected.' and the following configuration options:

- USB Modem: No USB modem connected.
- Config Type: Auto
- Location: Argentina
- Mobile ISP: Claro
- Connection Mode: Connect Automatically, Connect Manually
- Upload Bandwidth: 100000 Kbps (100-1000000)
- Download Bandwidth: 100000 Kbps (100-1000000)
- Authentication Type: Auto (The default is Auto, do not change unless necessary.)
- MTU Size(in bytes): 1480 (The default is 1480, do not change unless necessary)
- Use The following DNS Servers: Enable

At the bottom, there are buttons for 'Connect', 'Disconnect', and 'Save'. The 'Disconnect' button is disabled, and there is a 'Disconnected' status indicator.

In **3G/4G** section, select the Config Type as Auto. Enter the corresponding parameters and click **Save**.

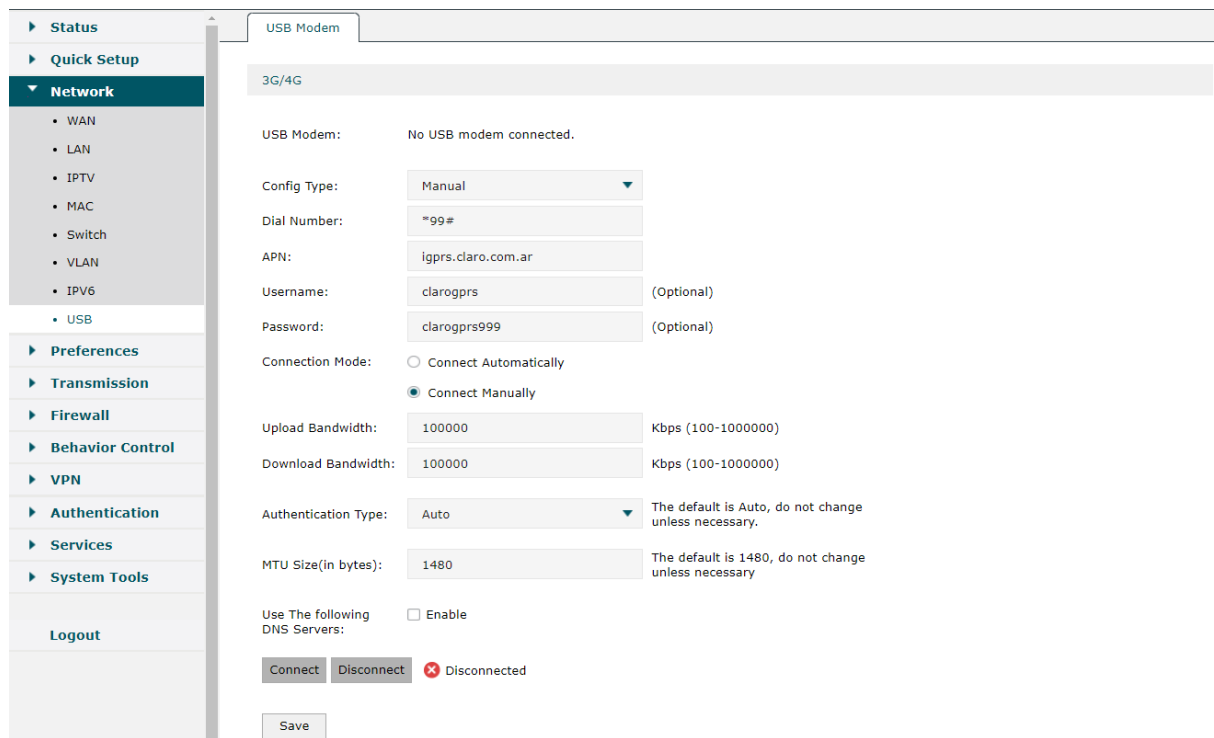
USB Modem	Displays the status of the 3G/4G USB modem.
Location	Automatically selects and displays the region when the USB modem and SIM card are successfully identified. If not, select the region from the drop-down menu.

Mobile ISP	Displays the ISP of the 3G/4G network. If not automatically detected, select the ISP from the drop-down menu.
Connection Mode	<p>Select the connection mode and configure the parameters according to the requirements of your ISP.</p> <p>Connect Automatically: In this mode, the Internet connection reconnects automatically anytime it gets disconnected.</p> <p>Connect Manually: In this mode, you can click the Connect or Disconnect button to control the Internet connection manually.</p>
Upload Bandwidth	Specify the upstream bandwidth of the USB Modem. This value is the upper limit of the Maximum Upstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of USB Modem and WAN ports after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
Download Bandwidth	Specify the downstream bandwidth of the USB Modem. This value is the upper limit of the Maximum Downstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of USB Modem and WAN ports after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
Authentication Type	<p>Select an authentication type. The default is Auto. Some ISPs require a specific authentication type, please confirm it with the ISP or keep the default settings.</p> <p>Auto: If Auto (default), the gateway automatically determines the authentication type used by the ISP.</p> <p>PAP: If PAP (Password Authentication Protocol), the gateway authenticates with the peer using two handshakes. Select this option if the ISP requires this authentication type.</p> <p>CHAP: If CHAP (Challenge Handshake Authentication Protocol), the gateway authenticates with the peer using three handshakes and validates the peer's identify periodically. Select this option if the ISP requires this authentication type.</p>
MTU Size	The default MTU (Maximum Transmission Unit) size is 1480 bytes. Do not change it unless required by the ISP.
Use the Following DNS Servers	<p>If the ISP provides DNS server IP addresses, select this checkbox and enter the Primary DNS and Secondary DNS (optional) IP addresses below. Otherwise, the DNS servers will be assigned dynamically by the ISP.</p> <p>Primary DNS: Enter the DNS IP address in dotted-decimal notation provided by the ISP.</p> <p>Secondary DNS: (Optional) Enter another DNS IP address in dotted-decimal notation provided by the ISP.</p>

■ Configuring the USB Modem manually

Choose the menu **Network > USB > USB Modem** to load the following page.

Figure 9-2 Configuring the USB Modem manually



In **3G/4G** section, select the Config Type as Manual. Enter the corresponding parameters and click **Save**.

USB Modem	Displays the status of the 3G/4G USB modem.
Dial Number, APN, Username and Password manually	If the ISP is not listed in the Mobile ISP list, please enter the Dial Number, APN (Access Point Name), Username and Password that are provided by the ISP.
Connection Mode	<p>Select the connection mode and configure the parameters according to the requirements of your ISP.</p> <p>Connect Automatically: In this mode, the Internet connection reconnects automatically anytime it gets disconnected.</p> <p>Connect Manually: In this mode, you can click the Connect or Disconnect button to control the Internet connection manually.</p>
Upload Bandwidth	Specify the upstream bandwidth of the USB Modem. This value is the upper limit of the Maximum Upstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of USB Modem and WAN ports after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
Download Bandwidth	Specify the downstream bandwidth of the USB Modem. This value is the upper limit of the Maximum Downstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of USB Modem and WAN ports after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.

Authentication Type	<p>Select an authentication type. The default is Auto. Some ISPs require a specific authentication type, please confirm it with the ISP or keep the default settings.</p> <p>Auto: If Auto (default), the gateway automatically determines the authentication type used by the ISP.</p> <p>PAP: If PAP (Password Authentication Protocol), the gateway authenticates with the peer using two handshakes. Select this option if the ISP requires this authentication type.</p> <p>CHAP: If CHAP (Challenge Handshake Authentication Protocol), the gateway authenticates with the peer using three handshakes and validates the peer's identify periodically. Select this option if the ISP requires this authentication type.</p>
MTU Size	<p>The default MTU (Maximum Transmission Unit) size is 1480 bytes. Do not change it unless required by the ISP.</p>
Use the Following DNS Servers	<p>If the ISP provides DNS server IP addresses, select this checkbox and enter the Primary DNS and Secondary DNS (optional) IP addresses below. Otherwise, the DNS servers will be assigned dynamically by the ISP.</p> <p>Primary DNS: Enter the DNS IP address in dotted-decimal notation provided by the ISP.</p> <p>Secondary DNS: (Optional) Enter another DNS IP address in dotted-decimal notation provided by the ISP.</p>

Part 5

USB

CHAPTERS

1. Overview
2. USB Modem Configuration
3. USB Storage

1 Overview

The USB Modem function is used to connect to the 3G/4G network of the ISP (Internet Service Provider) as the WAN connection, after you connect the 3G/4G USB modem to the USB port.

 **Note:**

- For LTE USB, the US versions of this device are compatible with USB dongle, mobile hotspot and mifi devices produced in the US after 2020 and devices compatible with AT&T, Verizon, and T-Mobile products. This device also supports Android Tethering and Plug-and-Play features. To use your Android phone as a Modem, just connect it to the LTE USB port with a USB cable.
 - You can click Connect/Disconnect to enable/disable the USB LTE function, or configure the Upload/Download Bandwidth according to your need.
-

2 USB Modem Configuration

The USB Modem function is used to connect to the 3G/4G network of the ISP (Internet Service Provider) as the WAN connection, after you connect the 3G/4G USB modem to the USB port.

To configure the USB Modem, follow these steps:

- 1) Confirm that the USB modem is connected to the USB port properly.
- 2) Specify the ISP information. You can specify the location and ISP, or you can set the Dial Number, APN, Username and Password manually.
- 3) Select the connection mode and configure the parameters according to the requirements of your ISP.
- 4) Click Save.

2.1 Configuring USB Modem automatically

Choose the menu **USB > USB Modem** to load the following page.

Figure 2-1 Configuring the USB Modem automatically

3G/4G

USB Modem: No USB modem connected.

Config Type:

Location:

Mobile ISP:

Connection Mode: Connect Automatically
 Connect Manually

Upload Bandwidth: Kbps (100-1000000)

Download Bandwidth: Kbps (100-1000000)

Authentication Type: The default is Auto, do not change unless necessary.

PDP Type:

MTU Size(in bytes): The default is 1480, do not change unless necessary. (If you use a USB-to-RJ45 device, please modify the MTU to 1500)

Use The following DNS Servers: Enable

✘ Disconnected

Note

The USB Modem cannot be on the same network segment as the LAN IP. Otherwise the USB Modem may not be able to dial.

In the **3G/4G** section, select the Config Type as Auto. Enter the corresponding parameters and click **Save**.

USB Modem	Displays the status of the 3G/4G USB modem.
Location	Automatically selects and displays the region when the USB modem and SIM card are successfully identified. If not, select the region from the drop-down menu.
Mobile ISP	Displays the ISP of the 3G/4G network. If not automatically detected, select the ISP from the drop-down menu.
Dial Number, APN, Username and Password manually	If the ISP is not listed in the Mobile ISP list, select this checkbox and enter the Dial Number, APN (Access Point Name), Username and Password that are provided by the ISP.
Connection Mode	<p>Select the connection mode and configure the parameters according to the requirements of your ISP.</p> <p>Connect Automatically: In this mode, the Internet connection reconnects automatically anytime it gets disconnected.</p> <p>Connect Manually: In this mode, you can click the Connect or Disconnect button to control the Internet connection manually.</p>
Upload Bandwidth	Specify the upstream bandwidth of the USB Modem. This value is the upper limit of the Maximum Upstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of USB Modem and WAN ports after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
Download Bandwidth	Specify the downstream bandwidth of the USB Modem. This value is the upper limit of the Maximum Downstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of USB Modem and WAN ports after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
Authentication Type	<p>Select an authentication type. The default is Auto. Some ISPs require a specific authentication type, please confirm it with the ISP or keep the default settings.</p> <p>Auto: If Auto (default), the gateway automatically determines the authentication type used by the ISP.</p> <p>PAP: If PAP (Password Authentication Protocol), the gateway authenticates with the peer using two handshakes. Select this option if the ISP requires this authentication type.</p> <p>CHAP: If CHAP (Challenge Handshake Authentication Protocol), the gateway authenticates with the peer using three handshakes and validates the peer's identify periodically. Select this option if the ISP requires this authentication type.</p>
MTU Size	The default MTU (Maximum Transmission Unit) size is 1480 bytes. Do not change it unless required by the ISP.

Use the Following DNS Servers

If the ISP provides DNS server IP addresses, select this checkbox and enter the Primary DNS and Secondary DNS (optional) IP addresses below. Otherwise, the DNS servers will be assigned dynamically by the ISP.

Primary DNS: Enter the DNS IP address in dotted-decimal notation provided by the ISP.

Secondary DNS: (Optional) Enter another DNS IP address in dotted-decimal notation provided by the ISP.

2.2 Configuring the USB Modem manually

Choose the menu **USB > USB Modem** to load the following page..

Figure 2-2 Configuring the USB Modem manually

3G/4G

USB Modem: No USB modem connected.

Config Type:

Location:

Mobile ISP:

Connection Mode: Connect Automatically
 Connect Manually

Upload Bandwidth: Kbps (100-1000000)

Download Bandwidth: Kbps (100-1000000)

Authentication Type: The default is Auto, do not change unless necessary.

PDP Type:

MTU Size(in bytes): The default is 1480, do not change unless necessary. (If you use a USB-to-RJ45 device, please modify the MTU to 1500)

Use The following DNS Servers: Enable

✘ Disconnected

Note

The USB Modem cannot be on the same network segment as the LAN IP. Otherwise the USB Modem may not be able to dial.

In the **3G/4G** section, select the Config Type as Manual. Enter the corresponding parameters and click **Save**.

USB Modem Displays the status of the 3G/4G USB modem.

Dial Number, APN, Username and Password manually	If the ISP is not listed in the Mobile ISP list, select this checkbox and enter the Dial Number, APN (Access Point Name), Username and Password that are provided by the ISP.
Connection Mode	<p>Select the connection mode and configure the parameters according to the requirements of your ISP.</p> <p>Connect Automatically: In this mode, the Internet connection reconnects automatically anytime it gets disconnected.</p> <p>Connect Manually: In this mode, you can click the Connect or Disconnect button to control the Internet connection manually.</p>
Upload Bandwidth	Specify the upstream bandwidth of the USB Modem. This value is the upper limit of the Maximum Upstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of USB Modem and WAN ports after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
Download Bandwidth	Specify the downstream bandwidth of the USB Modem. This value is the upper limit of the Maximum Downstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of USB Modem and WAN ports after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
Authentication Type	<p>Select an authentication type. The default is Auto. Some ISPs require a specific authentication type, please confirm it with the ISP or keep the default settings.</p> <p>Auto: If Auto (default), the gateway automatically determines the authentication type used by the ISP.</p> <p>PAP: If PAP (Password Authentication Protocol), the gateway authenticates with the peer using two handshakes. Select this option if the ISP requires this authentication type.</p> <p>CHAP: If CHAP (Challenge Handshake Authentication Protocol), the gateway authenticates with the peer using three handshakes and validates the peer's identify periodically. Select this option if the ISP requires this authentication type.</p>
MTU Size	The default MTU (Maximum Transmission Unit) size is 1480 bytes. Do not change it unless required by the ISP.
Use the Following DNS Servers	<p>If the ISP provides DNS server IP addresses, select this checkbox and enter the Primary DNS and Secondary DNS (optional) IP addresses below. Otherwise, the DNS servers will be assigned dynamically by the ISP.</p> <p>Primary DNS: Enter the DNS IP address in dotted-decimal notation provided by the ISP.</p> <p>Secondary DNS: (Optional) Enter another DNS IP address in dotted-decimal notation provided by the ISP.</p>

3 USB Storage

3.1 Managing the USB Storage

Choose the menu **USB > USB Storage > USB Storage** to load the following page.

Figure 3-1 Managing the USB Storage

Device

Scan and Remove USB storage device.

Disk Drivers	Partition	Total	Operation
--	--	--	--

Backup

Click Backup to save a copy of your current settings. It is recommended to back up your settings before changing configurations or upgrading firmware.

Backup: Config
 Log

Choose USB:

Restore

Restore saved settings from a file.

Choose USB:

Plug your USB device into the USB port, then you can:

- 1) In the **Device** section, click scan to view USB storage information.
- 2) In the **Backup** section, click Backup to save a copy of your current settings. It is recommended to back up your settings before changing configurations or upgrading firmware.
- 3) In the **Restore** section, click **Restore** to restore saved settings form a file.

3.2 Auto Backup

Choose the menu **USB > USB Storage > Auto Backup** to load the following page.

Figure 3-2 Managing Auto Backup

Auto Backup

Auto Backup: Enable

Backup: Config Log

Occurrence: Every --- Of --- at 00 : 00 in UTC.

Maximum Number of Files: (1-50)

Data Retention Days: ---

Saving Path: ---

Available Backup Files

Filename	Backup Time	Size	Operation
--	--	--	--

- 1) Enable Auto Backup.
- 2) Select the content to be saved to the USB storage device. We recommend that you back up your current settings before upgrading or modifying them.
- 3) Set the backup frequency.
- 4) Specify the maximum number of files can be auto backed up.
- 5) Set how long will the backup will be kept.
- 6) Choose the backup saving path.
- 7) Click **Apply** to save the settings.

3.3 Firmware Upgrade via USB

Choose the menu **USB > USB Storage > Firmware Upgrade via USB** to load the following page.

Figure 3-3 Managing Firmware Upgrade via USB

Firmware Upgrade via USB

Firmware Version: 1.0.0 Build 20230626 Rel.86025(4555)

Hardware Version: ER706W v1.0

New Firmware File: ---

- 1) Click Browse to choose the file from the USB
- 2) Click Upgrade to upgrade the firmware.

Part 6

Configuring Preferences

CHAPTERS

1. Overview
2. IP Group Configuration
3. IPv6 Group Configuration
4. Time Range Configuration
5. VPN IP Pool Configuration
6. Service Type Configuration

1 Overview

You can preset certain preferences, such as IP groups, time ranges, IP Pools and service types. These preferences will appear as options for you to choose when you are configuring the corresponding parameters for some functions. For example, the IP groups configured here will appear as options when you are configuring the effective IP addresses for functions like Bandwidth Control, Session Limit , Policy Routing and so on.

Once you configure a preference here, it can be applied to multiple functions, saving time during the configuration. For example, after configuring a time range in the **Preferences > Time Range > Time Range** page, you can use this time range as the effective time of Bandwidth Control rules, Link Backup rules, Policy Routing rules, and so on.

2 IP Group Configuration

IP groups configured here can be used as effective IP addresses for multiple functions like Bandwidth Control, Session Limit, Policy Routing and so on.

To complete IP Group configuration, follow these steps:

- 1) Add IP address entries.
- 2) Add IP address entries to an IP group.

2.1 Adding IP Address Entries

Choose the menu **Preferences > IP Group > IP Address** and click **Add** to load the following page.

Figure 2-1 Add an IP Address Entry

IP Address List + Add - Delete

	ID	Name	IP Address Type	IP Address Range	IP Address/Mask	Description	Operation
--	--	--	--	--	--	--	--

Name:

IP Address Type: IP Address Range IP Address/Mask

-

Description: (Optional)

--	1	IP_LAN	IP Address/Mask	---	192.168.0.0/24	IP_LAN	---
----	---	--------	-----------------	-----	----------------	--------	-----

Follow these steps to add an IP address entry:

- 1) Enter a name and specify the IP address range.

Name	Enter a name for the IP address entry. Only letters, digits or underscores are allowed.
IP Address Type	Choose a type and enter the IP address in the corresponding format. Two types are provided: IP Address Range: Specify a starting IP address and an ending IP address. IP Address/Mask: Specify a network address and the subnet mask.
Description	(Optional) Enter a brief description of this IP address entry to make identifying it easier.

- 2) Click **OK**.

2.2 Grouping IP Address Entries

Choose the menu **Preferences > IP Group > IP Group** and click **Add** to load the following page.


Figure 2-2 Create an IP Group

Follow these steps to create an IP group and add IP address entries to the group:

- 1) Specify a name and configure the range to add an IP address range.

Group Name	Enter a name for the IP group. Only letters, digits or underscores are allowed.
Address Name	Select the IP address entries as the members of the group from the drop-down list. It is multi-optional. If no IP address entries are selected, the rule that references this IP group will have no effect on any IP addresses.
Description	(Optional) Enter an brief description of this IP group to make identifying it easier.

- 2) Click **OK**.

You can also choose an existing IP group and click  to add or remove the IP address members.

Note:

An IP group that is being referenced by a rule cannot be deleted.

3 IPv6 Group Configuration

In IPv6 Group, you can preset IPv6 groups that will appear as options for you to choose when configuring related parameters for some features, such as Bandwidth Control, Session Limit, and Policy Routing. After creating the entries, you can apply them to multiple configurations, which saves you from repeatedly setting up the same information.

To complete IPv6 Group configuration, follow these steps:

- 3) Click Add to add a new IPv6 group.
- 4) Enter a name, select the preset IPv6 address entries, and then configure the corresponding parameters for the new entry.
- 5) Select the created IPv6 group entry in related configurations, such as Bandwidth Control, Session Limit, and Policy Routing.

3.1 Adding IP Address Entries

Choose the menu **Preferences > IPv6 Group > IPv6 Address** and click **Add** to load the following page.

Figure 3-1 Add an IPv6 Address Entry

IPv6 Address List

+ Add - Delete

<input type="checkbox"/>	ID	Name	IPv6 Address/Mask	Description	Operation
--	--	--	--	--	--
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Name: <input style="width: 150px;" type="text"/></p> <p>IPv6 Address/Mask: <input style="width: 200px;" type="text"/> / <input style="width: 30px;" type="text"/></p> <p>Description: <input style="width: 150px;" type="text"/> (Optional)</p> <p style="text-align: left; margin-top: 5px;"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </p> </div>					
--	1	IPV6_LAN	fe80::0/64,/64	IPV6_LAN	

Follow these steps to add an IPv6 address entry:

- 1) Enter a name and specify the IPv6 address range.

Name	Enter a name for the IPv6 address entry. Only letters, digits or underscores are allowed.
IPv6 Address/Mask:	Specify a network address and a subnet mask. A rule that references the IPv6 address entry will be applied to the IPv6 addresses within the range in the entry.
Description	Enter a brief description for the IP address entry to facilitate your management. It can be 50 characters at most.

2) Click **OK**.

3.2 Grouping IP Address Entries

Choose the menu **Preferences > IPv6 Group > IPv6 Group** and click **Add** to load the following page.

Figure 3-2 Create an IPv6 Group

Group List + Add - Delete

<input type="checkbox"/>	ID	Group Name	Address Name	Description	Operation
--	--	--	--	--	--
<div style="display: flex; justify-content: space-between;"> <div style="width: 60%;"> <p>Group Name: <input style="width: 100%;" type="text"/></p> <p>Address Name: <input style="width: 100%;" type="text" value="---"/></p> <p>Description: <input style="width: 100%;" type="text"/> (Optional)</p> </div> <div style="width: 35%; text-align: right;"> <p><input type="button" value="OK"/> <input type="button" value="Cancel"/></p> </div> </div>					
--	1	IPV6GROUP_ANY	---	IPV6GROUP_ANY	
--	2	IPV6GROUP_LAN	IPV6_LAN	IPV6GROUP_LAN	

Follow these steps to create an IPv6 group and add IPv6 address entries to the group:

1) Specify a name and configure the range to add an IPv6 address range.

Group Name	Enter a name for the IPv6 group. Only letters, digits or underscores are allowed.
Address Name	Select the IPv6 address entry, and you can select more than one entry for one IPv6 group. A rule that references the IPv6 group will be applied to all the IPv6 addresses in the group.
Description	Enter a brief description for the address group to facilitate your management. It can be 50 characters at most.

2) Click **OK**.

Note:

The IPv6 group that has been referenced by a rule cannot be deleted unless the rule no longer references the IPv6 group.

The IPv6 group can be null, which means the IPv6 group contains no IPv6 address. A rule that references the address group will not take effect on any IPv6 address.

4 Time Range Configuration

Time range configuration allows you to define time ranges by specifying the period in a day and days in a week. The time range configured here can be used as the effective time for multiple functions like Bandwidth Control, Link Backup, Policy Routing and so on.

Choose the menu **Preferences > Time Range > Time Range** and click **Add** to load the following page.

Figure 4-1 Add a Time Range Entry

Time Range List

+ Add
 - Delete

<input type="checkbox"/>	ID	Time Range Name	Working Time	Description	Operation
--	--	--	--	--	--
<div style="border: 1px solid #ccc; padding: 5px;"> <div style="display: flex; justify-content: space-between;"> Time Range Name: <input style="width: 150px;" type="text"/> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Time Settings: <input checked="" type="radio"/> Working Calendar <input type="radio"/> Manually </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Working Calendar: </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> Description: <input style="width: 150px;" type="text"/> (Optional) </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </div> </div>					
--	1	Any		Any time	---

Follow these steps to add a time range entry:

- 1) Enter a name for the time range entry.

Time Range Name

Enter a name for the time range entry. Only letters, digits or underscores are allowed.

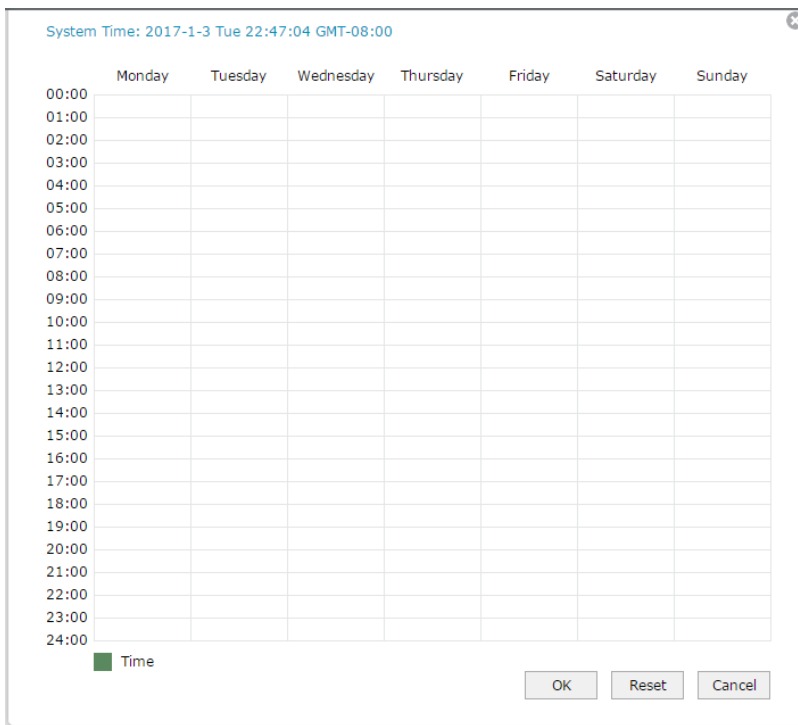
- 2) Choose a mode to set the time range. Two modes are provided: Working Calendar and Manually.

■ Working Calendar

Working Calendar mode allows you to set the time range on a calendar. In this mode, the effective time can be accurate to the hour.

Choose Working Calendar mode and click to load the following page.

Figure 4-2 Working Calendar Mode



Select the time slices and click **OK** to set the time range. You can click the time slices, or alternatively drag the areas to select or deselect the time slices.

■ **Manually**

Manually mode allows you to enter the time range and select the effective days in a week manually. In this mode, effective time can be accurate to the minute.

Choose Manually mode to load the following page.

Figure 4-3 Manually Mode

Time Settings: Working Calendar Manually

Week: Mon Tue Wed Thu Fri Sat Sun

Time range: [] : [] - [] : [] [+]

Week	Select the effective days in a week.
Time Range	Enter a start and end time. If the effective time is discontinuous, click [+] to add another time range.

- 3) (Optional) Enter an brief description of this time range to make identifying it easier.
- 4) Click **OK**.

 **Note:**

A time range entry that is being referenced by a rule cannot be deleted.

5 VPN IP Pool Configuration

The VPN IP pools configured here can be used as the VPN IP address pools when configuring L2TP VPN and PPTP VPN.

Choose the menu **Preferences > VPN IP Pool > VPN IP Pool** and click **Add** to load the following page.

Figure 5-1 Add an IP Pool Entry

IP Pool List

+ Add - Delete

<input type="checkbox"/>	ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
<input type="checkbox"/>	--	--	--	--	--

IP Pool Name:

Starting IP Address:

Ending IP Address:

OK Cancel

Follow these steps to add an IP Pool:

- 1) Enter a name and specify the starting and ending IP address of the IP Pool.

IP Pool Name	Enter a name for the IP Pool. Only letters, digits or underscores are allowed.
Starting IP Address/ Ending IP Address	Specify the starting and ending IP address. The range of the IP pool cannot overlap with the existing IP pools.

- 2) Click **OK**.

Note:

An IP pool entry that is being referenced by a rule cannot be deleted.

6 Service Type Configuration

The service type entries configured here can be used as part of the matching conditions when configuring the Access Control rules in Firewall.

Choose the menu **Preferences > Service Type > Service Type** to load the following page.

Figure 6-1 Service Type List

Service Type List						
<input type="checkbox"/>	ID	Service Type Name	Protocol	Detail	Description	Operation
--	1	ALL	0-255	---	ALL	---
--	2	FTP	TCP	Source Port = 0-65535; Destination Port = 21-21	FTP	---
--	3	SSH	TCP	Source Port = 0-65535; Destination Port = 22-22	SSH	---
--	4	TELNET	TCP	Source Port = 0-65535; Destination Port = 23-23	TELNET	---
--	5	SMTP	TCP	Source Port = 0-65535; Destination Port = 25-25	SMTP	---
--	6	DNS	UDP	Source Port = 0-65535; Destination Port = 53-53	DNS	---
--	7	HTTP	TCP	Source Port = 0-65535; Destination Port = 80-80	HTTP	---
--	8	POP3	TCP	Source Port = 0-65535; Destination Port = 110-110	POP3	---
--	9	SNTP	UDP	Source Port = 0-65535; Destination Port = 123-123	SNTP	---
--	10	H.323	TCP	Source Port = 0-65535; Destination Port = 1720-1720	H.323	---
--	11	ICMP_ALL	ICMP	Type =255; Code = 255	icmp	---
--	12	HTTPS	TCP	Source Port = 0-65535; Destination Port = 443-443	---	---

The entries in gray are system predefined service types. You can add other entries if your service type is not in the list.

Click **Add** to load the following page.

Figure 6-2 Add a Service Type Entry

Service Type List

+ Add - Delete

<input type="checkbox"/>	ID	Service Type Name	Protocol	Detail	Description	Operation
--	--	--	--	--	--	--

Service Type Name:

Protocol: TCP UDP TCP/UDP ICMP Other

Source Port Range: -

Destination Port Range: -

Description: (Optional)

Follow these steps to add a service type entry:

- 1) Enter a name for the service type.

Service Type Name Enter a name for the service type. Only letters, digits or underscores are allowed.

- 2) Select the protocol for the service type. The predefined protocols include **TCP**, **UDP**, **TCP/UDP** and **ICMP**. For other protocols, select the option **Other**.

When **TCP**, **UDP**, or **TCP/UDP** is selected, the following page will appear.

Figure 6-3 TCP/UDP Protocol

Protocol: TCP UDP TCP/UDP ICMP Other

Source Port Range: -

Destination Port Range: -

Source Port Range/ Destination Port Range Specify range of the source port and destination port of the TCP or UDP packets. Packets whose source port and destination port are both in the range are considered as the target packets.

When **ICMP** is selected, the following page will appear.

Figure 6-4 ICMP Protocol

Protocol: TCP UDP TCP/UDP ICMP Other

Type:

Code:

Type/Code Specify the type and code of the ICMP packets. ICMP packets with both the type and code fields matched are considered as the target packets.

When **Other** is selected, the following page will appear.

Figure 6-5 Other Protocols

Protocol:	<input type="radio"/> TCP	<input type="radio"/> UDP	<input type="radio"/> TCP/UDP	<input type="radio"/> ICMP	<input checked="" type="radio"/> Other
Protocol Number:	<input type="text"/>				

Protocol Number

Specify the protocol number of the packets. Packets with the protocol number field matched are considered as the target packets.

- 3) (Optional) Enter a brief description of this service type to make identifying it easier.
- 4) Click **OK**.

 **Note:**

A service type entry that is being referenced by a rule cannot be deleted.

Part 7

Configuring Transmission

CHAPTERS

1. Transmission
2. NAT Configurations
3. Bandwidth Control Configuration
4. Quality of Services Configurations
5. Session Limit Configurations
6. Load Balancing Configurations
7. Routing Configurations
8. Configuration Examples

1 Transmission

1.1 Overview

Transmission function provides multiple traffic control measures for the network. You can configure the transmission function according to your actual needs.

1.2 Supported Features

The transmission module includes NAT, Bandwidth Control, Session Limit, Load Balancing and Routing.

NAT

NAT (Network Address Translation) is the translation between private IP and public IP. NAT provides a way to allow multiple private hosts to access the public network using one public IP at the same time, which alleviates the shortage of IP addresses. Furthermore, NAT strengthens the LAN (Local Area Network) security since the address of LAN host never appears on the internet. The gateway supports following NAT features:

- One-to-One NAT

One-to-One NAT creates a relationship between a private IP address and a public IP address. A device with a private IP address can be accessed through the corresponding valid public IP address.

- Virtual Servers

When you build up a server in the local network and want to share it on the internet, Virtual Servers can realize the service and provide it to the internet users. At the same time Virtual Servers can keep the local network safe as other services are still invisible from the internet.

- Port Triggering

Port Triggering is a feature used to dynamically forward traffic on a certain port to a specific server on the local network. When a host in the local network initiates a connection to the triggering port, all the external ports will be opened for subsequent connections. The gateway can record the IP address of the host, when the data from the internet returns to the external ports, the gateway can forward them to the corresponding host. Port Triggering is mainly applied to online games, VoIPs, video players and so on.

- NAT-DMZ

When a PC is set to be a DMZ (Demilitarized Zone) host in the local network, it is totally exposed to the internet, which can realize the unlimited bidirectional communication between internal hosts and external hosts. The DMZ host becomes a virtual server with all ports opened. When you are not clear about which ports to open in some special applications, such as IP camera and database software, you can set the PC to be a DMZ host.

- ALG

Some special protocols such as FTP, H.323, SIP, IPSec and PPTP will work properly only when ALG (Application Layer Gateway) service is enabled.

Bandwidth Control

You can control the bandwidth by configuring bandwidth control rules for limiting various data flows. In this way, the network bandwidth can be reasonably distributed and utilized.

Session Limit

The amount of TCP and UDP sessions supported by the gateway is finite. If some local hosts transmit too many TCP and UDP sessions to the public network, the communication quality of the other local hosts will be affected, thus it is necessary to limit the sessions of those hosts.

Load Balancing

You can configure the traffic sharing mode of the WAN ports to optimize the resource utilization.

Routing

You can configure policy routing rules and static routing.

Policy routing provides a more accurate way to control the routing based on the policy defined by the network administrator.

Static routing is a form of routing that is configured manually by adding non-aging entries into a routing table. The manually-configured routing information guides the gateway in forwarding data packets to the specific destination.

2 NAT Configurations

With NAT configurations, you can:

- Configure the One-to-One NAT.
- Configure the Virtual Servers.
- Configure the Port Triggering.
- Configure the NAT-DMZ.
- Configure the ALG.

2.1 Configuring the One-to-One NAT

Choose the menu **Transmission > NAT > One-to-One NAT** and click **Add** to load the following page.

Figure 2-1 Configuring the One-to-One NAT

<input type="checkbox"/>	ID	Name	Interface	Original IP	Translated IP	DMZ Forwarding	Description	Status	Operation
--	--	--	--	--	--	--	--	--	--

Name:

Interface: ▼

Original IP:

Translated IP:

DMZ Forwarding: Enable

Description: (Optional)

Status: Enable

Follow these steps to configure the One-to-One NAT:

- 1) Specify the name of the One-to-One NAT rule and configure other related parameters.

Interface

Specify the effective interface for the rule. If you choose multiple ports, the entry will be applied to all selected ports simultaneously.

Original IP

Specify the original IP address for the rule. The original IP address cannot be the broadcast address, network address or IP address of the interface.

Translated IP	Specify the translated IP address for the rule. The translated IP address cannot be the broadcast address, network address or IP address of the interface.
DMZ Forwarding	Check the box to enable DMZ Forwarding. The packets transmitted to the translated IP address will be forwarded to the host of original IP address if DMZ Forwarding is enabled.
Description	Give a description for the rule entry to facilitate your management.
Status	Check the box to enable the rule.

2) Click **OK**.

 **Note:**

One-to-One NAT takes effect only when the connection type of WAN is Static IP.

2.2 Configuring the Virtual Servers

Choose the menu **Transmission > NAT > Virtual Servers** and click **Add** to load the following page.

Figure 2-2 Configuring the Virtual Servers

<input type="checkbox"/>	ID	Name	Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
--	--	--	--	--	--	--	--	--	--

Name:

Interface:

External Port: (XX or XX-XX ,1-65535)

Internal Port: (XX or XX-XX ,1-65535)

Internal Server IP:

Protocol:

Status: Enable

Follow these steps to configure the Virtual Servers:

1) Specify the name of the Virtual Server rule and configure other related parameters.

Interface	Specify the effective interface for the rule. If you choose multiple ports, the entry will be applied to all selected ports simultaneously.
External Port	Enter the service port or port range the gateway provided for accessing external network. The ports or port ranges cannot overlap with those of other virtual server rules.
Internal Port	Specify the service port or port range of the LAN host as virtual server.

Internal Server IP	Enter the IP address of the specified internal server for the entry. All the requests from the internet to the specified LAN port will be redirected to this host.
Protocol	Specify the protocol used for the entry.
Status	Check the box to enable the rule.

2) Click **OK**.

2.3 Configuring the Port Triggering

Choose the menu **Transmission > NAT > Port Triggering** and click **Add** to load the following page.

Figure 2-3 Configuring the Port Triggering

<input type="checkbox"/>	ID	Interface	Name	Trigger Port	Trigger Protocol	Incoming Port	Incoming Protocol	Status	Operation
--	--	--	--	--	--	--	--	--	--

Interface:

Name:

Trigger Port: (XX or XX-XX)

Trigger Protocol:

Incoming Port: (XX or XX-XX)

Incoming Protocol:

Status: Enable

Follow these steps to configure the Port Triggering:

1) Specify the name of the Port Triggering rule and configure other related parameters.

Interface	Specify the effective interface for the rule. If you choose multiple ports, the entry will be applied to all selected ports simultaneously.
Trigger Port	Enter the trigger port or port range. Each entry supports at most 5 groups of trigger ports. For example, you can enter 1-2, 3-4, 5-6, 7-8, 8-9. Note that the ports or port ranges cannot overlap with those of other port triggering rules.
Trigger Protocol	Specify the trigger protocol for the trigger port.
Incoming Port	Enter the incoming port or port range. Each entry supports at most 5 groups of incoming ports. For example, you can enter 1-2, 3-4, 5-6, 7-8, 8-9. Note that the ports or port ranges cannot overlap with those of other port triggering rules.
Incoming Protocol	Specify the incoming protocol for the incoming port.

Status	Check the box to enable the rule.
--------	-----------------------------------

2) Click **OK**.

2.4 Configuring the NAT-DMZ

Choose the menu **Transmission > NAT > NAT-DMZ** and click **Add** to load the following page.

Figure 2-4 Configuring the NAT-DMZ

<input type="checkbox"/>	ID	Name	Interface	Host IP Address	Status	Operation
--	--	--	--	--	--	--

Name:

Interface:

Host IP Address:

Status: Enable

Follow these steps to configure the NAT-DMZ:

1) Specify the name of the NAT-DMZ rule and configure other related parameters.

Interface	Specify the effective interface for the rule. If you choose multiple ports, the entry will be applied to all selected ports simultaneously.
-----------	---

Host IP Address	Specify the host IP address for NAT-DMZ.
-----------------	--

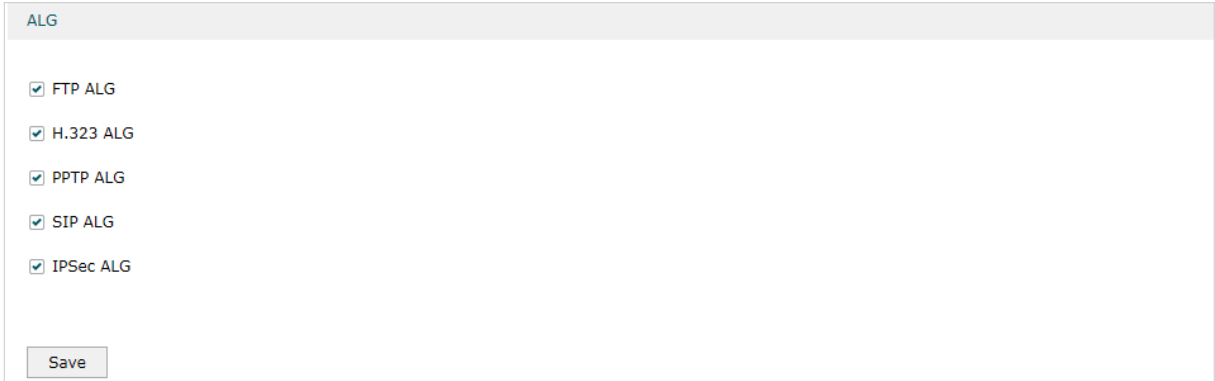
Status	Check the box to enable the rule.
--------	-----------------------------------

2) Click **OK**.

2.5 Configuring the ALG

Choose the menu **Transmission > NAT > ALG** to load the following page.

Figure 2-5 Configuring the ALG



The screenshot shows a configuration window titled "ALG". Inside the window, there are five checked checkboxes, each followed by a protocol name: "FTP ALG", "H.323 ALG", "PPTP ALG", "SIP ALG", and "IPSec ALG". At the bottom left of the window, there is a "Save" button.

Enable related ALG according to your needs and click **Save**.

3 Bandwidth Control Configuration

Bandwidth Control functions to control the bandwidth by configuring rules for limiting various data flows. In this way, the network bandwidth can be reasonably distributed and utilized.

Choose the menu **Transmission > Bandwidth Control** to load the following page.

Figure 3-1 Configuring the Bandwidth Control

Bandwidth Control Config

Enable Bandwidth Control

Enable Bandwidth Control when bandwidth usage reaches %

Bandwidth Control Rule List

+ Add - Delete

<input type="checkbox"/>	ID	Name	Direction	Group	Maximum Upstream Bandwidth	Maximum Downstream Bandwidth	Mode	Effective Time	Status	Operation
--	--	--	--	--	--	--	--	--	--	--

Follow these steps to configure the Bandwidth Control rule:

- 1) In the **Bandwidth Control Config** Section, enable Bandwidth Control function globally.

Enable
Bandwidth
Control

Check the box to enable Bandwidth Control globally.

Enable
Bandwidth
Control

With "Enable Bandwidth Control" selected, you can specify a percentage, and the Bandwidth Control will take effect only when the bandwidth usage reaches the percentage you specified.

- 2) In the **Bandwidth Control Rule List** section, click **Add** to load the following page.

Figure 3-2 Add Bandwidth Control rules

<input type="checkbox"/>	ID	Name	Direction	Group	Maximum Upstream Bandwidth	Maximum Downstream Bandwidth	Mode	Effective Time	Status	Operation
--	--	--	--	--	--	--	--	--	--	--

Name:

Direction: ▼

Group: ▼

Maximum Upstream Bandwidth: Kbps(100-10000000)

Maximum Downstream Bandwidth: Kbps(100-10000000)

Mode: Shared Individual

Effective Time: ▼

Description: (Optional)

ID: (Optional)

Status: Enable

Specify the name of the Bandwidth Control rule and configure other related parameters. Then click **OK**.

Direction	Specify the data stream direction for the rule.
Group	Specify the address group for the rule to define the controlled users. The IP group referenced here can be created on the Preferences > IP Group > IP Group page.
Maximum Upstream Bandwidth	Specify the Maximum Upstream Bandwidth in Kbps for the rule.
Maximum Downstream Bandwidth	Specify the Maximum Downstream Bandwidth in Kbps for the rule.
Mode	Specify the bandwidth control mode for the address group. Individual means the bandwidth of each user is equal to the current bandwidth of this entry. Shared means the total bandwidth of all controlled IP addresses is equal to the current bandwidth of this entry.
Effective Time	Specify the time for the rule to take effect. Any means it always takes effect. The time range referenced here can be created on the Preference > Time Range > Time Range page.
Description	Enter a brief description for the rule.
ID	Append the rule to the right position to give a priority for the rule.
Status	Check the box to enable the rule.














4 Quality of Services Configurations

4.1 Configuring Bandwidth Control

Bandwidth Control allows you to configure rules to limit various data flows. In this way, you can optimize the network performance by reasonably utilizing the bandwidth.

Choose the menu **Transmission > Quality of Services > Bandwidth Control** to load the following page.



Figure 4-1 Configuring the Bandwidth Control

Bandwidth Control								
Index	Status	Direction	Inbound/Outbound Bandwidth	Class 1	Class 2	Class 3	Others	Operation
WAN	Enabled 	Out	 1000000Kbps  1000000Kbps	25 %	25 %	25 %	25 %	 
---	Disabled	Out	 1000000Kbps  1000000Kbps	25 %	25 %	25 %	25 %	 
---	Disabled	Out	 1000000Kbps  1000000Kbps	25 %	25 %	25 %	25 %	 

Follow these steps to configure the Bandwidth Control rule:

- 1) Select a WAN interface, enable **Bandwidth Control** function.
- 2) In the **Operation** column, click **Edit** to load the following page.

Figure 4-2 Edit Bandwidth Control rules

Index	Status	Direction	Inbound/Outbound Bandwidth	Class 1	Class 2	Class 3	Others	Operation
WAN	Enabled	Out	↓1000000Kbps ↑1000000Kbps	25 %	25 %	25 %	25 %	 

Index: WAN

UDP Bandwidth Control: Enable

Limited Bandwidth Ratio: %


Outbound TCP ACK Prioritize: Enable

Status: Enable

Direction:

Inbound Bandwidth: Kbps(100-1000000)

Outbound Bandwidth: Kbps(100-1000000)



Class 1:	25	%
Class 2:	25	%
Class 3:	25	%
Others:	25	%

Configure the related parameters. Then click **OK**.

Index	Displays the WAN port. You can configure the QoS rule for a WAN port only when the port is enabled.
UDP Bandwidth Control	Check the box to enable UDP bandwidth control.
Limited Bandwidth Ratio	When UDP Bandwidth Control is enabled, specify the maximum bandwidth ratio allowed for UDP traffic in each class.
Outbound TCP ACK Prioritize	Check the box to prioritize outbound TCP ACK packets.
Status	Enable or disable QoS for the current entry.
Direction	Specify the direction of the controlled traffic. "Out" means control sending packets. "In" means receiving packets. "Both" means both are controlled.
Inbound/Outbound Bandwidth	Enter the maximum threshold of the inbound/outbound bandwidth.
Class1/Class2/Class3/Others	Specify the percentage of WAN bandwidth assigned to class1, class2, class3 and other traffic flowing through the WAN port.

4.2 Configuring Class Rule

Class Rule allows you to add or delete class rules. Rules will be matched from top to bottom according to the rule sequence number. When the traffic matches a rule, it will be assigned to the corresponding class and will not continue to match down.

Choose the menu **Transmission > Quality of Services > Class Rule**, click **Add** to load the following page.

Figure 4-3 Configuring the Class Rule

The screenshot shows a web interface for configuring a Class Rule. At the top right, there are '+ Add' and '- Delete' buttons. Below is a table with the following columns: Rule, Qos Class, Status, Local Address, Remote Address, DSCP, Service Type, and Operation. The table contains one row with dashes in all cells. Below the table is a configuration form with the following fields: Status (checked 'Enable'), IP Version (radio buttons for IPv4 and IPv6), Local Address (dropdown menu), Remote Address (dropdown menu), DSCP (dropdown menu), Service Type (dropdown menu), and Qos Class (dropdown menu). At the bottom of the form are 'OK' and 'Cancel' buttons.

Configure the related parameters. Then click **OK**.

Status	Check the box to enable the rule.
IP Version	Specify the protocol version: IPv4 or IPv6.
Local Address	Match the source IP address of the traffic. For IPv4 protocol, you can use the IP Group object configured in the Preferences > IP Group module. For the IPv6 protocol, you can use the IPv6 Group object configured in the Preferences > IPv6 Group module. QoS does not take effect on the traffic of LAN > LAN. When configuring the class rule, Local Address and Remote Address cannot select IPGROUP on the LAN side at the same time.
Remote Address	Match the destination IP address of the traffic. For IPv4 protocol, you can use the IP Group object configured in the Preferences > IP Group module. For the IPv6 protocol, you can use the IPv6 Group object configured in the Preferences > IPv6 Group module. QoS does not take effect on the traffic of LAN > LAN. When configuring the class rule, Local Address and Remote Address cannot select IPGROUP on the LAN side at the same time.
DSCP	Match the DSCP value of the traffic.

Service Type	Match the port number of the traffic. Select the service type object defined in the Preference > Service Type module.
QoS Class	Select the category of traffic that meets the rule.

4.3 Configuring VoIP Prioritization

You can enable the first priority for VoIP SIP/RTP traffic.

Choose the menu **Transmission > Quality of Services > VoIP Prioritization** to load the following page.

Figure 4-4 Configuring the VoIP Prioritization

Configure the related parameters. Then click **Save**.

Enable the First Priority for VoIP SIP/RTP	Check the box to enable prioritize VoIP traffic.
SIP UDP Port	Enter the UDP port ID of the VoIP traffic.

4.4 Configuring Tag Prioritization

You can add a DSCP or Precedence value for traffic in different classes.

Choose the menu **Transmission > Quality of Services > Tag Outbound Traffic** to load the following page.

Figure 4-5 Configuring the Tag Prioritization

Check the box for your desired class and select the DSCP or Precedence value. Then click **Save**.

5 Session Limit Configurations

To complete Session Limit configuration, follow these steps:

- 1) Configure session limit.
- 2) View the session limit information.

5.1 Configuring Session Limit

Choose the menu **Transmission > Session Limit > Session Limit** to load the following page.

Figure 5-1 Configuring the Session Limit

The screenshot shows a web interface for configuring session limits. It is divided into two main sections: 'General' and 'Session Limit Rule List'.

General Section:

- There is a checkbox labeled 'Enable Session Limit' which is currently unchecked.
- Below the checkbox is a 'Save' button.

Session Limit Rule List Section:

- At the top right of this section are two buttons: '+ Add' (in blue) and '- Delete' (in red).
- Below these buttons is a table with the following columns: ID, Name, Group, Max Sessions, Status, and Operation.
- The table currently contains one row with dashes ('--') in all columns, indicating no rules are currently defined.

Follow these steps to configure the Session Limit rule:

- 1) In the **General** Section, enable Session Limit function globally.
- 2) In the **Session Limit Rule List** section, click **Add** to load the following page.

Figure 5-2 Add Session Limit rules

The screenshot shows a dialog box for adding a new session limit rule. It features a table at the top and a form below.

Table:

ID	Name	Group	Max Sessions	Status	Operation
--	--	--	--	--	--

Form Fields:

- Name:** A text input field.
- Group:** A dropdown menu with a downward arrow.
- Max Sessions:** A text input field.
- Status:** A checkbox labeled 'Enable' which is checked.

At the bottom of the dialog are 'OK' and 'Cancel' buttons.

Specify the name of the Session Limit rule and configure other related parameters. Then click **OK**.

Group	Specify the address group to which the rule will be applied. The IP group referenced here can be created on the Preferences > IP Group > IP Group page.
Max Sessions	Specify the max sessions for the controlled users.
Status	Check the box to enable the rule.

5.2 Viewing the Session Limit Information

Choose the menu **Transmission > Session Limit > Session Monitor** to load the following page.

Figure 5-3 Viewing the Session Limit Information

Session Monitor List				
Entry Count: 1				 Refresh
<input type="checkbox"/>	ID	IP	Max Sessions	Current Sessions
<input type="checkbox"/>	1	192.168.0.100	1000	633

View the Session Limit information of hosts configured with Session Limit. Click the **Refresh** button to get the latest information.

6 Load Balancing Configurations

With load balancing configurations, you can:

- Configure the load balancing
- Configure the link backup
- Configure the online detection

6.1 Configuring the Load Balancing

Choose the menu **Transmission > Load Balancing > Basic Settings** to load the following page.

Figure 6-1 Configuring the Load Balancing

The screenshot shows a configuration page with two main sections: 'General' and 'Basic Settings'. In the 'General' section, there is a checkbox labeled 'Enable Load Balancing' which is checked, and a 'Save' button below it. The 'Basic Settings' section contains two checkboxes: 'Enable Application Optimized Routing' (checked) and 'Enable Bandwidth Based Balance Routing on port(s):' (unchecked). The latter checkbox is followed by a greyed-out drop-down menu. A 'Save' button is located at the bottom of the 'Basic Settings' section.

Follow these steps to configure the load balancing:

- 1) In the **General** Section, enable load balancing function globally and click **Save**.
- 2) In the **Basic Settings** section, select the appropriate method for load balancing and click **Save**.

Enable Application Optimized Routing

With Application Optimized Routing enabled, the gateway will consider the source IP address and destination IP address (or destination port) of the packets as a whole and record the WAN port they pass through. Then the packets with the same source IP address and destination IP address (or destination port) will be forwarded to the recorded WAN port. This feature ensures that multi-connected applications work properly.

Enable Bandwidth Based Balance Routing on port(s)

Select the WAN port from the drop-down list to enable Bandwidth Based Balance Routing.

6.2 Configuring the Link Backup

With Link Backup function, the gateway will switch all the new sessions from dropped lines automatically to another to keep an always on-line network.

Choose the menu **Transmission > Load Balancing > Link Backup** and click **Add** to load the following page.

Figure 6-2 Configuring the Link Backup Rule

<input type="checkbox"/>	ID	Primary WAN	Backup WAN	Mode	Effective Time	Status	Operation
--	--	--	--	--	--	--	--

Primary WAN:

Backup WAN:

Mode: Timing
 Failover(Enable backup link when any primary WAN fails).
 Failover(Enable backup link when all primary WANs fail).

Effective Time:

Status: Enable

Configure the following parameters on this page and click **OK**.


Primary WAN	Specify the primary WAN port. You can choose one primary WAN port, or choose multiple primary WAN ports to perform load balance.
Backup WAN	Specify the backup WAN port to back up the traffic for the primary WAN port under the specified condition.
Mode	Specify the mode as Timing or Failover. Timing: Link Backup will be enabled if the specified effective time is reached. All the traffic on the primary WAN will switch to the backup WAN at the beginning of the effective time; the traffic on the backup WAN will switch to the primary WAN at the ending of the effective time. Failover(Enable backup link when any primary WANs fails): Link Backup will be enabled when any primary WANs fails. Failover(Enable backup link when all primary WANs fail): Link Backup will be enabled only when all primary WANs fail.
Effective Time	Specify the time for the rule to take effect. "Any" means it takes effect at any time. The time range referenced here can be created on the Preference > Time Range > Time Range page.
Status	Check the box to enable the rule.

6.3 Configuring the Online Detection

With Online Detection function, you can detect the online status of the WAN port.

Choose the menu **Transmission > Load Balancing > Online Detection** and click  to load the following page.

Figure 6-3 Configuring the Online Detection

ID	Port	Port Status	Operation
1	WAN1	Offline	---
<div style="border: 1px solid #ccc; padding: 5px;"> <p>Port: <input type="text" value="WAN1"/></p> <p>Mode: <input checked="" type="radio"/> Auto <input type="radio"/> Manual <input type="radio"/> Always Online</p> <p>Ping: <input type="text" value="0.0.0.0"/></p> <p>DNS Lookup: <input type="text" value="0.0.0.0"/></p> <p><input type="button" value="OK"/> <input type="button" value="Cancel"/></p> </div>			
2	WAN2	Offline	

Configure the following parameters on this page and click **OK**.

Port	Displays the name of WAN Port.
Mode	Select the online detection mode. Auto: In Auto Mode, the DNS server of the WAN port will be selected as the destination for DNS Lookup to detect whether the WAN is online. Manual: In Manual Mode, you can configure the destination IP address for PING and DNS Lookup manually to detect whether the WAN is online. Always Online: In Always Online Mode, the status of the port will always be online.
Ping	With "Manual Mode" selected, specify the destination IP for Ping. The corresponding port will ping the IP address to detect whether the WAN port is online. 0.0.0.0 means Ping detection is disabled.
DNS Lookup	With "Manual Mode" selected, specify the IP address of DNS server. The corresponding port will perform the DNS lookup using default domain name to detect whether the WAN port is online. 0.0.0.0 means DNS Lookup is disabled.

7 Routing Configurations

With routing configurations, you can:

- Configure the static routing
- Configure the policy routing rule
- View the routing table

7.1 Configuring the Static Routing

Choose the menu **Transmission > Routing > Static Route** and click **Add** to load the following page.

Figure 7-1 Configuring the Static Routing

<input type="checkbox"/>	ID	Name	Destination IP	Subnet Mask	Next Hop	Interface	Metric	Status	Operation
--	--	--	--	--	--	--	--	--	--

Name:

Destination IP:

Subnet Mask:

Next Hop:

Interface: ▼

Metric: (0-15)

Description: (Optional)

Status: Enable

Specify the name of the static route entry and configure other related parameters. Then click **OK**.

Destination IP	Specify the destination IP address the route leads to.
Subnet Mask	Specify the subnet mask of the destination network.
Next Hop	Specify the IP address to which the packet should be sent next.
Interface	Specify the physical network interface through which this route is accessible.
Metric	Define the priority of the route. A smaller value means a higher priority. The default value is 0. It is recommended to keep the default value.

Description	Enter a brief description for the rule.
Status	Check the box to enable the rule.

7.2 Configuring the Policy Routing

Choose the menu **Transmission > Routing > Policy Routing** and click **Add** to load the following page.

Figure 7-2 Configuring the Policy Routing

<input type="checkbox"/>	ID	Name	Service Type	Source IP	Destination IP	WAN	Effective Time	Mode	Description	Status	Operation
--	--	--	--	--	--	--	--	--	--	--	--

Name:

Service Type:

Source IP:

Destination IP:

WAN:

Effective Time:

Mode:

Description: (Optional)

ID: (Optional)

Status: Enable

Specify the name of the policy routing entry and configure other related parameters. Then click **OK**.


Service Type	Specify the service type for the rule.
Source IP	Enter the source IP range for the rule. 0.0.0.0 - 0.0.0.0 means any IP is acceptable.
Destination IP	Enter the destination IP range for the rule. 0.0.0.0 - 0.0.0.0 means any IP is acceptable.
WAN	Specify the outgoing port for the rule. If you choose multiple ports, the entry will be applied to all selected ports simultaneously.
Effective Time	Specify the effective time for the rule.

Mode	Specify the policy routing mode for the rule. Priority: In Priority Mode, the rule depends on the online detection result. If any WAN port that you specify is online, the rule will take effect. If all the WAN ports that you specify are offline, the rule will not take effect. Only: In Only Mode, the rule always takes effect regardless of the WAN port status or online detection result.
Description	Enter a brief description for the rule.
Status	Check the box to enable the rule.

7.3 Viewing the Routing Table

Choose the menu **Transmission > Routing > Routing Table** to load the following page.

Figure 7-3 Routing Table

Routing Table					
Entry Count: 2					 Refresh
ID	Destination IP	Subnet Mask	Next Hop	Interface	Metric
1	127.0.0.0	255.0.0.0	0.0.0.0	lo	0
2	192.168.0.0	255.255.255.0	0.0.0.0	LAN	0

The **Routing Table** shows the information of the current route entries.

Destination IP	Displays the destination IP address the route leads to.
Subnet Mask	Displays the subnet mask of the destination network.
Next Hop	Displays the gateway IP address to which the packet should be sent next.
Interface	Displays the physical network interface through which this route is accessible.
Metric	Displays the metric to reach the destination IP address.

8 Configuration Examples

8.1 Example for Configuring NAT

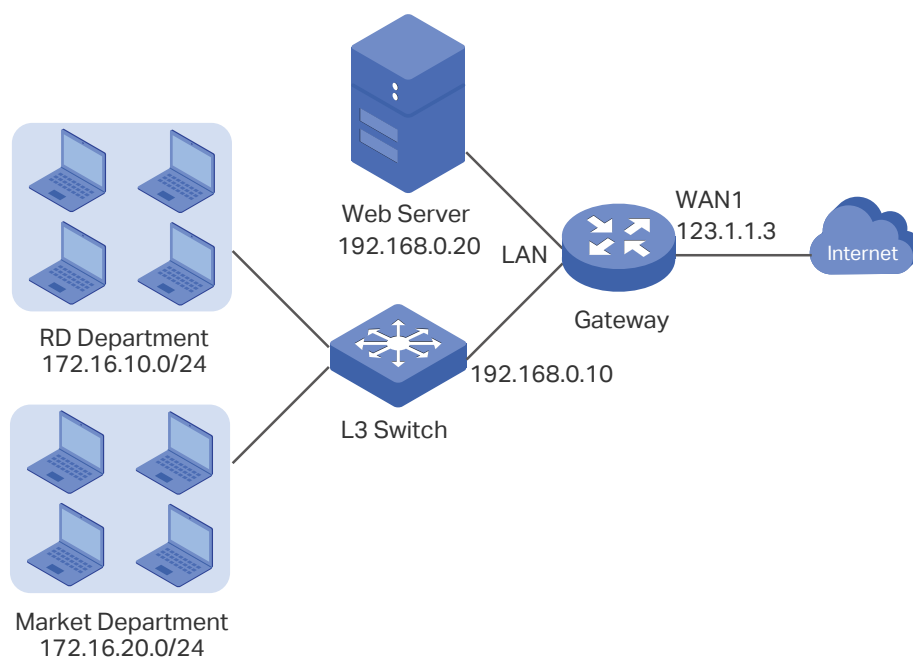
8.1.1 Network Requirements

A company has two departments: Market Department and RD department. Each department is assigned to an individual subnet. The company has the following requirements:

- 1) The two departments need to access the internet via the same gateway.
- 2) The company has a web server which needs to be accessed by the users on the internet.

8.1.2 Network Topology

Figure 8-1 Network Topology



8.1.3 Configuration Scheme

To meet the first requirement, configure static routing on the gateway to make sure the gateway know where to deliver the packets to IP addresses in different subnets (172.16.10.0/24, 172.16.20.0/24).

To meet the second requirement, add One-to-One NAT entry for the Web Server on the gateway, thus the web server with a private IP address can be accessed at a corresponding

valid public IP address. Note that One-to-One NAT take effects only when the connection type of WAN port is Static IP.

8.1.4 Configuration Procedure

Follow the steps below to configure NAT on the gateway:

■ Configuring the static routing

- 1) Choose the menu **Transmission > Routing > Static Route** to load the configuration page, and click **Add**.
- 2) Add static routes for the two departments respectively: Specify the entry name as RD/Market, enter 172.16.10.0/172.16.20.0 as the destination IP, and specify the VLAN 1 interface IP of L3 switch as next hop, then choose the interface as WAN1. Keep Status of this entry as **Enable**. Click **OK**.

Figure 8-2 Configuring the Static Routing for RD Department

Name:	RD
Destination IP:	172.16.10.0
Subnet Mask:	255.255.255.0
Next Hop:	192.168.0.10
Interface:	LAN
Metric:	0 (0-15)
Description:	(Optional)
Status:	<input checked="" type="checkbox"/> Enable

OK Cancel

Figure 8-3 Configuring the Static Routing for Market Department

Name:	Market
Destination IP:	172.16.20.0
Subnet Mask:	255.255.255.0
Next Hop:	192.168.0.10
Interface:	LAN
Metric:	0 (0-15)
Description:	(Optional)
Status:	<input checked="" type="checkbox"/> Enable

OK Cancel

■ Configuring the One-to-One NAT

- 1) Choose the menu **Transmission > NAT > One-to-One NAT** to load the configuration page, and click **Add**.

- 2) Add a One-to-One NAT entry for the web server: Specify the entry name as web, choose the interface as WAN1, and enter the original IP as 192.168.0.20, the translated IP as 123.1.1.3. Enable DMZ Forwarding, then keep Status of this entry as **Enable**. Click **OK**.

Figure 8-4 Adding a Multi-Nets Entry for RD Department

<input type="checkbox"/>	ID	Name	Interface	Original IP	Translated IP	DMZ Forwarding	Description	Status	Operation
--	--	--	--	--	--	--	--	--	--

Name:

Interface:

Original IP:

Translated IP:

DMZ Forwarding: Enable

Description: (Optional)

Status: Enable

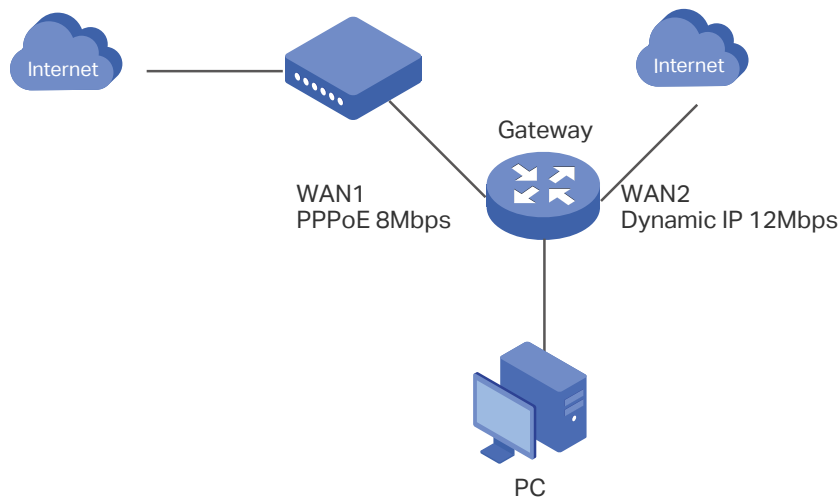
8.2 Example for Configuring Load Balancing

8.2.1 Network Requirements

To make good use of bandwidth, the network administrator decides to bind two WAN links using load balancing.

8.2.2 Network Topology

Figure 8-5 Network Topology



8.2.3 Configuration Scheme

To meet the requirement, configure WAN parameters on the gateway in order that the two WAN links can work properly and have access to the internet, then configure load balancing on the gateway to aggregate two WAN links.

8.2.4 Configuration Procedure

Follow the steps below to configure load balancing on the gateway:

■ Configuring the WAN parameters

For WAN1 port, configure the connection type as PPPoE, and specify Upstream and Downstream bandwidth for this link based on your ADSL bandwidth (You could consult your internet Service Provider for the bandwidth information).

For WAN2 port, configure the connection type as Dynamic IP, and specify Upstream and Downstream bandwidth for this link according to data that ISP provides.

Make sure two WAN links can work properly and have access to the internet.

■ Configuring the Load Balancing

Choose the menu **Transmission > Load Balancing > Basic Settings** to load the configuration page. Enable Load Balancing globally, and click **Save**. Enable Application Optimized Routing, and enable Bandwidth Based Balancing Routing on WAN1 port and WAN2 port. Click **Save**.

Figure 8-6 Configuring the Load Balancing

The screenshot shows a configuration window with two sections: 'General' and 'Basic Settings'. In the 'General' section, the checkbox 'Enable Load Balancing' is checked, and there is a 'Save' button below it. In the 'Basic Settings' section, two checkboxes are checked: 'Enable Application Optimized Routing' and 'Enable Bandwidth Based Balance Routing on port(s):'. The second checkbox has a dropdown menu next to it showing 'WAN1, WAN2'. There is also a 'Save' button at the bottom of this section.

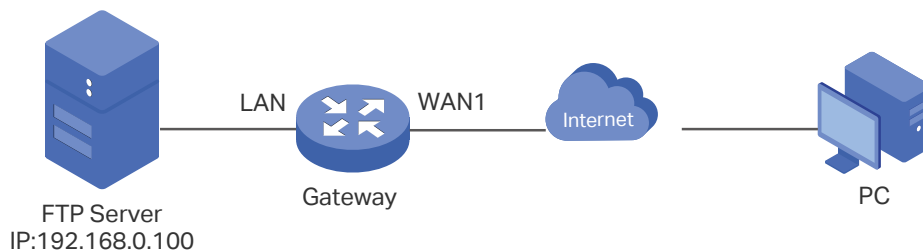
8.3 Example for Configuring Virtual Server

8.3.1 Network Requirements

The network administrator builds up a FTP server on the local network and wants to share it on the internet.

8.3.2 Network Topology

Figure 8-7 Network Topology



8.3.3 Configuration Scheme

In this scenario, both virtual server and DMZ host can be configured to meet the requirement. Here we take configuring Virtual Server as an example, owing to that for a DMZ host all ports are open which may result in unsafety. Configure the FTP server as a virtual server on the gateway so that the FTP server can be accessed by the internet user.

8.3.4 Configuration Procedure

Follow the steps below to configure virtual server on the gateway:

- 1) Choose the menu **Transmission > NAT > Virtual Servers** to load the configuration page, and click **Add**.

- 2) Specify the entry name as ftp, choose the interface as WAN1, and specify the internal/external port as 21, enter the IP address of FTP server (192.168.0.100) as the internal server IP. Select the protocol as All, then keep Status of this entry as **Enable**. Click **OK**.

Figure 8-8 Configuring the Virtual Server

ID	Name	Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
--	--	--	--	--	--	--	--	--

Name:

Interface:

External Port: (XX or XX-XX ,1-65535)

Internal Port: (XX or XX-XX ,1-65535)

Internal Server IP:

Protocol:

Status: Enable

8.4 Example for Configuring Policy Routing

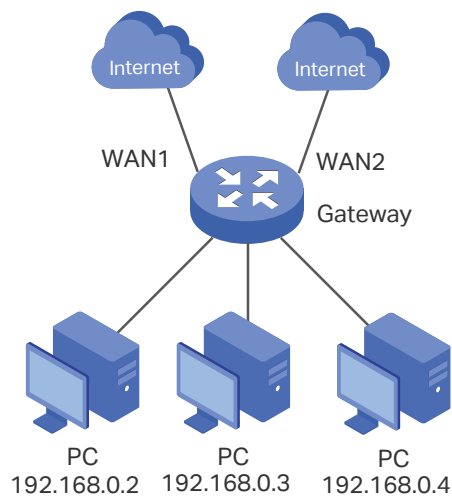
8.4.1 Network Requirements

The network administrator has a gateway with 3 computers (192.168.0.2-192.168.0.4) connected to the LAN side, all computers are routed to internet by WAN1 port and WAN2 port, the requirements are as follows:

- WAN2 link is used to backup WAN1 link to keep an always on-line network.
- The two computers with IP addresses 192.168.0.2 and 192.168.0.3 are required to use WAN1 for web surfing, WAN2 for other internet activities.

8.4.1 Network Topology

Figure 8-9 Network Topology



8.4.2 Configuration Scheme

To meet the first requirement, configure link backup on the gateway. To meet the second requirement, configure policy routing rules for two computers which use 192.168.0.2 and 192.168.0.3. Note that link backup rule has a higher priority than policy routing rule.

8.4.3 Configuration Procedure

Follow the steps below to configure link backup and policy routing on the gateway:

■ Configuring the Link Backup

- 1) Choose the menu **Transmission > Load Balancing > Link Backup** to load the configuration page, and click **Add**.
- 2) Specify the primary WAN as WAN1, the backup WAN as WAN2 and the mode as **Failover (Enable backup link when any primary WAN fails)**, so that the backup WAN will be enabled when the primary WAN failed. Keep Status of this entry as Enable. Click **OK**.

Figure 8-10 Configuring the Link Backup

<input type="checkbox"/>	ID	Primary WAN	Backup WAN	Mode	Effective Time	Status	Operation
--	--	--	--	--	--	--	--

Primary WAN: WAN1

Backup WAN: WAN2

Mode:

Timing

Failover(Enable backup link when any primary WAN fails).

Failover(Enable backup link when all primary WANs fail).

Effective Time: Any

Status: Enable

OK Cancel

■ **Configuring the Policy Routing Rules**

- 1) Choose the menu **Preferences > IP Group > IP Address** to load the configuration page, and click **Add**. Specify the IP address name as tp, the IP address type as IP Address Range (192.168.0.2-192.168.0.3). Click **OK**.

Figure 8-11 Configuring the IP Address

<input type="checkbox"/>	ID	Name	IP Address Type	IP Address Range	IP Address/Mask	Description	Operation
--	--	--	--	--	--	--	--

Name: tp

IP Address Type:

IP Address Range IP Address/Mask

192.168.0.2 - 192.168.0.3

Description: (Optional)

OK Cancel

- 2) Choose the menu **Preferences > IP Group > IP Address** to load the configuration page and click **Add**. Specify the IP group name as group1, the IP address name as tp to reference the IP address you have created. Click **OK**.

Figure 8-12 Configuring the IP Group

<input type="checkbox"/>	ID	Group Name	Address Name	Description	Operation
--	--	--	--	--	--

Group Name: group1

Address Name: tp

Description: (Optional)

OK Cancel

- 3) Choose the menu **Transmission > Routing > Policy routing** to load the configuration page, and click **Add**.

Specify the policy routing rule name as policy1, the service type as HTTP, the source IP as group1, the destination IP as IPGROUP_ANY which means no limit. Choose WAN1, and keep Status of this entry as **Enable**. Click **OK**.

Figure 8-13 Configuring the Policy Routing Rule 1

ID	Name	Service Type	Source IP	Destination IP	WAN	Effective Time	Mode	Description	Status	Operation
--	--	--	--	--	--	--	--	--	--	--

Name:

Service Type:

Source IP:

Destination IP:

WAN:

Effective Time:

Mode:

Description: (Optional)

ID: (Optional)

Status: Enable

Specify the policy routing rule name as policy2, the service type as ALL, the source IP as group1, the destination IP as IPGROUP_ANY which means no limit. Choose WAN2, and keep Status of this entry as **Enable**. Click **OK**.

Figure 8-14 Configuring the Policy Routing Rule 2

ID	Name	Service Type	Source IP	Destination IP	WAN	Effective Time	Mode	Description	Status	Operation
--	--	--	--	--	--	--	--	--	--	--

Name:

Service Type:

Source IP:

Destination IP:

WAN:

Effective Time:

Mode:

Description: (Optional)

ID: (Optional)

Status: Enable

Part 8

Configuring Firewall

CHAPTERS

1. Firewall
2. Firewall Configuration
3. Configuration Examples

1 Firewall

1.1 Overview

Firewall is used to enhance the network security. It can prevent external network threats from spreading to the internal network, protect the internal hosts from ARP attacks, and control the internal users' access to the external network.

1.2 Supported Features

The Firewall module supports four functions: Anti ARP Spoofing, Attack Defense, and Access Control.

Anti ARP Spoofing

ARP (Address Resolution Protocol) is used to map IP addresses to the corresponding MAC addresses so that packets can be delivered to their destinations. However, since ARP is implemented with the premise that all the hosts and gateways are trusted, there are high security risks on real, complex networks. If attackers send ARP spoofing packets with false IP address-to-MAC address mapping entries, the device will update the ARP table based on the false ARP packets and record wrong mapping entries, which results in a breakdown of normal communication.

Anti ARP Spoofing can protect the network from ARP spoofing attacks. It works based on the IP-MAC Binding entries. These entries record the correct one-to-one relationships between IP addresses and MAC addresses. When receiving an ARP packet, the gateway checks whether it matches any of the IP-MAC Binding entries. If not, the gateway will ignore the ARP packets. In this way, the gateway maintains the correct ARP table.

In addition, the gateway provides the following two sub functions:

- Permitting the packets matching the IP-MAC Binding entries only and discarding other packets.
- Sending GARP packets to the hosts when it detects ARP attacks. The GARP packets can inform hosts of the correct ARP table, preventing their ARP tables from being falsified by ARP spoofing packets.

Attack Defense

Attacks on a network device can cause device or network paralysis. With the Attack Defense feature, the gateway can identify and discard various attack packets which are sent to the CPU, and limit the packet receiving rate. In this way, the gateway can protect itself and the connected network against malicious attacks.

The gateway provides two types of Attack Defense: Flood Defense and Packet Anomaly Defense. Flood Defense limits the receiving rate of the specific types of packets, and Packet Anomaly Defense discards the illegal packets directly.

Access Control

Access Control can filter the packets passing through the gateway based on the Access Control rules. An Access Control rule includes a filter policy and some conditions, such as service type, receiving interface and effective time. The gateway will apply the filter policy to the packets matching these conditions, and thus to limit network traffic, manage network access behaviors and more.

Access Control can prevent various network attacks, such as attacks on TCP (Transmission Control Protocol) and ICMP (Internet Control Message Protocol) packets, and can also manage network access behaviors, such as controlling access to the internet.

2 Firewall Configuration

In Firewall module, you can configure the following features:

- Anti ARP Spoofing
- Attack Defense
- MAC Filtering
- Access Control

2.1 Anti ARP Spoofing

To complete Anti ARP Spoofing configuration, there are two steps. First, add IP-MAC Binding entries to the IP-MAC Binding List. Then enable Anti ARP Spoofing for these entries.

 **Note:**

In case Anti ARP Spoofing causes access problems to the currently connected devices, we recommend that you add and verify the IP-MAC Binding entries first before enabling Anti ARP Spoofing.

2.1.1 Adding IP-MAC Binding Entries

You can add IP-MAC Binding entries in two ways: manually and via ARP scanning.

- Adding IP-MAC Binding Entries Manually

You can manually bind the IP address, MAC address and interface together on the condition that you have got the related information of the hosts on the network.

- Adding IP-MAC Binding Entries via ARP Scanning

With ARP Scanning, the gateway sends the ARP request packets with the specific IP field to the hosts. Upon receiving the ARP reply packet, the gateway can get the IP address, MAC address and connected interface of the host.

The following sections introduce these two methods in detail.

Adding IP-MAC Binding Entries Manually

Before adding entries manually, get the IP addresses and MAC addresses of the hosts on the network and make sure of their accuracy.

Choose the menu **Firewall > Anti ARP Spoofing > IP-MAC Binding** to load the following page.

Figure 2-1 IP-MAC Binding Page

General

Enable ARP Spoofing Defense

Permit the packets matching the IP-MAC Binding entries only

Send GARP packets when ARP attack is detected

Interval: ms

IP-MAC Binding List

<input type="checkbox"/>	ID	IP Address	MAC Address	Interface	Description	Status	Operation
<input type="checkbox"/>	--	--	--	--	--	--	--

Follow the steps below to add IP-MAC Binding entries manually. The entries will take effect on the LAN interface.

- 1) In the **IP-MAC Binding List** section, click **Add** to load the following page.

Figure 2-2 Add IP-MAC Binding Entries Manually

IP-MAC Binding List

<input type="checkbox"/>	ID	IP Address	MAC Address	Interface	Description	Status	Operation
<input type="checkbox"/>	--	--	--	--	--	--	--

IP Address:

MAC Address:

Description: (Optional, 0-50 characters)

Status: Enable

- 2) Configure the following parameters on this page.

IP Address	Enter an IP address to be bound.
MAC Address	Enter a MAC address to be bound.

Description	Give a description for identification.
Status	Enable this entry. Only when the status is Enable will this entry be effective.

3) Click **OK** and the added entry will be displayed in the list.

Adding IP-MAC Binding Entries via ARP Scanning

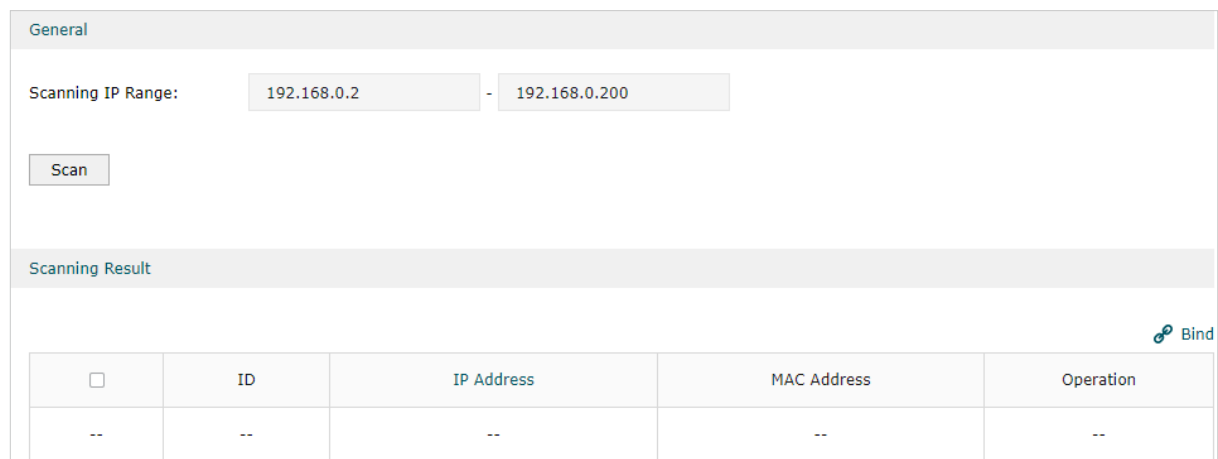
If you want to get the IP addresses and MAC addresses of the hosts quickly, you can use ARP Scanning to facilitate your operation.

 **Note:**

Before using this feature, make sure that your network is safe and the hosts are not suffering from ARP attacks at present; otherwise, you may obtain incorrect IP-MAC Binding entries. If your network is being attacked, it's recommended to bind the entries manually.

Choose the menu **Firewall > Anti ARP Spoofing > ARP Scanning** to load the following page.

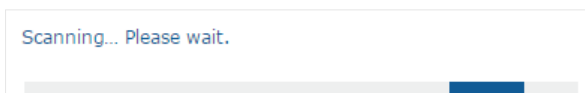
Figure 2-3 Add IP-MAC Binding Entries via ARP Scanning



Follow the steps below to add IP-MAC Binding entries via ARP Scanning.

1) Click **Scan** and the following window will pop up.

Figure 2-4 ARP Scanning Process





2) Wait for a moment without any operation. The scanning result will be displayed in the following table. Click  to export the corresponding entry to the IP-MAC Binding table, or select multiple entries and click  Bind to export the entries to the IP-MAC Binding table in batch.

Figure 2-5 ARP Scanning Result

Scanning Result				
<input type="checkbox"/>	ID	IP Address	MAC Address	Operation
<input type="checkbox"/>	1	192.168.0.100	00-0A-EB-13-A2-3D	
<input type="checkbox"/>	2	192.168.0.200	00-19-66-35-E1-B0	
<input type="checkbox"/>	3	192.168.0.73	00-0A-EB-00-13-01	
<input type="checkbox"/>	4	192.168.0.37	00-0A-EB-03-12-A4	

Also, you can go to **Firewall > Anti ARP Spoofing > ARP List** to view and bind the ARP Scanning entries. The ARP Scanning list displays all the historical scanned entries. Click to export the corresponding entry to the IP-MAC Binding table, or select multiple entries and click **Bind** to export the entries to the IP-MAC Binding table in batch.

Figure 2-6 ARP List

ARP List					
<input type="checkbox"/>	ID	IP Address	MAC Address	Interface	Operation
<input type="checkbox"/>	1	192.168.0.100	00-0A-EB-13-A2-3D	LAN	---
<input type="checkbox"/>	2	192.168.0.200	00-19-66-35-E1-B0	LAN	

2.1.2 Enable Anti ARP Spoofing

Choose the menu **Firewall > Anti ARP Spoofing > IP-MAC Binding** to load the following page.

Figure 2-7 IP-MAC Binding-General Config

General

Enable ARP Spoofing Defense

Permit the packets matching the IP-MAC Binding entries only

Send GARP packets when ARP attack is detected

Interval: ms

IP-MAC Binding List

Add Delete

<input type="checkbox"/>	ID	IP Address	MAC Address	Interface	Description	Status	Operation
<input type="checkbox"/>	--	--	--	--	--	--	--

Follow the steps below to configure Anti ARP Spoofing rule:

- 1) In the **General** section, enable ARP Spoofing Defense globally. With this option enabled, the gateway can protect its ARP table from being falsified by ARP spoofing packets.
- 2) Choose whether to enable the two sub functions.

Permit the packets matching the IP-MAC Binding entries only

With this option enabled, when receiving a packet, the gateway will check whether the IP address, MAC address and receiving interface match any of the IP-MAC Binding entries. Only the matched packets will be forwarded.

Send GARP packets when ARP attack is detected

With this option enabled, the gateway will send GARP packets to the hosts if it detects ARP spoofing packets on the network. The GARP packets will inform the hosts of the correct ARP information, which is used to replace the wrong ARP information in the hosts.

Interval

If the **Send GARP packets when ARP attack is detected** is enabled, configure the time interval for sending GARP packets. The valid values are from 1 to 10000 milliseconds.

- 3) Click **Save**.

 **Note:**

Before enabling "Permit the packets matching the IP-MAC Binding entries only", you should make sure that your management host is in the IP-MAC Binding list. Otherwise, you cannot log in to the Web management page of the gateway. If this happens, restore your gateway to factory defaults and then log in using the default login credentials.

2.2 Configuring Attack Defense

Choose the menu **Firewall > Attack Defense > Attack Defense** to load the following page.

Figure 2-8 Attack Defense

Flood Defense

<input type="checkbox"/> Multi-connections TCP SYN Flood	10000	Pkt/s
<input type="checkbox"/> Multi-connections UDP Flood	12000	Pkt/s
<input type="checkbox"/> Multi-connections ICMP Flood	1500	Pkt/s
<input type="checkbox"/> Stationary source TCP SYN Flood	4000	Pkt/s
<input type="checkbox"/> Stationary source UDP Flood	6000	Pkt/s
<input type="checkbox"/> Stationary source ICMP Flood	600	Pkt/s

Packet Anomaly Defense

- Block TCP Scan (Stealth FIN/Xmas/Null)
- Block Ping of Death
- Block Large Ping
- Block Ping from WAN
- Block WinNuke attack
- Block TCP packets with SYN and FIN Bits set
- Block TCP packets with FIN Bit set but no ACK Bit set
- Block packets with specified IP options
 - Security Option Loose Source Route Option
 - Strict Source Route Option Record Route Option
 - Stream Option Timestamp Option
 - No Operation Option

Follow the steps below to configure Attack Defense.

- 1) In the **Flood Defense** section, check the box and configure the corresponding parameters to enable your desired feature. By default, all the options are disabled. For details, refer to the following table:

<p>Multi-connections TCP SYN Flood</p>	<p>With this feature enabled, the gateway will filter the subsequent TCP SYN packets if the number of this kind of packets reaches the specified threshold. The valid threshold ranges from 100 to 99999.</p>
<p>Multi-connections UDP Flood</p>	<p>With this feature enabled, the gateway will filter the subsequent UDP packets if the number of this kind of packets reaches the specified threshold. The valid threshold ranges from 100 to 99999.</p>
<p>Multi-connections ICMP Flood</p>	<p>With this feature enabled, the gateway will filter the subsequent ICMP packets if the number of this kind of packets reaches the specified threshold. The valid threshold ranges from 100 to 99999.</p>

Stationary source TCP SYN Flood	With this feature enabled, the gateway will filter the subsequent stationary source TCP SYN packets if the number of this kind of packets reaches the specified threshold. The valid threshold ranges from 100 to 99999.
Stationary source UDP Flood	With this feature enabled, the gateway will filter the subsequent stationary source UDP SYN packets if the number of this kind of packets reaches the specified threshold. The valid threshold ranges from 100 to 99999.
Stationary source ICMP Flood	With this feature enabled, the gateway will filter the subsequent stationary source ICMP SYN packets if the number of this kind of packets reaches the specified threshold. The valid threshold ranges from 100 to 99999.

- 2) In the **Packet Anomaly Defense** section, directly check the box to enable your desired feature. By default, all the options are enabled. For details, refer to the following table:

Block TCP Scan (Stealth FIN/Xmas/Null)	With this option enabled, the gateway will filter the TCP scan packets of Stealth FIN, Xmas and Null.
Block Ping of Death	With this option enabled, the gateway will block Ping of Death attack. Ping of Death attack means that the attacker sends abnormal ping packets larger than 65535 bytes to cause system crash on the target computer.
Block Large Ping	With this option enabled, the gateway will block Large Ping attacks. Large Ping attack means that the attacker sends multiple ping packets larger than 1500 bytes to cause the system crash on the target computer.
Block Ping from WAN	With this option enabled, the gateway will block the ICMP request from WAN.
Block WinNuke attack	With this option enabled, the gateway will block WinNuke attacks. WinNuke attack refers to a remote denial-of-service attack (DoS) that affects some Windows operating systems, such as the Windows 95 and Windows N. The attacker sends a string of OOB (Out of Band) data to the target computer on TCP port 137, 138 or 139, causing system crash or Blue Screen of Death.
Block TCP packets with SYN and FIN Bits set	With this option enabled, the gateway will filter the TCP packets with both SYN Bit and FIN Bit set.
Block TCP packets with FIN Bit set but no ACK Bit set	With this option enabled, the gateway will filter the TCP packets with FIN Bit set but without ACK Bit set.
Block packets with specified IP options	With this option enabled, the gateway will filter the packets with specified IP options. You can choose the options according to your needs.

- 3) Click **Save** to save the settings.

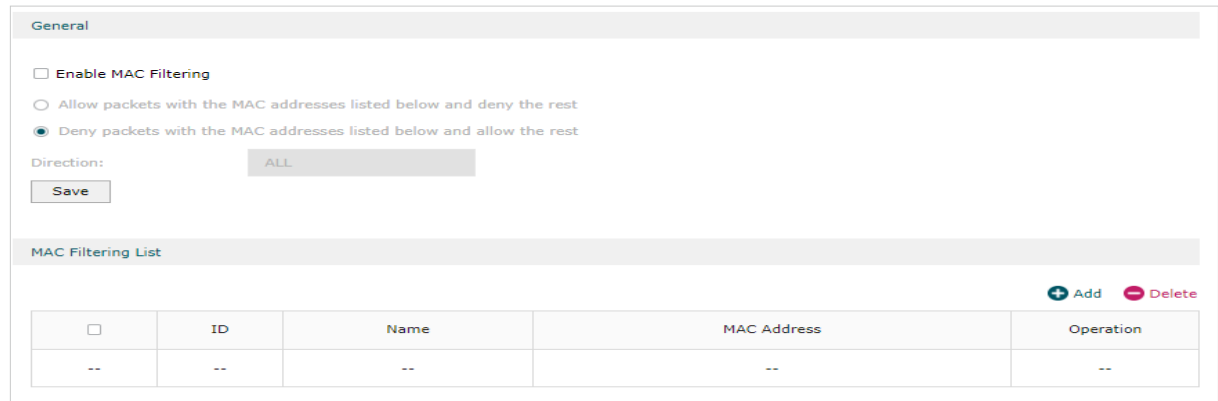
2.3 Configuring MAC Filtering

MAC Filtering can drop or allow packets from certain devices passing through the gateway based on the MAC address of the devices. After the MAC filtering policy and MAC filtering

list are configured, the gateway will apply the filter policy to the packets matching the MAC address, and thus limit network traffic and manage network access behaviors.

Choose the menu **Firewall > MAC Filtering > MAC Filtering** to load the following page.

Figure 2-9 MAC Filtering



Follow the steps below to configure MAC Filtering.

- 1) In the **General** section, check the box to enable the MAC Filtering feature, configure the corresponding parameters and click **Save**.

Allow packets with the MAC addresses listed below and deny the rest

Select to allow packets with the listed MAC address to pass through the gateway, and packets with other MAC addresses will be dropped.

Deny packets with the MAC addresses listed below and allow the rest

Select to drop packets with the listed MAC address, and the packets with other MAC addresses will be allowed to pass through the gateway.

Direction

Select All when you want to apply the policy to traffic both from LAN to LAN and from LAN to WAN. Select LAN -> WAN when you want to apply the policy only to traffic from LAN to WAN.

- 2) In the **MAC Filtering List** section, click Add to load the following page.

Figure 2-10 MAC Filtering



- 3) Specify the MAC name and address and click **OK**.

MAC Address

Specify the MAC address of the device, and the MAC filtering policy will be applied to traffic with the MAC address.

2.4 Configuring Access Control

Choose the menu **Firewall > Access Control > Access Control** and click **Add** to load the following page.

Figure 2-11 Access Control

<input type="checkbox"/>	ID	Name	Source	Destination	Policy	Service Type	Interface	Effective Time	Operation
--	--	--	--	--	--	--	--	--	--

Name: (1-50 characters)

This table displays the Access Control entries. Follow the steps below to add a new Access Control entry.

- 1) Click **Add** and the following page will appear.

Figure 2-12 Access Control

Access Control List

ID Name Source Destination Policy Service Type Interface Effective Time Operation

-- -- -- -- -- -- -- -- -- --

Name: (1-50 characters)

Policy:

Service Type:

Interface:

Source:

Destination:

Effective Time:

ID: (Optional)

- 2) Configure the required parameters and click **OK**:

Name	Specify a name for the rule. It can be 50 characters at most. The name of each entry cannot be repeated.
Policy	Select whether to block or allow the packets matching the rule to access the network.
Service Type	Select the effective service for the rule. The service referenced here can be created on the Preferences > Service Type page.
Direction	Select the effective traffic direction for the rule.

Source	Select an IP group to specify the source address range for the rule. The IP group referenced here can be created on the Preferences > IP Group page.
Destination	Select an IP group to specify the destination address range for the rule. The IP group referenced here can be created on the Preferences > IP Group page.
Effective Time	Select the effective time for the rule. The effective time referenced here can be created on the Preferences > Time Range page.
ID	Specify a rule ID. A smaller ID means a higher priority. This value is optional, and the newly added rule without this value configured will get the largest ID among all rules, which means the newly added rule has the lowest priority.

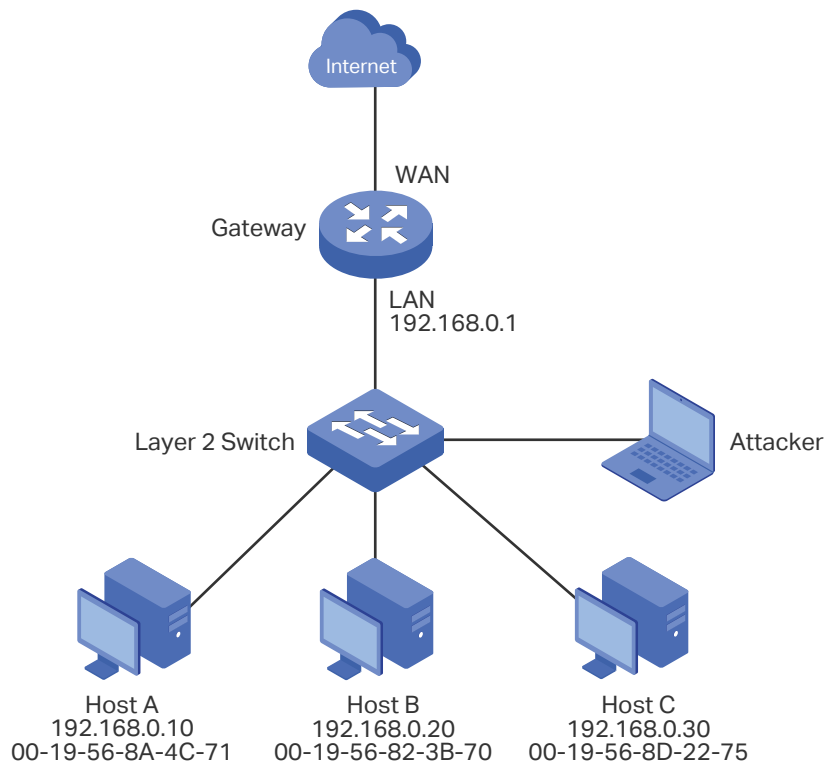
3 Configuration Examples

3.1 Example for Anti ARP Spoofing

3.1.1 Network Requirements

In the diagram below, several hosts are connected to the network via a layer 2 switch, and the gateway is the gateway of this network. Since there exists the possibility that the attacker will launch a series of ARP attacks, it is required to configure the gateway to protect itself and the terminal hosts from the ARP attacks.

Figure 3-1 Network Topology



3.1.2 Configuration Scheme

The attacker can launch three types of ARP attacks: cheating gateway, imitating gateway and cheating terminal hosts. The following section introduces the three ARP attacks and the corresponding solutions.

- Cheating Gateway

Cheating gateway attack is aimed at the gateway.

The attacker pretends to be legal terminal hosts and sends fake ARP packets to the gateway, cheating the gateway into recording wrong ARP maps of the hosts. As a result, packets from the gateway cannot be correctly sent to the hosts. To protect the gateway from this kind of attack, you can configure Anti ARP Spoofing on the gateway.

■ Imitating Gateway and Cheating Hosts

These two attacks are aimed at the terminal hosts.

Imitating Gateway means that the attacker imitates the gateway and sends fake ARP packets to the hosts. As a result, the hosts record wrong ARP map of the gateway and cannot send packets to the gateway correctly.

Cheating Hosts means that the attacker pretends to be a legal host and sends fake ARP packets to other hosts. As a result, the cheated hosts record an incorrect ARP map of the legal host and cannot send packets to legal host correctly.

To protect the hosts from the attacks above, it is recommend to take both of the precautions below.

- » Configure the firewall feature on the hosts.
- » Configure the gateway to send GARP packets to the hosts when the gateway detects ARP attacks. The GARP packets will inform the hosts of the correct ARP maps, and the wrong ARP maps in the hosts will be replaced by the correct ones.

In conclusion, to protect the network from ARP attacks, we should make sure both the gateway and the hosts are configured with the relevant ARP defense features. Here we introduce how to configure Anti ARP Spoofing on the gateway. There are mainly three steps:

- 1) Get the IP and MAC addresses of the legal hosts and bind them to the IP-MAC Binding list.
- 2) Enable Anti ARP Spoofing.
- 3) Configure the gateway to send GARP packets when ARP attacks are detected.

3.1.3 Configuration Procedure

Follow the steps below to configure Anti ARP Spoofing on the gateway:

- 1) Choose the menu **Firewall > Anti ARP Spoofing > IP-MAC Binding** to load the following page. In the **IP-MAC Binding List** section, click **Add**.

Figure 3-2 Anti ARP Spoofing Page

General

Enable ARP Spoofing Defense

Permit the packets matching the IP-MAC Binding entries only

Send GARP packets when ARP attack is detected

Interval: ms

IP-MAC Binding List

<input type="checkbox"/>	ID	IP Address	MAC Address	Interface	Description	Status	Operation
--	--	--	--	--	--	--	--

- The following page will appear. Enter the IP address and MAC address of Host A, give a description "Host A" for this entry. Keep **Status** of this entry as "Enable". Click **OK**.

Figure 3-3 Add IP-MAC Binding Entry

IP-MAC Binding List

<input type="checkbox"/>	ID	IP Address	MAC Address	Interface	Description	Status	Operation
--	--	--	--	--	--	--	--

IP Address:

MAC Address:

Description: (Optional, 0-50 characters)

Status: Enable

- Add the IP-MAC Binding entries for Host B and Host C as introduced above, and verify your configurations.

Figure 3-4 Verify IP-MAC Binding Entries

IP-MAC Binding List

<input type="checkbox"/>	ID	IP Address	MAC Address	Interface	Description	Status	Operation
<input type="checkbox"/>	1	192.168.0.10	00-19-56-8A-4C-71	LAN	Host A	Enabled <input style="border: 1px solid red; border-radius: 50%; padding: 2px 5px;" type="button" value="✖"/>	<input style="border: 1px solid red; border-radius: 50%; padding: 2px 5px;" type="button" value="📄"/> <input style="border: 1px solid red; border-radius: 50%; padding: 2px 5px;" type="button" value="🗑️"/>
<input type="checkbox"/>	2	192.168.0.20	00-19-56-82-3B-70	LAN	Host B	Enabled <input type="button" value="✖"/>	<input type="button" value="📄"/> <input type="button" value="🗑️"/>
<input type="checkbox"/>	3	192.168.0.30	00-19-56-8D-22-75	LAN	Host C	Enabled <input type="button" value="✖"/>	<input type="button" value="📄"/> <input type="button" value="🗑️"/>

- In the **General** section on the same page, check the boxes to enable **ARP Spoofing Defense** and **Send GARP packets when ARP attack is detected**, and keep the interval as 1000 milliseconds. Click **Save**.

Figure 3-5 Configure Anti ARP Spoofing

General

Enable ARP Spoofing Defense

Permit the packets matching the IP-MAC Binding entries only

Send GARP packets when ARP attack is detected

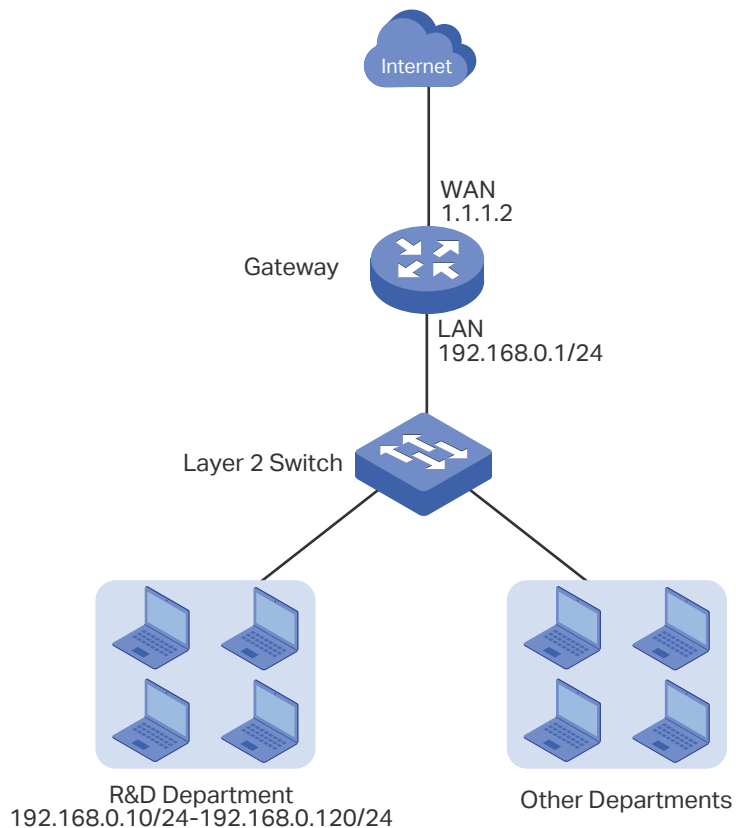
Interval: ms

3.2 Example for Access Control

3.2.1 Network Requirements

In the diagram below, the R&D and some other departments are connected to a layer 2 switch and access the internet via the gateway. To limit the acts of the R&D department users, such as sending emails with the exterior mailbox, it is required that the R&D users can only visit websites via HTTP and HTTPs on the internet at any time. For other departments, there is no limitation.

Figure 3-1 Network Topology



3.2.2 Configuration Scheme

To meet these requirements, we can configure Access Control rules on the gateway to filter the specific types of packets from R&D department: only the HTTP and HTTPs packets are allowed to be sent to the internet, and other types of packets are not allowed. The configuration overview is as follows:

- 1) Add an IP group for the R&D department in the **Preferences** module.
- 2) By default, the HTTP service type already exists, and you need to add HTTPs to the Service Type list in the **Preferences** module.
- 3) Create two rules to allow the HTTP and HTTPs packets from the R&D department to be sent to the WAN.
- 4) Since visiting the internet needs DNS service, add a rule to allow the DNS packets to be sent to the WAN. DNS service is already in the Service Type list by default.
- 5) Create a rule to block all packets from the R&D department to the WAN. This rule should have the lowest priority among all the rules.

3.2.3 Configuration Procedure

Follow the steps below to complete the configuration:

- 1) Choose the menu **Preferences > IP Group > IP Address** to load the configuration page, and click **Add**. Specify a name RD, select **IP Address Range** and enter the IP address range of the R&D department. Click **OK**.

Figure 3-2 Configure IP Address Range

The screenshot shows the 'IP Address List' configuration page. At the top right, there are '+ Add' and '- Delete' buttons. Below is a table with the following columns: ID, Name, IP Address Type, IP Address Range, IP Address/Mask, Description, and Operation. The table is currently empty. Below the table, there is a form for adding a new IP address range. The form fields are: Name (RD), IP Address Type (IP Address Range selected), IP Address Range (192.168.0.10 - 192.168.0.120), and Description (Optional). The Add and OK buttons are highlighted with red boxes.

- 2) Choose the menu **Preferences > IP Group > IP Group** to load the configuration page, and click **Add**. Specify a group name "RD_Dept", select the preset address range "RD" and click **OK**.

Figure 3-3 Configure IP Group

ID	Group Name	Address Name	Description	Operation
--	--	--	--	--

Group Name:

Address Name:

Description: (Optional)

- 3) Choose the menu **Preferences > Service Type > Service Type** to load the configuration page, and click **Add**. Specify the service type name as "HTTPS", select the protocol as "TCP", specify the source port range as "0-65535" and destination port range as "443-443", and click **OK**.

Figure 3-4 Configure HTTPS Service Type

ID	Service Type Name	Protocol	Detail	Description	Operation
--	--	--	--	--	--

Service Type Name:

Protocol: TCP UDP TCP/UDP ICMP Other

Source Port Range: -

Destination Port Range: -

Description: (Optional)

- 4) Choose the menu **Firewall > Access Control > Access Control** to load the configuration page, and click **Add**. Specify a name for this rule. Select "Allow" as the rule policy, "HTTP" as the service type, "LAN -> WAN" as the effective traffic direction, "RD_Dept" as the source IP group, "IPGROUP_ANY" as the destination IP group, and "Any" as the effective time. Click **OK**.

This rule means that all the HTTP packets from the R&D department are allowed to be transmitted from LAN to the internet at any time.

Figure 3-5 Configure Allow Rule for HTTP Service

Access Control List

+ Add - Delete

<input type="checkbox"/>	ID	Name	Source	Destination	Policy	Service Type	Interface	Effective Time	Operation
--	--	--	--	--	--	--	--	--	--

Name: (1-50 characters)

Policy:

Service Type:

Interface:

Source:

Destination:

Effective Time:

ID: (Optional)

- Choose the menu **Firewall > Access Control > Access Control** to load the configuration page, and click **Add**. Specify a name for this rule. Select "Allow" as the rule policy, "HTTPS" as the service type, "LAN -> WAN" as the effective traffic direction, "RD_Dept" as the source IP group, "IPGROUP_ANY" as the destination IP group, and "Any" as the effective time. Click **OK**.

This rule means that all the HTTPS packets from the R&D department are allowed to be sent from the LAN to the internet at any time.

Figure 3-6 Configure Allow Rule for HTTPS Service

Access Control List

+ Add - Delete

<input type="checkbox"/>	ID	Name	Source	Destination	Policy	Service Type	Interface	Effective Time	Operation
--	--	--	--	--	--	--	--	--	--

Name: (1-50 characters)

Policy:

Service Type:

Interface:

Source:

Destination:

Effective Time:

ID: (Optional)

- Choose the menu **Firewall > Access Control > Access Control** to load the configuration page, and click **Add**. Specify a name for this rule. Select "Allow" as the rule policy, "DNS" as the service type, "LAN -> WAN" as the effective traffic direction, "RD_

Dept" as the source IP group, "IPGROUP_ANY" as the destination IP group, and "Any" as the effective time. Click **OK**.

This rule means that all DNS packets from the R&D department are allowed to be sent from the LAN to the internet at any time.









The screenshot shows the 'Access Control List' configuration window. At the top right, there are '+ Add' and '- Delete' buttons. Below is a table with columns: ID, Name, Source, Destination, Policy, Service Type, Interface, Effective Time, and Operation. The table is currently empty. Below the table, the configuration fields are: Name: Allow_DNS (1-50 characters), Policy: Allow, Service Type: DNS, Interface: LAN, Source: RD_Dept, Destination: IPGROUP_ANY, Effective Time: Any, and ID: (Optional). At the bottom left, there are 'OK' and 'Cancel' buttons.

- 7) Choose the menu **Firewall > Access Control > Access Control** to load the configuration page, and click **Add**. Specify a name for this rule. Select "Block" as the rule policy, "ALL" as the service type, "LAN -> WAN" as the effective traffic direction, "RD_Dept" as the source IP group, "IPGROUP_ANY" as the destination IP group, and "Any" as the effective time. Click **OK**.

This rule means that all packets from the R&D department are blocked from being sent from the LAN to the internet at all times.

The screenshot shows the 'Access Control List' configuration window. At the top right, there are '+ Add' and '- Delete' buttons. Below is a table with columns: ID, Name, Source, Destination, Policy, Service Type, Interface, Effective Time, and Operation. The table is currently empty. Below the table, the configuration fields are: Name: Block_All (1-50 characters), Policy: Block, Service Type: ALL, Interface: LAN, Source: RD_Dept, Destination: IPGROUP_ANY, Effective Time: Any, and ID: (Optional). At the bottom left, there are 'OK' and 'Cancel' buttons.

- 8) Verify your configuration result. In the Access Control List, the rule with a smaller ID has a higher priority. Since the gateway matches the rules beginning with the highest priority, make sure the three Allow rules have the smaller ID numbers compared with the Block rule. In this way, the gateway checks whether the received packet matches the three Allow rules first, and only packets that do not match any of the Allow rules will be blocked.

Access Control List									
<input type="checkbox"/>	ID	Name	Source	Destination	Policy	Service Type	Interface	Effective Time	Operation
<input type="checkbox"/>	1	Allow_HTTP	RD_Dept	IPGROUP_ANY	Allow	HTTP	LAN	Any	 
<input type="checkbox"/>	2	Allow_HTTPS	RD_Dept	IPGROUP_ANY	Allow	HTTPS	LAN	Any	 
<input type="checkbox"/>	3	Allow_DNS	RD_Dept	IPGROUP_ANY	Allow	DNS	LAN	Any	 
<input type="checkbox"/>	4	Block_All	RD_Dept	IPGROUP_ANY	Block	ALL	LAN	Any	 

Part 9

Configuring Behavior Control

CHAPTERS

1. Behavior Control
2. Behavior Control Configuration
3. Configuration Examples

1 Behavior Control

1.1 Overview

With the Behavior Control feature, you can control the online behavior of local hosts. You can block specific hosts' access to specific websites using URLs or keywords, block HTTP posts and prevent certain types of files from being downloaded from the internet.

1.2 Supported Features

The Behavior Control module supports two features: Web Filtering and Web Security.

Web Filtering

Web Filtering is used to filter specific websites. The gateway provides two ways to filter websites: Web Group Filtering and URL Filtering.

- **Web Group Filtering:** You can configure multiple websites as a web group, and set a filtering rule for the group. More than one group can be created and several groups can share a same filtering rule.
- **URL Filtering:** You can directly set a filtering rule for specific entire URLs or keywords.

Web Security

Web Security is used to control the specific online behaviors of local users. You can configure this feature to block HTTP post, which means that the local users cannot log in, submit comments or perform any other operation which needs HTTP post. Also, you can prohibit local users from downloading specific types of files from the internet.

2 Behavior Control Configuration

In Behavior Control module, you can configure the following features:

- Web Filtering
- Web Security

2.1 Configuring Web Filtering

There are two methods to filter websites: Web Group Filtering and URL Filtering.

2.1.1 Configure Web Group Filtering

To configure Web Group Filtering, add one or more web groups first, and then add web group filtering entries using the created groups.

Add Web Groups

Choose the menu **Behavior Control > Web Filtering > Web Group** and click **Add** to load the following page.

Figure 2-1 Web Group Page

Web Group List
+ Add - Delete

<input type="checkbox"/>	ID	Name	Member	Description	Operation
--	--	--	--	--	--

Name: (1-28 characters)

Member:

(Use the Enter key, Space key, "," or ";" to divide different websites.)

File Path: (Optional. TXT file is required.)

Import web list file.

Description: (Optional)

Configure the following parameters and click **OK**.

Name	Specify a name for the group. The name of each group cannot be repeated.
Member	Add one or more website members to the group. The format of the website members is "www.tp-link.com" or "*.tp-link.com", in which "*" is a wildcard. Use Enter key, Space key, "," or ";" to divide different websites.
File Path	Import member list in your TXT file from your host. The format is "www.tp-link.com" or "*.tp-link.com", in which "*" is a wildcard. Use Enter key, Space key, "," or ";" to divide different websites.
Description	Enter a brief description for the group.

Add Web Group Filtering Entries

Before configuring web group entries, go to the **Preferences** module to configure the IP Group and Effective Time according to your needs.

Choose the menu **Behavior Control > Web Filtering > Web Group Filtering** and click **Add** to load the following page.

Figure 2-2 Web Group Filtering Page

General

Enable Web Filtering

Web Filtering List

<input type="checkbox"/>	ID	IP Group	Policy	Web Group	Effective Time	Status	Description	Operation
<input type="checkbox"/>	--	--	--	--	--	--	--	--

IP Group:

Policy: Whitelist Blacklist

Web Group:

Effective Time:

Description: (Optional)

ID: (Optional)

Status: Enable

Follow the steps below to add Web group filtering entries:

- 1) In the **Web Filtering List** section, configure the required parameters and click **OK**.

IP Group	Select an IP group for the rule. The IP group referenced here can be created on the Preferences > IP Group page.
-----------------	--

Policy	Choose to allow or deny the websites that are in the selected web group(s).
Web Group	Select one or more web groups. The web group referenced here can be created on the Behavior Control > Web Filtering > Web Group page.
Effective Time	Select the effective time. The effective time referenced here can be created on the Preferences > Time Range page.
Description	Enter a brief description for the group.
ID	Specify a rule ID. A smaller ID means a higher priority. This value is optional. A newly added rule with this field left blank will get the largest ID among all rules, which means that the newly added rule has the lowest priority.
Status	Check the box to enable the rule.

- 2) In the **General** section, enable Web Filtering. Click **Save**.

2.1.2 Configuring URL Filtering

Before configuring URL Filtering, go to the **Preferences** module to configure the IP Group and Effective Time according to your needs.

Choose the menu **Behavior Control > Web Filtering > URL Filtering** and click **Add** to load the following page.

Figure 2-3 URL Filtering Page

Follow the steps below to configure URL filtering:

- 1) In the URL Filtering List section, click **Add** and configure the required parameters. Click **OK**.

IP Group	Select an IP group for the rule. The IP group referenced here can be created on the Preferences > IP Group page.
Policy	Choose to allow or deny the websites that match the filtering content.

Mode	<p>Select the filtering mode.</p> <p>Keywords: If a website address contains any of the keywords, the policy will be applied to this website.</p> <p>URL Path: If a website address is the same as any of the entire URLs, the policy will be applied to this website.</p>
Filtering Content	<p>Add filtering contents. Use the Enter key, Space key, "," or ";" to divide different filtering contents.</p> <p> "." means that this rule will be applied to any website. For example, if you want to allow website A and deny other websites, you can add an Allow rule with the filtering content "A" and add a Deny rule with the filtering content ".". Note that "." rule should have the largest ID number, which means that it has the lowest priority.</p>
Effective Time	<p>Select the effective time. The effective time referenced here can be created on the Preferences > Time Range page.</p>
Status	<p>Check the box to enable the rule.</p>
Description	<p>Enter a brief description for the group.</p>
ID	<p>Specify a rule ID. A smaller ID means a higher priority. This value is optional. The newly added rule without this value configured will get the largest ID among all rules, which means that the newly added rule has the lowest priority.</p>

- 2) In the **General** section, enable URL filtering. Click **Save**.

2.2 Configuring Web Security

Before configuring Web Security, go to **Preferences** module to configure the IP Group and Effective Time according to your needs.

Choose the menu **Behavior Control > Web Security > Web Security** and click **Add** to load the following page.

Figure 2-4 Web Security Page

The screenshot displays the 'Web Security' configuration interface. At the top, under the 'General' tab, there is a checkbox for 'Enable Web Security' and a 'Save' button. Below this is the 'Web Security List' section, which contains a table with the following columns: ID, IP Group, File Suffix, Effective Time, Description, Status, and Operation. The table currently shows a single row with dashes in each cell. To the right of the table are '+ Add' and '- Delete' buttons. Below the table is a form for adding a new rule. The form includes:

- IP Group:** A dropdown menu currently showing '---'.
- Block HTTP Post:** A checkbox labeled 'Enable'.
- File Suffix:** A large text area for entering file suffixes. A note next to it says: '(Use Enter key, Space key, "," or ";" to divide different file suffixes.)'
- Effective Time:** A dropdown menu currently showing 'Any'.
- Description:** A text input field with '(Optional)' next to it.
- Status:** A checkbox labeled 'Enable' which is currently checked.

 At the bottom of the form are 'OK' and 'Cancel' buttons.

Follow the steps below to configure Web Security.

- 1) In the **Web Security List** section, configure the following parameters and click **OK** to add a Web Security rule.

IP Group	Select an IP group for the rule. The IP group referenced here can be created on the Preferences > IP Group page.
Block HTTP Post	With this option enabled, HTTP posts will be blocked. The hosts of the selected IP group cannot log in, submit comments or do any operation using HTTP post.

File Suffix	Enter file suffixes to specify the file types. Use Enter key, Space key, "," or ";" to divide different file suffixes. The hosts of the selected IP group cannot download these types of files from the internet.
Effective Time	Select the effective time. The effective time referenced here can be created on the Preferences > Time Range page.
Description	Enter a brief description for the group.
Status	Check the box to enable the rule.

- 2) In the **General** section, enable Web Security and click **Save**.

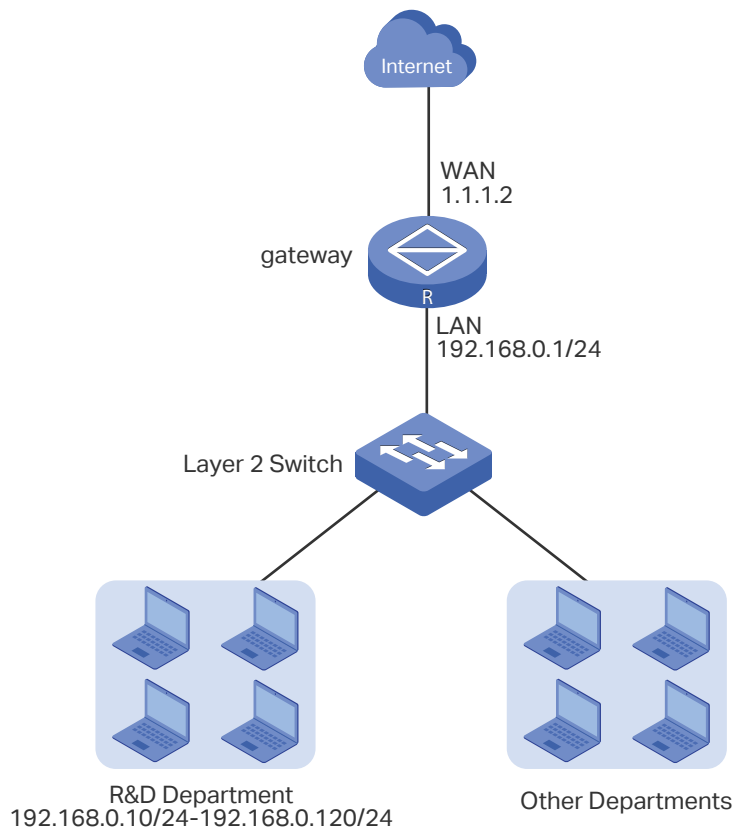
3 Configuration Examples

3.1 Example for Access Control

3.1.1 Network Requirements

In the diagram below, the R&D and some other departments are connected to a layer 2 switch and access the internet via the gateway. For data security purposes, it is required that the R&D department users can only visit the official website of the company, for example: <https://www.tp-link.com>. For other departments, there is no limitation of website access.

Figure 3-1 Network Topology



3.1.2 Configuration Scheme

We can configure Web Filtering to limit the website access of the specific hosts. Both Web Group Filtering and URL Filtering can achieve this. In this example, the configuration difference between Web Group Filtering and URL Filtering is as follows:

- In Web Group Filtering, you need to add the official website address to a web group before configuring the filtering rule.
- In URL Filtering, you can directly specify the official website address in the filtering rule.

Here we take Web Group Filtering as an example. The configuration overview is as follows:

- 1) Add an IP group for the R&D department in the **Preferences** module.
- 2) Create a web group with the group member www.tp-link.com.
- 3) Add a Whitelist rule to allow the R&D department users to access www.tp-link.com.
- 4) Add a Blacklist rule to forbid the R&D department users from accessing all websites. Note that the priority of this rule should be lower than the Whitelist rule.

3.1.3 Configuration Procedure

Follow the steps below to complete the configuration:

- 1) Choose the menu **Preferences > IP Group > IP Address** to load the configuration page, and click **Add**. Specify a name "RD", select **IP Address Range** and enter the IP address range of the R&D department. Click **OK**.

Figure 3-2 Configure IP Address Range

IP Address List

+ Add - Delete

<input type="checkbox"/>	ID	Name	IP Address Type	IP Address Range	IP Address/Mask	Description	Operation
--	--	--	--	--	--	--	--

Name:

IP Address Type: IP Address Range IP Address/Mask

-

Description: (Optional)

- 2) Choose the menu **Preferences > IP Group > IP Group** to load the configuration page, and click **Add**. Specify a group name "RD_Dept", select the preset address range "RD" and click **OK**.

Figure 3-3 Configure IP Group

Group List

+ Add - Delete

<input type="checkbox"/>	ID	Group Name	Address Name	Description	Operation
--	--	--	--	--	--

Group Name:

Address Name:

Description: (Optional)

- 3) Choose the menu **Behavior Control > Web Filtering > Web Group** to load the configuration page, and click **Add**. Specify a name "RD_Filtering" for this web group and add the member "www.tp-link.com". Click **OK**.

Figure 3-4 Configure Web Group

Web Group List

+ Add - Delete

<input type="checkbox"/>	ID	Name	Member	Description	Operation
--	--	--	--	--	--

Name: (1-28 characters)

Member:

(Use the Enter key, Space key, "," or ";" to divide different websites.)

File Path: (Optional. TXT file is required.)

Import web list file.

Description: (Optional)

- 4) Choose the menu **Behavior Control > Web Filtering > Web Group Filtering** to load the configuration page, and click **Add**. Select "RD_Dept" as the **IP Group**, "Whitelist" as the **Policy**, "RD_Filtering" as the **Web Group**, and "Any" as the **Effective Time**. Click **OK**.

This rule means that the hosts in the R&D department are allowed to access the website www.tp-link.com at any time.

Figure 3-5 Configure Whitelist Rule

The screenshot shows the 'Web Filtering List' configuration interface. At the top right, there are '+ Add' and '- Delete' buttons. Below is a table with columns: ID, IP Group, Policy, Web Group, Effective Time, Status, Description, and Operation. The table is currently empty. Below the table is a configuration form for a new rule. The form fields are: IP Group (RD_Dept), Policy (Whitelist selected, Blacklist unselected), Web Group (RD_Filtering), Effective Time (Any), Description (Optional), ID (Optional), and Status (checked Enable). The 'OK' button is highlighted with a red box.

- 5) On the same page, click **Add**. Select "RD_Dept" as the **IP Group**, "Blacklist" as the **Policy**, "All" as the **Web Group**, and "Any" as the **Effective Time**. Click **OK**.

This rule means that the hosts in the R&D department are denied access to all websites at all times.

Figure 3-6 Configure Blacklist Rule

The screenshot shows the 'Web Filtering List' configuration interface. At the top right, there are '+ Add' and '- Delete' buttons. Below is a table with columns: ID, IP Group, Policy, Web Group, Effective Time, Status, Description, and Operation. The table is currently empty. Below the table is a configuration form for a new rule. The form fields are: IP Group (RD_Dept), Policy (Blacklist selected, Whitelist unselected), Web Group (All), Effective Time (Any), Description (Optional), ID (Optional), and Status (checked Enable). The 'OK' button is highlighted with a red box.

- 6) On the same page, verify your configurations. In the Web Filtering List, the rule with a smaller ID has a higher priority. Since the gateway matches the rules beginning with the highest priority, make sure the Whitelist rule has the smaller ID number. In this way, the gateway allows the hosts to access the Whitelist website and denies them to access others.

Figure 3-7 Verify Configuration Result

Web Filtering List								
+ Add - Delete								
<input type="checkbox"/>	ID	IP Group	Policy	Web Group	Effective Time	Status	Description	Operation
<input type="checkbox"/>	1	RD_Dept	Whitelist	RD_Filtering	Any	Enabled ✘	---	
<input type="checkbox"/>	2	RD_Dept	Blacklist	All	Any	Enabled ✘	---	

7) In the **General** section on the same page, enable Web Filtering globally and click **Save**.

Figure 3-8 Enable Web Filtering

General

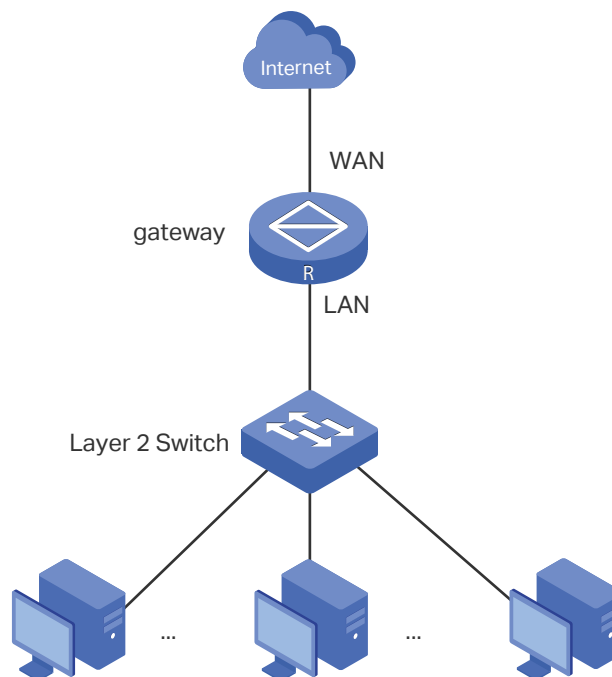
Enable Web Filtering

3.2 Example for Web Security

3.2.1 Network Requirements

In the diagram below, the company’s hosts are connected to a layer 2 switch and access the internet via the gateway. For security reasons, it is required that the users in the LAN cannot log in, submit comments or download rar files on the internet.

Figure 3-9 Network Topology



3.2.2 Configuration Scheme

We can configure Web Security to meet these requirements. To block behaviors such as login and comment submitting, we can configure the gateway to block HTTP post; to block downloading of rar files, we can specify the suffix "rar" in the file suffix column.

3.2.3 Configuration Procedure

Follow the steps below to complete the configuration:

- 1) Choose the menu **Behavior Control > Web Security > Web Security** and click **Add** to load the following page. Select "IPGROUP_LAN" as the **IP Group**, enable **Block HTTP Post**, enter "rar" in the **File Suffix** field, select "Any" as the **Effective Time**, and keep the **Status** as "Enable". Click **OK**.

Figure 3-10 Configure Web Security Entry

Web Security List

+ Add - Delete

<input type="checkbox"/>	ID	IP Group	File Suffix	Effective Time	Description	Status	Operation
--	--	--	--	--	--	--	--

IP Group: IPGROUP_LAN

Block HTTP Post: Enable

File Suffix: rar (Use Enter key, Space key, "," or ";" to divide different file suffixes.)

Effective Time: Any

Description: (Optional)

Status: Enable

OK Cancel

- 2) In the **General** section on the same page, enable **Web Security** and click **Save**.

Figure 3-11 Enable Web Security

General

Enable Web Security

Save

Part 10

Configuring VPN

CHAPTERS

1. VPN
2. IPSec VPN Configuration
3. GRE VPN Configuration
4. L2TP Configuration
5. PPTP Configuration
6. OpenVPN Configuration
7. WireGuard VPN Configuration
8. Users Configuration

1 VPN

1.1 Overview

VPN (Virtual Private Network) provides a means for secure communication between remote computers across a public WAN (Wide Area Network), such as the internet. Virtual indicates the VPN connection is based on the logical end-to-end connection instead of the physical end-to-end connection. Private indicates users can establish the VPN connection according to their requirements and only specific users are allowed to use the VPN connection.

The core of VPN is to realize tunnel communication, which fulfills the task of data encapsulation, data transmission and data decompression via the tunneling protocol. Common tunneling protocols are Layer 2 tunneling protocol and Layer 3 tunneling protocol.

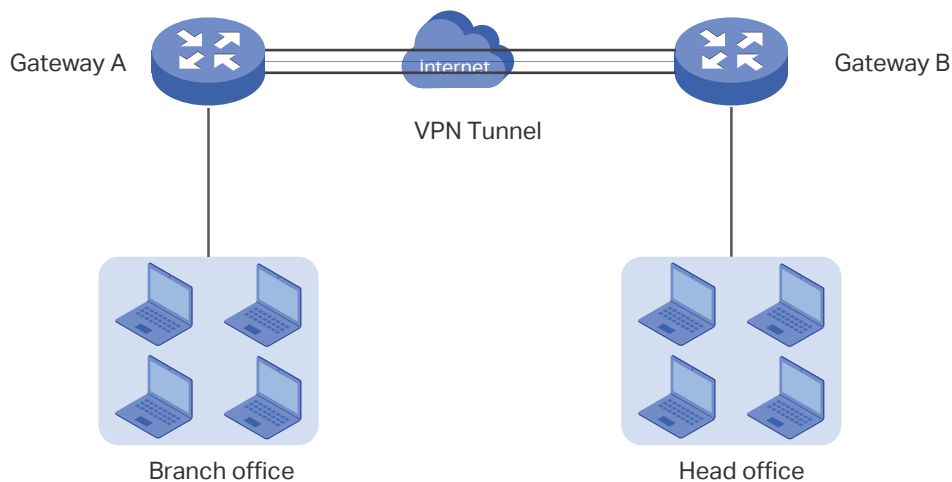
Depending on your network topology, there are two basic application scenarios: LAN-to-LAN VPN and Client-to-LAN VPN.

Depending on your network topology, there are two basic application scenarios: LAN-to-LAN VPN and Client-to-LAN VPN.

■ LAN-to-LAN VPN

In this scenario, different private networks are connected together via the internet. For example, the private networks of the branch office and head office in a company are located at different places. LAN-to-LAN VPN can satisfy the demand that hosts in these private networks need to communicate with each other. The following figure shows the typical network topology in this scenario.

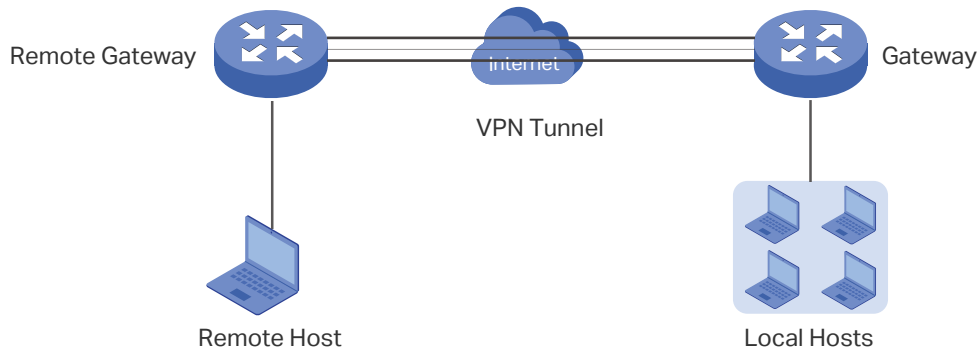
Figure 1-1 LAN-to-LAN VPN



■ Client-to-LAN VPN

In this scenario, the remote host is provided with secure access to the local hosts. For example, an employee on business can access the private network of his company securely. Client-to-LAN VPN can satisfy this demand. The following figure shows the typical network topology in this scenario.

Figure 1-2 Client-to-LAN VPN



1.2 Supported Features

The gateway supports IPsec, L2TP, PPTP and OpenVPN.

IPsec

IPsec (IP Security) can provide security services such as data confidentiality, data integrity and data origin authentication at the IP layer. IPsec uses IKEv1 (Internet Key Exchange version 1) and IKEv2 (Internet Key Exchange version 2) to handle negotiation of protocols and algorithms based on the user-specified policy, and generate the encryption and authentication keys to be used by IPsec. IKEv1/IKEv2 negotiation includes two phases, that is IKEv1/IKEv2 Phase-1 and IKEv1/IKEv2 Phase-2. The basic concepts of IPsec are as follows:

■ Proposal

Proposal is the security suite configured manually to be applied in IPsec IKEv1 negotiation. Specifically speaking, it refers to hash algorithm, symmetric encryption algorithm, asymmetric encryption algorithm applied in IKEv1 Phase-1, and security protocol, hash algorithm, symmetric encryption algorithm applied in IKEv1 Phase-2.

■ Negotiation Mode

The negotiation mode configured for IKEv1 Phase-1 negotiation determines the role that the VPN gateway plays in the negotiation process. You can specify the negotiation mode as responder mode or initiator mode.

Responder Mode: In responder mode, the VPN gateway responds to the requests for IKEv1 negotiation and acts as the VPN server or the responder.

Initiator Mode: In initiator mode, the VPN gateway sends requests for IKEv1 negotiation and acts as the VPN client or the initiator.

- Exchange Mode

The exchange mode determines the way VPN gateways negotiate in IKEv1 Phase-1. You can specify the exchange mode as main mode or aggressive mode.

Main Mode: In main mode, the identification information for authentication is encrypted, thus enhancing security.

Aggressive Mode: In aggressive mode, less packets are exchanged, thus improving speed.

- Authentication ID Type

The authentication ID type determines the type of authentication identifiers applied in IKEv1 Phase-1. It includes the local ID type and the remote ID type. The local ID indicates the authentication identifier sent to the other end, and the remote ID indicates that expected from the other end. You can specify the authentication ID type as IP address or name.

IP Address: The gateway uses the IP address for authentication.

Name: The gateway uses the FQDN (Fully Qualified Domain Name) for authentication.

- Encapsulation Mode

The encapsulation mode determines how packets transferred in the VPN tunnel are encapsulated. You can select tunnel mode or transport mode as the encapsulation mode. For most users, it is recommended to use the tunnel mode.

- PFS

PFS (Perfect Forward Secrecy) determines whether the key generated in IKEv1 Phase-2 is relevant with that in IKEv1 Phase-1. You can specify PFS as none, dh1, dh2, or dh5. None indicates that no PFS is configured, and the key generated in IKEv1 Phase-2 is relevant with that in IKEv1 Phase-1, whereas dh1, dh2, or dh5 means different key exchange groups, which make the key generated in IKEv1 Phase-2 irrelevant with that in IKEv1 Phase-1.

GRE

GRE VPN encapsulates data packets of some network layer protocols, so that they can be transmitted in another network protocol. But GRE cannot encrypt packets, so it is usually used together with IPsec.

L2TP

L2TP (Layer 2 Tunneling Protocol) provides a way for a dial-up user to make a virtual PPP (Point-to-Point Protocol) connection to a VPN server. Because of the lack of confidentiality

inherent in the L2TP protocol, it is often implemented along with IPsec. The basic concepts of L2TP are as follows:

- **IPsec Encryption**

IPsec encryption determines whether the traffic of the tunnel is encrypted with IPsec. You can select encrypted or unencrypted as the IPsec encryption. If encrypted is selected, a pre-shared key needs to be entered, and then the L2TP traffic will be encrypted with a default IPsec configuration. If unencrypted is selected, the VPN tunnel traffic will not be encrypted.

- **Authentication**

L2TP uses an account name and password for authentication on the VPN server. Only legal clients can set up a tunnel with the server, thus enhancing network security.

PPTP

PPTP (Point-to-Point Tunneling Protocol) is a network protocol that enables the secure transfer of data from a remote client to a private enterprise server by creating a VPN across TCP/IP-based data networks. PPTP supports on-demand, multi-protocol, virtual private networking over public networks, such as the internet. The basic concepts of PPTP are as follows:

- **MPPE Encryption**

MPPE (Microsoft Point-to-Point Encryption) scheme is a means of representing PPP packets in an encrypted form defined in RFC 3078. You can select encrypted or unencrypted as MPPE encryption. If encrypted is selected, the VPN tunnel traffic will be encrypted with RSA RC4 algorithm to ensure data confidentiality. If unencrypted is selected, the VPN tunnel traffic will not be encrypted.

- **Authenticaiton**

PPTP uses an account name and password for authentication on the VPN server. Only legal clients can set up a tunnel with the server, thus enhancing network security.

OpenVPN

OpenVPN uses OpenSSL (Open Secure Sockets Layer) for encryption of UDP and TCP for traffic transmission. OpenVPN uses a client-server connection to provide secure communications between a server and a remote client over the Internet.

WireGuard VPN

Wireguard VPN is a secure, fast and modern VPN protocol. It is based on the UDP protocol and uses modern encryption algorithms to improve work efficiency.

User Account List

This feature enables you to create VPN connection accounts for remote devices to connect to the VPN server. If the gateway acts as the L2TP/PPTP client, you don't need to configure the L2TP/ PPTP user accounts on this page.

2 IPSec VPN Configuration

To complete the IPSec VPN configuration, follow these steps:

- 1) Configure the IPSec Policy.
- 2) Verify the connectivity of the IPSec VPN tunnel.

Configuration Guidelines

- For both ends of the VPN tunnel, the Pre-shared key, Proposal, Exchange Mode, and Encapsulation Mode should be identical.
- For both ends of the VPN tunnel, the Remote Gateway, Local/Remote Subnet, Local/Remote ID Type should be matched.

2.1 Configuring the IPSec Policy

2.1.1 Configuring the Basic Parameters

Choose the menu **VPN > IPSec > IPSec Policy** and click **Add** to load the following page.

Figure 2-1 Configuring the Basic Parameters

<input type="checkbox"/>	ID	Policy Name	Mode	Remote Gateway	Local Subnet	Remote Subnet	Status	Operation
--	--	--	--	--	--	--	--	--

Policy Name: (1-32 characters)

Mode: LAN-to-LAN ▼

Remote Gateway: (IP Address/Domain Name)

WAN: --- ▼

Local Subnet: /

Remote Subnet: /

Pre-shared Key: (1-128 characters)

Status: Enable

⊖ Advanced Settings

Follow these steps to configure the basic parameters:

- 1) Specify the name of the IPSec Policy.

- 2) Configure the Network Mode. Select **LAN-to-LAN** when the network is connected to the other network. Select **Client-to-LAN** when a host is connected to the network.

When the **LAN-to-LAN** mode is selected, the following section will appear.

Mode:	LAN-to-LAN	
Remote Gateway:	<input type="text"/>	(IP Address/Domain Name)
WAN:	---	
Local Subnet:	<input type="text"/>	/ <input type="text"/>
Remote Subnet:	<input type="text"/>	/ <input type="text"/>
Pre-shared Key:	<input type="text"/>	(1-128 characters)
Status:	<input checked="" type="checkbox"/> Enable	

Remote Gateway Enter an IP address or a domain name (1 to 255 characters) as the remote gateway. 0.0.0.0 represents any IP address. Only when the negotiation mode is set to Responder Mode can you enter 0.0.0.0.

WAN Specify the WAN port on which the IPSec tunnel is established.

Local Subnet Specify the local network. (It's always the IP address range of LAN on the local side of the VPN tunnel.) It's formed from the IP address and subnet mask.

Remote Subnet Specify the remote network. (It's always the IP address range of LAN on the remote peer of the VPN tunnel.) It's formed from the IP address and subnet mask.

Pre-shared Key Specify the unique pre-shared key for both peers' authentication.

Status Choose to enable the IPSec policy.

Note:

The Local Subnet and Remote Subnet should not be in the same network segment when choosing LAN-to-LAN as the VPN mode.

When the **Client-to-LAN** mode is selected, the following section will appear.

Mode:	Client-to-LAN	
Remote Host:	<input type="text"/>	(IP Address/Domain Name)
WAN:	---	
Local Subnet:	<input type="text"/>	/ <input type="text"/>
Pre-shared Key:	<input type="text"/>	(1-128 characters)
Status:	<input checked="" type="checkbox"/> Enable	

Remote Host Enter the IP address of the remote host. 0.0.0.0 represents any IP address.

WAN Specify the WAN port on which the IPSec tunnel is established.

Local Subnet Specify the local network. (This is the IP address range of the LAN on the local side of the VPN tunnel.) It's formed from the IP address and subnet mask.

Pre-shared Key Specify the unique pre-shared key for both peers' authentication.

Status	Choose to enable the IPSec policy.
--------	------------------------------------

3) Click **OK**.

2.1.2 Configuring the Advanced Parameters

Advanced settings include IKEv1/IKEv2 phase-1 settings and IKEv1/IKEv2 phase-2 settings. Phase-1 is used to authenticate both sides of the communication and establish the IKE SA. Phase-2 is used to negotiate about keys and security related parameters, then establish the IPSec SA. It is suggested to keep the default advanced settings. You can complete the configurations according to your actual needs.

■ Configuring the IKE Phase-1 Parameters

Choose the menu **VPN > IPSec > IPSec Policy** and click **Advanced Settings** to load the following page.

Figure 2-2 Configuring the IKE Phase-1 Parameters

Phase-1 Settings

IKE Protocol Version: IKEv1 IKEv2

Proposal: sha1-aes256-dh2 ▼

Proposal: --- ▼

Proposal: --- ▼

Proposal: --- ▼

Exchange Mode: Main Mode Aggressive Mode

Negotiation Mode: Initiator Mode Responder Mode

Local ID Type: IP Address NAME

Local ID: (1-28 non-blank characters)

Remote ID Type: IP Address NAME

Remote ID: (1-28 non-blank characters)

SA Lifetime: 28800 seconds (60-604800)

DPD: Enable

DPD Interval: 10 seconds (1-300)

In the **Phase-1 Settings** section, configure the IKE phase-1 parameters and click **OK**.

Proposal	Select the proposal for IKE negotiation phase 1 to specify the encryption algorithm, authentication algorithm and DH group. Up to four proposals can be selected.
----------	---

Exchange Mode	<p>Specify the IKE Exchange Mode as Main Mode or Aggressive Mode. By default, it is Main Mode.</p> <p>Main Mode: Main mode provides identity protection and exchanges more information, which applies to scenarios with higher requirements for identity protection.</p> <p>Aggressive Mode: Aggressive Mode establishes a faster connection but with lower security, which applies to scenarios with lower requirements for identity protection.</p>
Negotiation Mode	<p>Specify the IKE Negotiation Mode as Initiator Mode or Responder Mode.</p> <p>Initiator Mode: The local device initiates a connection to the peer.</p> <p>Initiator Mode: The local device initiates a connection to the peer.</p>
Local ID Type	<p>Specify the local ID type for IKE negotiation.</p> <p>IP Address: Use an IP address as the ID in IKE negotiation. It is the default type.</p> <p>NAME: Use a name as the ID in IKE negotiation. It refers to FQDN (Fully Qualified Domain Name).</p>
Local ID	<p>When the Local ID Type is configured as NAME, enter a name for the local device as the ID in IKE negotiation.</p>
Remote ID Type	<p>Specify the remote ID type for IKE negotiation.</p> <p>IP Address: Use an IP address as the ID in IKE negotiation. It is the default type.</p> <p>NAME: Use a name as the ID in IKE negotiation. It refers to FQDN (Fully Qualified Domain Name).</p>
Remote ID	<p>When the Remote ID Type is configured as NAME, enter a name of the remote peer as the ID in IKE negotiation .</p>
SA Lifetime	<p>Specify ISAKMP SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related ISAKMP SA will be deleted.</p>
DPD	<p>Check the box to enable or disable DPD (Dead Peer Detect) function. If enabled, the IKE endpoint can send a DPD request to the peer to inspect whether the IKE peer is alive.</p>
DPD Interval	<p>If DPD is triggered, specify the interval between sending DPD requests. If the IKE endpoint receives a response from the peer during this interval, it considers the peer alive. If the IKE endpoint does not receive a response during the interval, it considers the peer dead and deletes the SA.</p>

■ Configuring the IKE Phase-2 Parameters

Choose the menu **VPN > IPSec > IPSec Policy** and click **Advanced Settings** to load the following page.

Figure 2-3 Configuring the IKE Phase-2 Parameters

In the **Phase-2 Settings** section, configure the IKE phase-2 parameters and click **OK**.

Encapsulation Mode	Specify the Encapsulation Mode as Tunnel Mode or Transport Mode. When both ends of the tunnel are hosts, either mode can be chosen. When at least one of the endpoints of a tunnel is a security gateway, tunnel mode is recommended to ensure safety.
Proposal	Select the proposal for IKE negotiation phase 2 to specify the encryption algorithm, authentication algorithm and protocol. Up to four proposals can be selected.
PFS	Select the DH group to enable PFS (Perfect Forward Security) for IKE mode, then the key generated in phase 2 will be irrelevant with the key in phase 1, which enhance the network security. If you select None, it means PFS is disabled and the key in phase 2 will be generated based on the key in phase 1.
SA Lifetime	Specify IPSec SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related IPSec SA will be deleted.

2.1.3 Configuring the Failover Group

You can two IPsec connections in a failover group. If the primary connection fails, the secondary connection in the group automatically takes over.

Choose the menu **VPN > IPSec > IPSec Policy**, add multiple connection in the **IPsec Policy List** section, and then in the **Failover Group** section, click **Add** to load the following page.

Figure 2-4 Configuring the Failover Group

+ Add
 - Delete

<input type="checkbox"/>	ID	Group Name	Primary IPsec	Secondary IPsec	Status	Operation
--	--	--	--	--	--	--

Group Name:

Primary IPsec:

Secondary IPsec:

Automatic Failback: Enable

Gateway failover time-out: seconds (10-3600)

Status: Enable

Follow these steps to configure the parameters, then click **OK**:

Group Name:	Give a name to identify the group.
Primary IPsec	Select a IP sec connection as the primary IPsec connection.
Secondary IPsec	Select a IP sec connection as the primary IPsec connection.
Automatic Failback	When enabled, the primary IPsec connection will be reused when it is restored,
Gateway failover time-out:	Set the time interval for the gateway to send a request to query the status of the primary IPsec connection.
Status:	Check the box to enable the group.

Note: The two IPsec connections are established to the same remote IP, and the related parameters should be the same.

2.2 Verifying the Connectivity of the IPSec VPN tunnel

Choose the menu **VPN > IPSec > IPSec SA** to load the following page.

Figure 2-5 IPSec SA List

IPSec SA List										
Entry Count: 2										Refresh
<input type="checkbox"/>	ID	Name	SPI	Direction	Tunnel ID	Data Flow	Protocol	AH Authentication	ESP Authentication	ESP Encryption
<input type="checkbox"/>	1	tplink	32474659 60	in	30.30.30.1<- -20.20.20.1	192.168.2.0/24 <- - 192.168.1.0/24	ESP	--	MD5	3DES
<input type="checkbox"/>	2	tplink	12359900 6	out	30.30.30.1-- >20.20.20.1	192.168.2.0/24 -- > 192.168.1.0/24	ESP	--	MD5	3DES

The **IPSec SA List** shows the information of the established IPSec VPN tunnel.

Name	Displays the name of the IPSec policy associated with the SA.
SPI	Displays the SPI (Security Parameter Index) of the SA, including outgoing SPI and incoming SPI. The SPI of each SA is unique.
Direction	Displays the direction (in: incoming/out: outgoing) of the SA.
Tunnel ID	Displays the IP addresses of the local and remote peers.
Data Flow	Displays the Local Subnet and Remote Subnet/host covered by the SA.
Protocol	Displays the authentication protocol and encryption protocol used by the SA.
AH Authentication	Displays the AH authentication algorithm used by the SA.
ESP Authentication	Displays the ESP authentication algorithm used by the SA.
ESP Encryption	Displays the ESP encryption algorithm used by the SA.

3 GRE VPN Configuration

To complete the GRE VPN configuration, make sure you have configured the IPsec VPN. Choose the menu **VPN > GRE** to load the following page. Click **Add** to add a GRE policy.

Figure 3-1 Configuring GRE Policy

The screenshot shows the 'GRE Policy List' configuration interface. At the top right, there are '+ Add' and '- Delete' buttons. Below is a table with the following columns: ID, Name, Wan, Remote Gateway, IPsec Encryption, Local Subnets, Remote Subnets, Status, and Operation. The table currently contains one row with dashes in all cells. Below the table is a configuration form with the following fields:

- Name: [Text input field]
- Wan: [Dropdown menu]
- Remote Gateway: [Text input field]
- IPsec Encryption: [Dropdown menu]
- Pre-shared Key: [Text input field] (1-128 characters)
- Local Subnets: [Text input field] / [Text input field]
- Remote Subnets: [Text input field] / [Text input field]
- Local GRE IP: [Text input field]
- Remote GRE IP: [Text input field]
- Status: Enable

At the bottom of the form are 'OK' and 'Cancel' buttons.

Name	Enter a name to identify the GRE VPN.
WAN	Specify the WAN port on which the GRE tunnel is established.
Remote Gateway	Enter an IP address as the remote gateway.
IPsec Encryption	Specify whether to enable the encryption for the tunnel. If enabled, the GRE tunnel will be encrypted by IPsec (GRE over IPsec).
Pre-shared Key	When the IPsec Encryption is configured as Encrypted, specify the Pre-shared Key for IKE authentication.
Local Subnet	Specify the local network. It's always the IP address range of LAN on the local side of the VPN tunnel. It's formed from the IP address and subnet mask. After the VPN tunnel is established, the peer can access the local subnet.
Remote Subnet	Specify the remote network. It's always the IP address range of LAN on the remote peer of the VPN tunnel. It's formed from the IP address and subnet mask. Only the traffic to the remote subnet will be forwarded through the VPN tunnel.

Local GRE IP	Specify the local virtual IP address for the GRE VPN. The IP should not be the same as the Remote Gateway IP, nor should it be in Local Subnet or Remote Subnet.
Remote GRE IP	Specify the remote virtual IP address for the GRE VPN. The IP should not be the same as the Remote Gateway IP, nor should it be in Local Subnet or Remote Subnet.
Status	Check the box to enable the GRE VPN.

4 L2TP Configuration

To complete the L2TP configuration, follow these steps:

- 1) Configure the VPN IP pool.
- 2) Configure L2TP globally.
- 3) Configure the L2TP server/client.
- 4) (Optional) Configure the L2TP users.
- 5) Verify the connectivity of the L2TP VPN tunnel.

Configuration Guidelines

- When the network mode is configured as Client-to-LAN and the gateway acts as the L2TP server, you don't need to configure the L2TP client on the gateway.
- When the network mode is configured as LAN-to-LAN and the gateway acts as the L2TP client gateway, you don't need to configure the L2TP users on the gateway.

4.1 Configuring the VPN IP Pool

Choose the menu **Preferences > VPN IP Pool > VPN IP Pool** and click **Add** to load the following page.

Figure 4-1 Configuring the VPN IP Pool

IP Pool List + Add - Delete

<input type="checkbox"/>	ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
--	--	--	--	--	--

IP Pool Name:

Starting IP Address:

Ending IP Address:

Follow these steps to configure the VPN IP Pool:

- 1) Specify the name of the IP Pool.
- 2) Specify the starting IP address and ending IP address for the IP Pool.

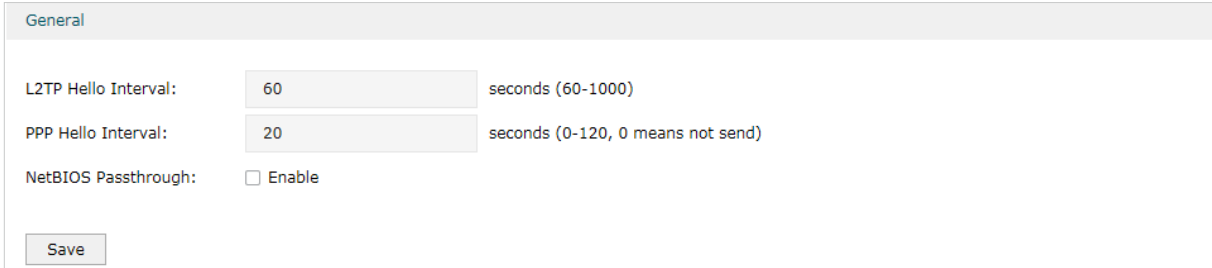
 **Note:**

- The starting IP address should not be greater than the ending IP address.
- The ranges of IP Pools cannot overlap.

4.2 Configuring L2TP Globally

Choose the menu **VPN > L2TP > Global Config** to load the following page.

Figure 4-2 Configuring L2TP Globally



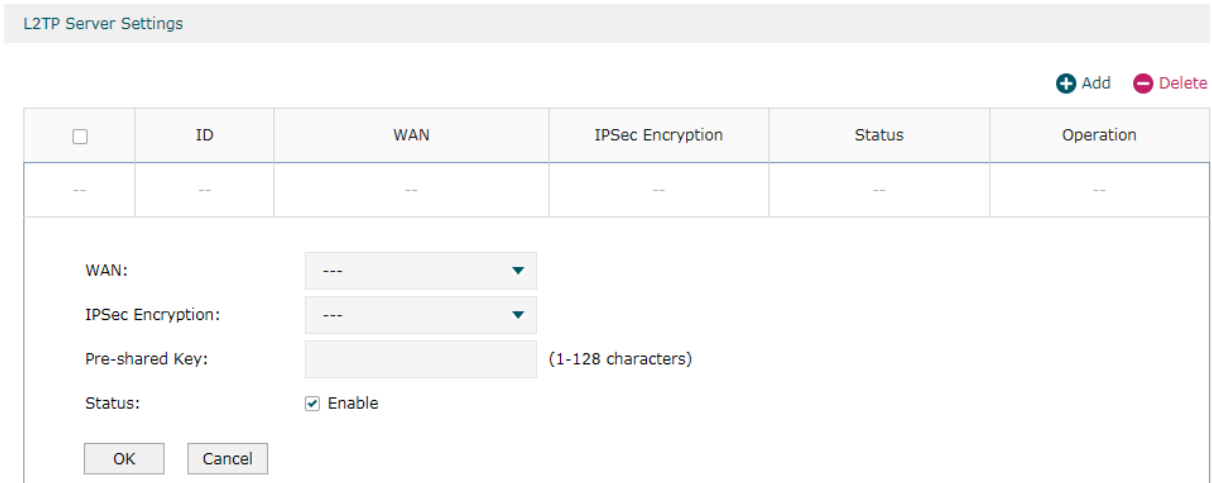
In the **General** section, configure L2TP parameters globally and click **Save**.

L2TP Hello Interval	Specify the time interval of sending L2TP peer detect packets.
PPP Hello Interval	Specify the time interval of sending PPP peer detect packets.
NetBIOS Passthrough	Enable NetBIOS Passthrough function to allow NetBIOS packets to be broadcasted through VPN tunnel.

4.3 Configuring the L2TP Server

Choose the menu **VPN > L2TP > L2TP Server** and click **Add** to load the following page.

Figure 4-3 Configuring the L2TP Server



Follow these steps to configure the L2TP server:

- 1) Specify the WAN port used for L2TP tunnel.
- 2) Specify whether to enable the encryption for the tunnel.

IPSec Encryption

Specify whether to enable the encryption for the tunnel. If enabled, the L2TP tunnel will be encrypted by IPSec (L2TP over IPSec). If you choose Auto, the L2TP server will determine whether to encrypt the tunnel according to the client 's encryption settings.

- 3) Specify the Pre-shared Key for IKE authentication.
- 4) Enable the L2TP tunnel.
- 5) Click **OK**.

4.4 Configuring the L2TP Client

Choose the menu **VPN > L2TP > L2TP Client** and click **Add** to load the following page.

Figure 4-4 Configuring the L2TP Client

<input type="checkbox"/>	ID	Tunnel	Account Name	WAN	Server IP	IPSec Encryption	Remote Subnet	Working Mode	Status	Operation
--	--	--	--	--	--	--	--	--	--	--

Tunnel: (1-12 characters)

Account Name:

Password:

WAN: Low Middle High ---

Server IP:

IPSec Encryption: ---

Pre-shared Key: (1-128 characters)

Remote Subnet: /

Upstream Bandwidth: Kbps(100-1000000)

Downstream Bandwidth: Kbps(100-1000000)

Working Mode: NAT Route

Status: Enable

Follow these steps to configure the L2TP client:

- 1) Specify the name of the L2TP tunnel and configure other relevant parameters of the L2TP client according to your actual network environment.

Tunnel Specify the name of L2TP tunnel.

Account Name	Specify the account name of L2TP tunnel. It should be configured identically on server and client.
Password	Specify the password of L2TP tunnel. It should be configured identically on server and client.
WAN	Specify the WAN port used for L2TP tunnel.
Server IP	Specify the IP address or domain name of L2TP server.
IPSec Encryption	Specify whether to enable the encryption for the tunnel. If enabled, the L2TP tunnel will be encrypted by IPSec (L2TP over IPSec).
Pre-shared Key	Specify the Pre-shared Key for IKE authentication.
Remote Subnet	Specify the remote network. (It's always the IP address range of LAN on the remote peer of the VPN tunnel.) It's the combination of IP address and subnet mask.
Upstream Bandwidth	Specify the upstream limited rate in Kbps for L2TP tunnel.
Downstream Bandwidth	Specify the downstream limited rate in Kbps for L2TP tunnel.
Working Mode	Specify the Working Mode as NAT or Routing. NAT: NAT (Network Address Translation) mode allows the gateway to translate source IP address of L2TP packets to its WAN IP when forwarding L2TP packets. Route: Route mode allows the gateway to forward L2TP packets via routing protocol.
Status	Check the box to enable the L2TP tunnel.

2) Click **OK**.

4.5 (Optional) Configuring the L2TP Users

Choose the menu **VPN > Users > Users** and click **Add** to load the following page.

Figure 4-5 Configuring the L2TP User

<input type="checkbox"/>	ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operation
--	--	--	--	--	--	--	--	--

Account Name:

Password:

Low
 Middle
 High

Protocol: ▼

Local IP Address:

IP Address Pool:

DNS Address:

Network Mode: ▼

Max Connections: (1-100)

Remote Subnet: /

Follow these steps to configure the L2TP User:

- 1) Specify the account name and password of the L2TP User.

Account Name Specify the account name used for the VPN tunnel. This parameter should be the same with that of the L2TP client.

Password Specify the password of user. This parameter should be the same with that of the L2TP client.

- 2) Specify the protocol as L2TP and configure other relevant parameters cc.

Protocol Specify the protocol for the VPN tunnel. There are two types: L2TP and PPTP.

Local IP Address Specify the local IP address of the tunnel. You can enter the LAN IP of the local device.

IP Address Pool Specify the IP address pool from which the IP address will be assigned to the VPN client. The IP Pool referenced here can be created on the **Preferences > VPN IP Pool** page.

DNS Address Specify the DNS address to be assigned to the VPN client (8.8.8.8 for example).

Network Mode Specify the network mode. There are two modes:

Client-to-LAN: Select this option when the L2TP/PPTP client is a single host.

LAN-to-LAN: Select this option when the L2TP/PPTP client is a VPN gateway. The tunneling request is always initiated by a device.

Max Connections Specify the maximum number of connections that the tunnel can support.

Remote Subnet Specify a remote network. (This is the IP address range of the LAN on the remote peer of the L2TP/PPTP tunnel.) It's the combination of IP address and subnet mask.

3) Click **OK**.

4.6 Verifying the Connectivity of L2TP VPN Tunnel

Choose the menu **VPN > L2TP > Tunnel List** to load the following page.

Figure 4-6 L2TP VPN Tunnel List

Tunnel List							
ID	Account Name	Mode	Tunnel	Local IP	Remote IP	Remote Local IP	DNS
1	tplink	Server	---	192.168.0.1	172.30.30.152	192.168.1.100	---

The **Tunnel List** shows the information of the established L2TP VPN tunnel.

Account Name Displays the account name of L2TP tunnel.

Mode Displays whether the device is server or client.

Tunnel Displays the name of the tunnel when the gateway is an L2TP client.

Local IP Displays the local IP address of the tunnel.

Remote IP Displays the remote real IP address of the tunnel.

Remote Local IP Displays the remote local IP address of the tunnel.

DNS Displays the DNS address of the tunnel.

5 PPTP Configuration

To complete the PPTP configuration, follow these steps:

- 1) Configure the VPN IP pool.
- 2) Configure PPTP globally.
- 3) Configure the PPTP server/client.
- 4) (Optional) Configure the PPTP users.
- 5) Verify the connectivity of the PPTP VPN tunnel.

Configuration Guidelines

- When the network mode is configured as Client-to-LAN and the gateway acts as the PPTP server, you don't need to configure a PPTP client on the gateway.
- When the network mode is configured as LAN-to-LAN and the gateway acts as the PPTP client gateway, you don't need to configure PPTP users on the gateway.

5.1 Configuring the VPN IP Pool

Choose the menu **Preferences > VPN IP Pool > VPN IP Pool** and click **Add** to load the following page.

Figure 5-1 Configuring the VPN IP Pool

IP Pool List + Add - Delete

<input type="checkbox"/>	ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
--	--	--	--	--	--

IP Pool Name:

Starting IP Address:

Ending IP Address:

Follow these steps to configure the VPN IP Pool:

- 1) Specify the name of the IP Pool.
- 2) Specify the starting IP address and ending IP address for the IP Pool.

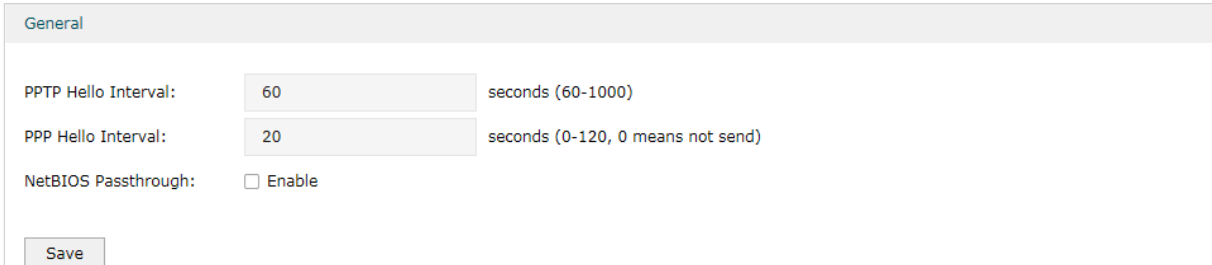
 **Note:**

- The starting IP address should not be greater than the ending IP address.
- The ranges of IP Pools cannot overlap.

5.2 Configuring PPTP Globally

Choose the menu **VPN > PPTP > Global Config** to load the following page.

Figure 5-2 Configuring PPTP Globally



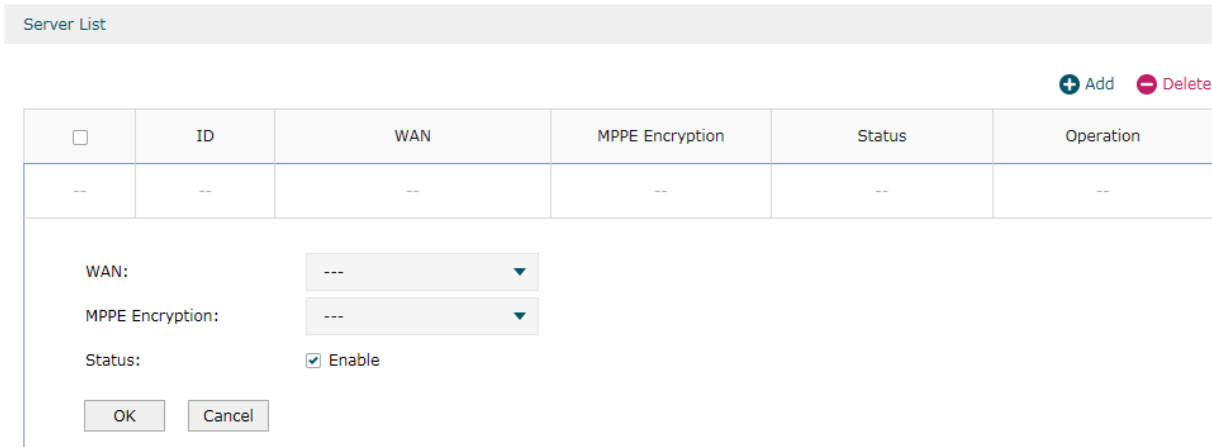
In the **General** section, configure PPTP parameters globally and click **Save**.

PPTP Hello Interval	Specify the time interval of sending PPTP peer detect packets.
PPP Hello Interval	Specify the time interval of sending PPP peer detect packets.
NetBIOS Passthrough	Enable NetBIOS Passthrough function to allow NetBIOS packets to be broadcasted through VPN tunnel.

5.3 Configuring the PPTP Server

Choose the menu **VPN > PPTP > PPTP Server** and click **Add** to load the following page.

Figure 5-3 Configuring the PPTP Server



Follow these steps to configure the PPTP server:

- 1) Specify the WAN port used for PPTP tunnel.
- 2) Specify whether to enable the MPPE encryption for the PPTP tunnel.
- 3) Enable the PPTP tunnel.
- 4) Click **OK**.

5.4 Configuring the PPTP Client

Choose the menu **VPN > PPTP > PPTP Client** and click **Add** to load the following page.

Figure 5-4 Configuring the PPTP Client

<input type="checkbox"/>	ID	Tunnel	Account Name	Server IP	WAN	MPPE Encryption	Remote Subnet	Working Mode	Status	Operation
--	--	--	--	--	--	--	--	--	--	--

Tunnel: (1-12 characters)

Account Name:

Password:

Low Middle High

WAN: ▼

Server IP:

MPPE Encryption: ▼

Remote Subnet: /

Upstream Bandwidth: Kbps (100-1000000)

Downstream Bandwidth: Kbps (100-1000000)

Working Mode: NAT Route

Status: Enable

Follow these steps to configure the PPTP client:

- 1) Specify the name of the PPTP tunnel and configure other relevant parameters of the PPTP client according to your actual network environment.

Tunnel	Specify the name of PPTP tunnel.
Account Name	Specify the account name of PPTP tunnel. It should be configured identically on server and client.
Password	Specify the password of PPTP tunnel. It should be configured identically on server and client.
WAN	Specify the WAN port used for PPTP tunnel.
Server IP	Specify the IP address or domain name of PPTP server.

MPPE Encryption	Specify whether to enable the encryption for the tunnel. If enabled, the PPTP tunnel will be encrypted by MPPE.
Remote Subnet	Specify the remote network. (It's always the IP address range of LAN on the remote peer of the VPN tunnel.) It's the combination of IP address and subnet mask.
Upstream Bandwidth	Specify the upstream limited rate in Kbps for PPTP tunnel.
Downstream Bandwidth	Specify the downstream limited rate in Kbps for PPTP tunnel.
Working Mode	Specify the Working Mode as NAT or Routing. NAT: NAT (Network Address Translation) mode allows the gateway to translate source IP address of PPTP packets to its WAN IP when forwarding PPTP packets. Route: Route mode allows the gateway to forward PPTP packets via routing protocol.
Status	Check the box to enable the PPTP tunnel.

2) Click **OK**.

5.5 (Optional) Configuring the PPTP Users

Choose the menu **VPN > Users > Users** and click **Add** to load the following page.

Figure 5-5 Configuring the PPTP User

<input type="checkbox"/>	ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operation
--	--	--	--	--	--	--	--	--

Account Name:

Password:

Protocol: ▼

Local IP Address:

IP Address Pool:

DNS Address:

Network Mode: ▼

Max Connections: (1-100)

Remote Subnet: /

Follow these steps to configure the PPTP User:

1) Specify the account name and password of the PPTP User.

Account Name	Specify the account name used for the VPN tunnel. This parameter should be the same as that of the PPTP client.
Password	Specify the password of users. This parameter should be the same as that of the PPTP client.

2) Specify the protocol as PPTP and configure other relevant parameters according to your actual network environment.

Protocol	Specify the protocol for the VPN tunnel. There are two types: L2TP and PPTP.
Local IP Address	Specify the local IP address of the tunnel. You can enter the LAN IP of the local device.
IP Address Pool	Specify the IP address pool from which the IP address will be assigned to the VPN client. The IP Pool referenced here can be created on the Preferences > VPN IP Pool page.
DNS Address	Specify the DNS address to be assigned to the VPN client (8.8.8.8 for example).
Network Mode	Specify the network mode. There are two modes: Client-to-LAN: Select this option when the PPTP/PPTP client is a single host. LAN-to-LAN: Select this option when the PPTP/PPTP client is a VPN gateway. The tunneling request is always initiated by a device.
Max Connections	Specify the maximum number of connections that the tunnel can support.
Remote Subnet	Specify a remote network. (This is the IP address range of the LAN on the remote peer of the PPTP/PPTP tunnel.) It's the combination of IP address and subnet mask.

3) Click **OK**.

5.6 Verifying the Connectivity of PPTP VPN Tunnel

Choose the menu **VPN > PPTP > Tunnel List** to load the following page.

Figure 5-6 PPTP VPN Tunnel List

Tunnel List  Refresh

ID	Account	Mode	Tunnel	Local IP	Remote IP	Remote Local IP	DNS
1	tplink	Server	---	192.168.0.1	172.30.30.152	192.168.1.102	---

The **Tunnel List** shows the information of the established PPTP VPN tunnel.

Account	Displays the account name of PPTP tunnel.
Mode	Displays whether the device is server or client.

Tunnel	Displays the name of the tunnel when the gateway is a PPTP client.
Local IP	Displays the local IP address of the tunnel.
Remote IP	Displays the remote real IP address of the tunnel.
Remote Local IP	Displays the remote local IP address of the tunnel.
DNS	Displays the DNS address of the tunnel.

6 OpenVPN Configuration

To complete the OpenVPN Configuration, follow these steps:

- 1) Configure the OpenVPN server/client.
- 2) Check the tunnel list to verify the connectivity of the OpenVPN tunnel.

Configuration Guidelines

- If you only use the gateway as the OpenVPN server, you don't need to configure the OpenVPN client.

6.1 Configuring the OpenVPN Server

Choose the menu **VPN > OpenVPN > OpenVPN Server** and click **Add** to load the following page.

Figure 6-1 Configuring the OpenVPN Server

+ Add - Delete

<input type="checkbox"/>	ID	Server Name	Protocol	Service Port	Local Network	Primary DNS	Secondary DNS	Status	Operation
--	--	--	--	--	--	--	--	--	--

Server Name: (1-32 characters)

AccountPWD: Enable

Status: Enable

Full Mode: Enable

Protocol: TCP UDP

Service Port: (1-65535)

Local Network: /

WAN: ▼

IP Pool: /

Primary DNS:

Secondary DNS: (Optional)

Authentication Type:

Specify the name of the OpenVPN server, configure other relevant parameters according to your actual network environment, and click **OK**.

Server Name	Enter a name to identify the VPN server.
AccountPWD	When enabled, OpenVPN will use username/password to authenticate users.
Status	Check the box to enable the OpenVPN server.
Full Mode	Select this option to allow all client traffic to pass through the tunnel.
Protocol	Select the communication protocol for the gateway which works as an OpenVPN Server. Two communication protocols are available: TCP and UDP.
Service Port	Enter a VPN service port to which a VPN device connects. The default port is 1194.
Local Network	Select the network on the local side of the VPN tunnel. The VPN policy will be only applied to the selected local network.
WAN	Select the WAN port on which the VPN tunnel is established. Each WAN port supports only one OpenVPN tunnel when the gateway works as a OpenVPN server.
IP Pool	Enter the IP address and subnet mask to decide the range of the VPN IP pool. The VPN server will assign IP address to the remote host when the tunnel is established. You can specify any reasonable IP address that will not cause overlap with the IP address of the LAN on the local peer gateway.
Primary DNS	Specify the primary DNS server pushed to clients.
Secondary DNS	Specify the secondary DNS server pushed to clients.
Authentication Type	Specify the authentication method used by the OpenVPN server. Local: Use a built-in authentication server to authenticate when the tunnel is created. If you don't have an additional external server, you can choose local authentication. LDAP: Use an external LDAP server to authenticate when the tunnel is created.

 **Note:**

- After saving the settings, export the OpenVPN file that ends in .ovpn which is to be used by the remote client. The exported OpenVPN file contains the certificate and configuration information. It may take about 2 minutes to export the certificate.

6.2 Configuring the OpenVPN Client

Choose the menu **VPN > OpenVPN > OpenVPN Client** and click **Add** to load the following page. The gateway will act as an OpenVPN client to establish the VPN tunnel with the remote Server.

Figure 6-2 Configuring the OpenVPN Client

+ Add - Delete

☐	ID	Client Name	Service Port	Remote Server	Local Network	Status	Operation
--	--	--	--	--	--	--	--

Client Name: (1-32 characters)

Mode: CA CA+PWD

Service Port: (1-65535)

Remote Server:

Local Network: /

WAN: ▼

File Path: (OVPN file is required.)

Export the certificate file of the OpenVPN Server.

Status: Enable

Specify the name of the OpenVPN client, configure other relevant parameters according to your actual network environment, and click **OK**.


Client Name	Specify the name of OpenVPN client.
Mode	Select the authentication method used by the client. In ca mode, only the certificate file is required. In ca+pwd mode, additional username and password are required. Username - Enter the username required for client authentication. Password - Enter the password required for client authentication.
Service Port	Enter a VPN service port to which a VPN device connects. The default port is 1194.
Remote Server	Enter the IP address or domain name of the OpenVPN server.
Local Network	Select the network on the local side of the VPN tunnel. The VPN policy will be only applied to the selected local network.
WAN	Select the WAN port on which the VPN tunnel is established.

File Path	Browse the file to find the OpenVPN file that ends in .ovpn generated by the OpenVPN server.
Import	Click this button to import the OpenVPN file that ends in .ovpn generated by the OpenVPN server. Only one file can be imported. If the certificate file and configuration file are generated singly by the OpenVPN server, combine two files and import the whole file.
Status	Check the box to enable the OpenVPN client.

6.3 Viewing the OpenVPN Tunnel

Choose the menu **VPN > OpenVPN > OpenVPN Tunnel** to load the following page.

Figure 6-3 Viewing the OpenVPN Tunnel

OpenVPN Tunnel List							
Entry Count: 0							 Refresh
ID	Name	WAN	Local IP	Remote IP	Up Bytes	Down Bytes	Up Time
--	--	--	--	--	--	--	--

Click **Refresh** to view the latest information.

Name	Displays the account name of OpenVPN server/client.
WAN	Displays the WAN port on which the VPN tunnel is established.
Local IP	Displays the assigned virtual local IP address of the tunnel.
Remote IP	Displays the assigned virtual local IP address of the tunnel.
Up Bytes	Displays the upstream throughput.
Down Bytes	Displays the downstream throughput.
Up Time	Displays how long the tunnel has been up.

7 WireGuard VPN Configuration

To complete the WireGuard VPN Configuration, follow these steps:

- 1) Configure the WireGuard Server.
- 2) Configure the Peers settings.

7.1 Configuring the WireGuard VPN Server

Choose the menu **VPN > WireGuard > WireGuard** and click **Add** to load the following page.

Figure 7-1 Configuring the WireGuard VPN Server

The screenshot shows the 'Wireguard' configuration page. At the top right, there are '+ Add' and '- Delete' buttons. Below is a table with columns: ID, Name, MTU, TX Bytes, RX Bytes, TX Packets, RX Packets, Listen Port, Status, and Operation. The table is currently empty. Below the table is a configuration form for a new server with the following fields:

- Name:** [Empty text input]
- MTU:** [1420] (576-1440)
- Listen Port:** [51820] (1-65535)
- Private Key:** [Masked with dots] (Optional)
- Public Key:** [2nKaZJITLWtm7IoPU6CpU]
- Local IP Address:** [Empty text input]
- Status:** Enable

At the bottom of the form are 'OK' and 'Cancel' buttons.

Specify the name of the WireGuard VPN server, configure other relevant parameters according to your actual network environment, and click **OK**.

Name	Specify the name that identifies the Wireguard interface.
MTU	Specify the MTU value of the Wireguard interface. The default value 1420 is recommended.
Listen Port	Specify the port number that the Wireguard interface listens to.
Service Port	Enter a VPN service port to which a VPN device connects. The default port is 1194.
Private Key	Specify the private key of the Wireguard interface. The value will be automatically generated on the device, and you can also modify it manually.

Public Key	Specify the public key of the Wireguard interface. This field will be automatically generated based on the private key.
Local IP Address	Specify the IP address of the WireGuard interface. Please select a reserved address to avoid IP conflicts.
Status	Specify whether to enable the Wireguard interface.

7.2 Configuring the Peers Settings

Choose the menu **VPN > WireGuard > Peers** and click **Add** to load the following page.

Figure 7-2 Configuring the Peers

+ Add
 - Delete

<input type="checkbox"/>	Interface	Endpoint	Endpoint Port	Allowed Address	TX Bytes	RX Bytes	TX Packets	RX Packets	Last Handshake	Status	Operation
--	--	--	--	--	--	--	--	--	--	--	--

Interface:

Public Key:

Endpoint: (Optional)

Endpoint Port: (Optional, 1-65535)

Allowed Address: /

Preshared Key: (Optional)

Persistent Keepalive: (0-65535)

Comment: (0-128 characters)

Status: Enable

You should configure an Endpoint and an Endpoint Port for at least one peer gateway.

Interface	Specify the Wireguard interface to which the peer belongs.
Public key	Specify the public key of the peer.
Endpoint	Specify the IP address of the peer.
Endpoint Port	Specify the port number of the peer.

Allowed Address	Specify the address segment that allows traffic to pass through. Generally, you can fill in the subnet address of the peer.
Persistent Keepalive	Specify the tunnel keepalive packet interval.
Comment	Enter the description of the peer.
Status	Specify whether to enable the peer.

8 Users Configuration

To configure the accounts of users, Choose the menu **VPN > Users > Users** and click **Add** to load the following page.

Figure 8-1 Configuring the User Account

+ Add - Delete

<input type="checkbox"/>	ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operation
--	--	--	--	--	--	--	--	--

Account Name:

Password:

Low
Middle
High

Protocol: ▼

Local IP Address:

IP Address Pool:

DNS Address:

Network Mode: ▼

Max Connections: (1-100)

Remote Subnet: /

Enter the account name and password, configure other relevant parameters according to your actual network environment, and click **OK**.

Account Name	Specify the account name used for the VPN tunnel.
Password	Specify the account password used for the VPN tunnel. Your VPN clients will use the account name and password for authentication.
Protocol	Specify the protocol for the VPN tunnel. There are two types: L2TP and PPTP.
Local IP Address	Specify the local virtual IP address for the VPN server. Please avoid using the IP address in the DHCP range, which may cause IP confliction, you can enter the LAN IP of the gateway. To find out the DHCP Range, go to Network > LAN > Network List and view the information of the desired network.
IP Address Pool	Specify the IP address pool from which the IP address will be assigned to the VPN client. The IP Pool referenced here can be created on the Preferences > VPN IP Pool page.
DNS Address	Specify the DNS address to be assigned to the VPN client (8.8.8.8 for example), you can enter the LAN IP of the gateway.

Network Mode	<p>Specify the network mode. There are two modes:</p> <p>Client-to-LAN: Select this option when the L2TP/PPTP client is a single host. It's commonly used to access the internal service from outside.</p> <p>LAN-to-LAN: Select this option when the L2TP/PPTP client is a VPN gateway. The tunneling request is always initiated by a device. It's commonly used for access between two offices.</p>
Max Connections	<p>Specify the maximum number of connections that the tunnel can support. When Client-to-LAN network mode is enabled, it can be used to limit the number of devices connected at the same time.</p>
Remote Subnet	<p>Specify a remote network. (This is the IP address range of the LAN on the remote peer of the L2TP/PPTP tunnel.) It's the combination of IP address and subnet mask. It takes effect when LAN-to-LAN network mode is enabled.</p>

 **Note:**

- Create VPN connection accounts for remote devices to connect to the VPN server.
 - If the gateway acts as the L2TP/PPTP client, you don't need to configure the L2TP/ PPTP user accounts on this page.
-

Part 11

Configuring Authentication

CHAPTERS

1. Overview
2. Local Authentication Configuration
3. Radius Authentication Configuration
4. Onekey Online Configuration
5. LDAP Configuration
6. Guest Resources Configuration
8. Viewing the Authentication Status
9. Configuration Example

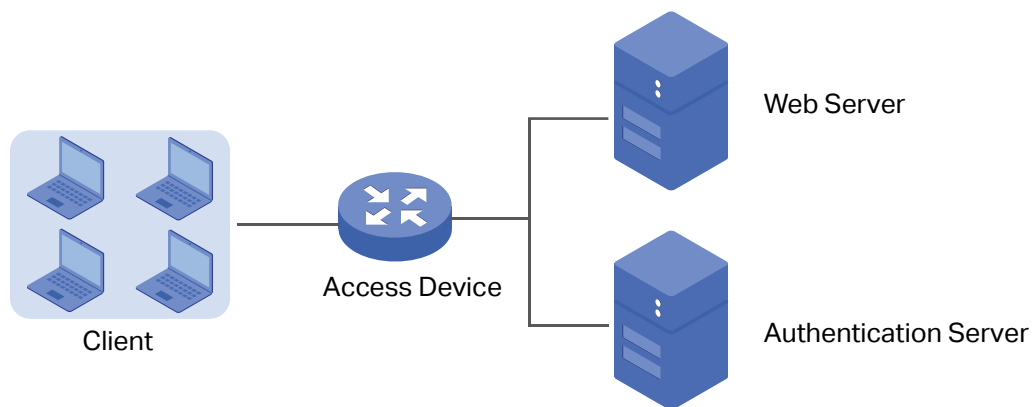
1 Overview

Portal authentication, also known as Web authentication, is usually deployed in a guest-access network (like a hotel or a coffee shop) to control the client's internet access. In portal authentication, all the client's HTTP requests will be redirected to an authentication page first. The client needs to enter the account information on the page to authenticate, then can visit the internet after the authentication succeeded.

1.1 Typical Topology

The typical topology of portal authentication is shown as below:

Figure 1-1 Topology of Portal Authentication



■ Client

The end device that needs to be authenticated before permitted to access the internet.

■ Access Device

The device that supports portal authentication. In this user guide, it means the gateway. The Access Device helps to: redirect all HTTP requests to the Web Server before authenticated; interact with the Authentication Server to authenticate the client during the authentication process; permit users to access the internet after the authentication succeeded.

■ Web Server

The web server responds to client's HTTP requests, and returns an authentication login page.

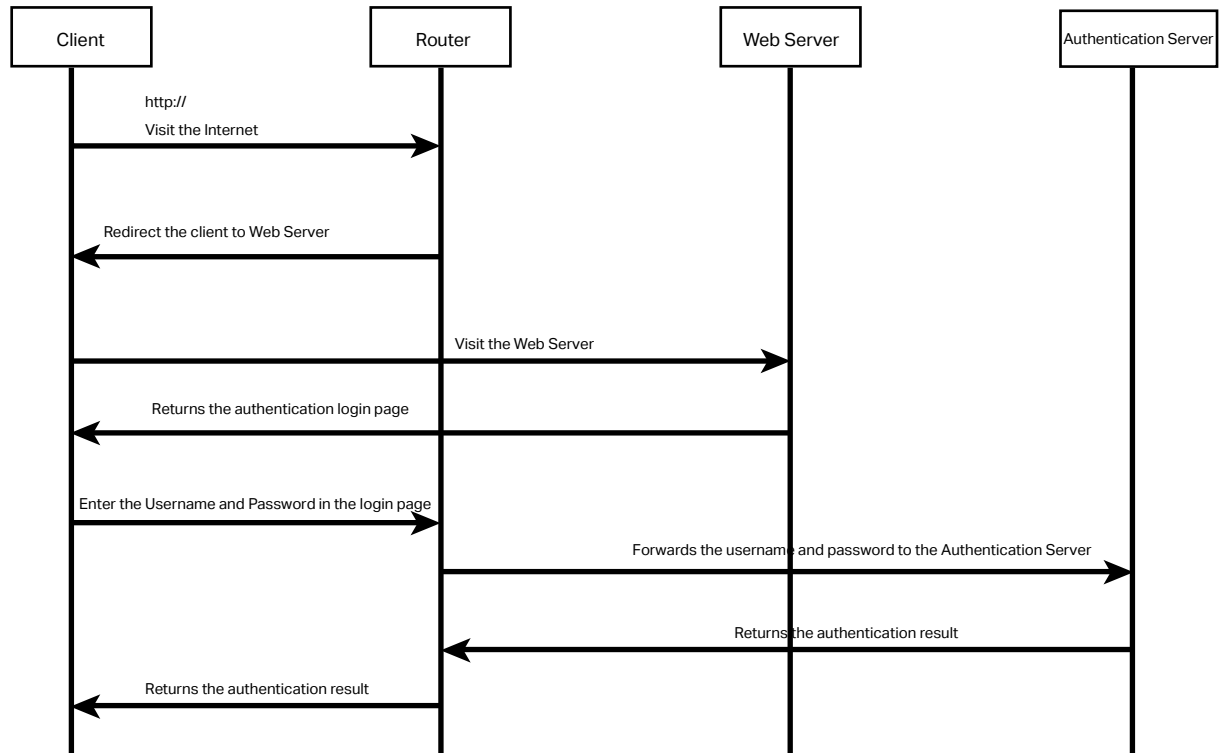
■ Authentication Server

The authentication server records the information of the user's account, and interacts with the access device to authenticate clients.

1.2 Portal Authentication Process

The portal authentication process is shown as below:

Figure 1-2 Portal Authentication Process



- 1) The client is connected to the gateway but not authenticated, and starts to visit the internet through HTTP;
- 2) The gateway redirects the client's HTTP request to the web server;
- 3) The client visits the web server;
- 4) The Web server returns the authentication login page to the client;
- 5) The client enters the username and password on the authentication login page;
- 6) The gateway forwards the username and password to the authentication server;
- 7) The authentication server returns the authentication result to the gateway;
- 8) The gateway replies to the client with the authentication result;
- 9) The client visits the internet after the authentication succeeded.

1.3 Supported Features

To configure portal authentication, you need to configure both the web server and the authentication server. The web server provides the authentication page for login; the authentication server records the account information and authenticates the clients.

1.3.1 Supported Web Server

The gateway has a built-in web server and also supports external web server. You can configure the authentication page either using the built-in server or the external server.

Custom Page

You can use the built-in web server and customize the authentication page on your gateway.

External Links

You can specify the external web server and configure the authentication page on the external web server.

1.3.2 Supported Authentication Server

The gateway provides three types of portal authentication:

Radius Authentication

In Radius authentication, you can specify an external Radius server as the authentication server. The user's account information are recorded in the Radius server.

Local Authentication

If you don't have an additional Radius server, you can choose local authentication. In local authentication, the gateway uses the built-in authentication server to authenticate. The built-in authentication server can record at most 500 local user accounts, and each account is can be used for at most 1024 clients to authenticate.

Onekey Online

In Onekey Online Authentication, users can access the network without entering any account information.

1.3.3 Guest Resources

Guest Resources is used to provide free resources for users before they pass the portal authentication.

2 Local Authentication Configuration

To configure local authentication, follow the steps:

- 1) Configure the authentication page.
- 2) Configure the local user account.

2.1 Configuring the Authentication Page

The browser will redirect to the authentication page when the client try to access the internet. On the authentication page, the user need to enter the username and password to log in. After the authentication succeeded, the user can access the internet.

Choose the menu **Authentication > Authentication Settings > Web Authentication** to load the following page.

Figure 2-1 Configuring the Authentication Page

The screenshot shows the configuration interface for Web Authentication. It is organized into two main sections: 'Settings' and 'Authentication Parameters'.
Settings Section:
 - **Status:** A checkbox labeled 'Enable' is currently unchecked.
 - **Interface:** A dropdown menu is set to 'LAN'.
 - **Idle Timeout:** A text input field contains '30', with a note 'minutes (0 or 5-1440, 0 means always online)'.
 - **Portal Authentication Port:** A text input field contains '8080', with a note '(8080, 1024-65535)'.
Authentication Parameters Section:
 - **Authentication Page:** A dropdown menu is set to 'Custom Page'.
 - **Background Picture:** An 'Upload' button is next to a dashed line, with a note '(The image size cannot exceed 200KB.)'.
 - **Welcome Information:** A text input field with a note '(1-50 characters)'.
 - **Copyright:** A text input field with a note '(1-50 characters)'.
 - **Page Preview:** A button labeled 'Login Page Preview'.
 - **Authentication Type:** A dropdown menu is set to 'Local Authentication'.
 - **Expiration Reminder:** A checkbox labeled 'Enable' is checked.
 - **Time to Remind:** A text input field contains '3', with a note 'days (1-10)'.
 - **Remind Type:** A dropdown menu is set to 'Remind Periodically'.
 - **Remind Interval:** A text input field with a note 'minutes (1-120)'.
 - **Remind Content:** A text input field with a note '(1-50 characters)'.
 - **Page Preview:** A button labeled 'Remind Page Preview'.
 At the bottom left of the form is a 'Save' button.

Follow these steps to configure authentication page:

- 1) In the **Settings** section, enable authentication status, configure the idle timeout and portal authentication port.

Status	Check the box to enable portal authentication.
Interface	Specify the effective interface.
Idle Timeout	Specify the idle timeout. The client will be disconnected after the specified period (Idle Timeout) of inactivity, and is required to be authenticated again. Value 0 means the client will always keep online until the authentication timeout leased, even if the client remains inactive.
Portal Authentication Port	Enter the service port for portal authentication. The default setting is 8080.

- 2) In the **Authentication Parameters** section, configure the parameters of the authentication page.

Authentication Page	<p>Choose the authentication page type.</p> <p>Custom: You can use the built-in web server to customize the authentication page by specifying the background picture, welcome information and copyright information.</p> <p>External Links: You can specify a external web server to provide the authentication page by entering the URL of the external web server.</p>
Background Picture	Click the Upload button to choose a local image as the background picture of the custom authentication page.
Welcome Information	Specify the welcome information to be displayed on the custom authentication page.
Copyright	Specify the copyright information to be displayed on the custom authentication page.
Page Preview	Click the Login Page Preview button, and you can preview the customized authentication page.
Authentication URL	Specify the URL for authentication page if you choose the Authentication Page as "External Links". The browser will redirect to this URL when the client starts the authentication.
Success Redirect URL	Specify the Success Redirect URL if you choose the Authentication Page as "External Links". The browser will redirect to this URL after the authentication succeeded.
Fail redirect URL	Specify the Fail Redirect URL if you choose the Authentication Page as "External Links". The browser will redirect to this URL if the authentication failed.

 **Note:**

If the web server is not deployed in the LAN, you need to create a Guest Resource entry to ensure the client can access the external web server before the authentication succeeded. For the configuration of Guest Resource, go to Guest Resources Configuration.

3) Choose the authentication type, and configure the expiration reminder, then click **Save**.

Authentication Type	Choose the authentication type as Local Authentication.
Expiration Reminder	Check the box to enable expiration reminder. A remind page will appear to remind users when the online time is about to expire.
Time to Remind	Specify the number of days before the expiration date to remind users.
Remind Type	Specify the remind type. Remind Once: Remind the user only once after the authentication succeeded. Remind Periodically: Remind users at specified intervals during the remind period.
Remind Interval	Specify the interval at which the gateway reminds users if the remind type is specified as "Remind Periodically".
Remind Content	Specify the remind content. The content will be displayed on the Remind page.
Page Preview	Click the button to view the remind page.

2.2 Configuring the Local User Account

In Local authentication, the gateway uses the built-in authentication server to authenticate users. You need to configure the authentication accounts for the local users.

The gateway supports two types of local users:

Formal User: If you want to provide the user with network service for a long period of time (in days), you can create Formal User accounts for them.

Free User: If you want to provide the user with network service for a short period of time (in minutes), you can create Free User accounts for them.

2.2.1 Configuring the Local User Account

■ Configuring the Formal User Account

Choose the menu **Authentication > User Management > User Management** and click **Add** to load the following page.

Figure 2-2 Configuring the Formal User Account

<input type="checkbox"/>	ID	User Type	Username	Authentication Timeout	MAC Address	Description	Status	Operation
--	--	--	--	--	--	--	--	--

User Type: Formal User ▼

Username: (1-100 Characters)

Password: (1-100 Characters)

Expiration Date: 2017-12-31 (YYYY-MM-DD)

Authentication Period: 00:00-24:00 (HH:MM-HH:MM)

MAC Binding Type: Static Binding ▼

MAC Address : (XX-XX-XX-XX-XX)

Maximum Users: 1 (1-1024)

Upstream Bandwidth: 0 Kbps (0 or 10-1,000,000. 0 means no limit)

Downstream Bandwidth: 0 Kbps (0 or 10-1,000,000. 0 means no limit)

Name: (1-50 characters, optional)

Telephone: (1-50 characters, optional)

Description: (1-50 characters, optional)

Status: Enable

OK
Cancel

Specify the user type, configure the username and password for the formal user account, and configure the other corresponding parameters. Then click **OK**.

User Type	Specify the user type as Formal User.
Username / Password	Specify the username and password of the account. The username cannot be the same as any existing one.
Expiration Date	Specify the expiration date of the account. The formal user can use this account to authenticate before this date.
Authentication Period	Specify the period during which the client is allowed to be authenticated.
MAC Binding Type	<p>Specify the MAC Binding type. There are three types of MAC Binding: No binding, Static Binding and Dynamic Binding.</p> <p>No Binding: The client's MAC address will not be bound.</p> <p>Static Binding: Manually enter the MAC address of the client to be bound. Only the bound client is able to use the username and password to authenticate.</p> <p>Dynamic Binding: The MAC address of the first client that passes the authentication will be bound. Afterwards only the bound client is able to use the username and password to authenticate.</p>
MAC Address	Enter the MAC address of the client to be bound if you choos the MAC Binding type as "Static Binding".

Maximum Users	Specify the maximum number of users that are allowed use this account to authenticate. Note: If the MAC Binding Type is either Static Binding or Dynamic Binding, only one client can use this username and password to authenticate,i.e., the bound client, even if the value of Maximum Users is configured to be greater than one.
Upstream Bandwidth / Downstream Bandwidth	(Optional) Specify the upstream / downstream bandwidth for the user. 0 means no limit.
Name	(Optional) Record the user's name.
Telephone	(Optional) Record the user's telephone number.
Description	(Optional) Enter a brief description for the user.
Status	Check the box to enable this account.

■ **Configuring the Free User Account**

Choose the menu **Authentication > User Management > User Management** and click **Add** to load the following page.

Figure 2-3 Configuring the Free User Account

<input type="checkbox"/>	ID	User Type	Username	Authentication Timeout	MAC Address	Description	Status	Operation
--	--	--	--	--	--	--	--	--

User Type: Free User ▼

Username: (1-100 Characters)

Password: (1-100 Characters)

Authentication Timeout (minutes): (1-1440)

Authentication Period: (HH:MM-HH:MM)

Maximum Users: (1-1024)

Upstream Bandwidth: Kbps (0 or 10-1,000,000. 0 means no limit)

Downstream Bandwidth: Kbps (0 or 10-1,000,000. 0 means no limit)

Description: (1-50 characters, optional)

Status: Enable

Specify the user type, configure the username and password for the free user account, and configure the other corresponding parameters. Then click **OK**.

User Type	Specify the user type as Free User.
------------------	-------------------------------------

Username / Password	Specify the username and password of the user account. The username cannot be the same as any existing one.
Authentication Timeout	Specify the free duration of the account. The default value is 30 minutes.
Maximum Users	Specify the maximum number of users that are allowed to use this username and password to authenticate.
Upstream Bandwidth / Downstream Bandwidth	(Optional) Specify the upstream/downstream bandwidth for the user. 0 means no limit.
Status	Check the box to enable this account.

2.2.2 (Optional) Configuring the Backup of Local Users

Choose the menu **Authentication > User Management > Configuration Backup** to load the following page.

Figure 2-4 Configuring the Formal User

■ To backup local users' accounts

Click **Backup** button to backup all the local users accounts as a CSV file in ANSI coding format.

■ To restore local users' accounts

You can import the accounts to the gateway if you have backups. Click **Browse** to select the file path (the backup must be a CSV file), then click **Restore** to restore the accounts.

You can also manually add multiple local user accounts at a time:

- 1) Create an Excel file and add the local user accounts to it, then save the Excel file as a CSV file with ANSI coding format. You can click **Backup** to obtain a CSV file to view the correct format.
- 2) Click **Browse** to select the file path, then click **Restore** to restore the file.

Note:

Using Excel to open the CSV file may cause some numerical format changes, and the number may be displayed incorrectly. If you use Excel to edit the CSV file, please set the cell format as text.

3 Radius Authentication Configuration

To configure Radius Authentication, follow the steps:

- 1) Configure the authentication page.
- 2) Specify the external Radius server and configure the corresponding parameters.

3.1 Configuring Radius Authentication

Choose the menu **Authentication > Authentication Settings > Web Authentication** to load the following page.

Figure 3-1 Configuring the Radius Authentication

The screenshot shows a web-based configuration interface for Radius Authentication. It is organized into two main sections: 'Settings' and 'Authentication Parameters'.
Settings Section:
 - **Status:** A checkbox labeled 'Enable' is currently unchecked.
 - **Interface:** A dropdown menu is set to 'LAN'.
 - **Idle Timeout:** A text input field contains '30', with a note indicating the unit is 'minutes (0 or 5-1440, 0 means always online)'.
 - **Portal Authentication Port:** A text input field contains '8080', with a note indicating the range '(8080, 1024-65535)'.
Authentication Parameters Section:
 - **Authentication Page:** A dropdown menu is set to 'Custom Page'.
 - **Background Picture:** An 'Upload' button is followed by a dashed line '---' and a note '(The image size cannot exceed 200KB.)'.
 - **Welcome Information:** A text input field with a note '(1-50 characters)'.
 - **Copyright:** A text input field with a note '(1-50 characters)'.
 - **Page Preview:** A button labeled 'Login Page Preview'.
 - **Authentication Type:** A dropdown menu is set to 'Radius Authentication'.
 - **Primary Radius Server:** A text input field with a note '(Required)'.
 - **Secondary Radius Server:** A text input field with a note '(Optional)'.
 - **Authentication Port:** A text input field contains '1812' with a note '(1024-65535)'.
 - **Authorized Share Key:** A text input field with a note '(1-48 characters)'.
 - **Retry Times:** A text input field contains '3' with a note '(1-10)'.
 - **Timeout Interval:** A text input field contains '3' with a note '(1-60 seconds)'.
 - **Authentication Method:** A dropdown menu is set to 'PAP'.
 At the bottom left of the form, there is a 'Save' button.

Follow these steps to configure Radius Authentication:

- 1) In the **Settings** section, enable the authentication status, configure the idle timeout and portal authentication port.

Status	Check the box to enable portal authentication.
Interface	Specify the effective interface.
Idle Timeout	Specify the idle timeout. The client will be disconnected after the specified period (Idle Timeout) of inactivity, and is required to be authenticated again. Value 0 means the client will always keep online until the authentication timeout leased, even if the client remains inactive.
Portal Authentication Port	Enter the service port for portal authentication. The default setting is 8080.

- 2) In the **Authentication Parameters** section, configure the parameters of the authentication page.

Authentication Page	<p>Choose the authentication page type.</p> <p>Custom: You can use the built-in web server to customize the authentication page by specifying the background picture, welcome information and copyright information.</p> <p>External Links: You can use external pages by specifying the external links as the authentication page.</p>
Background Picture	Click the Upload button to choose a local image as the background picture of the custom authentication page.
Welcome Information	Specify the welcome information to be displayed on the custom authentication page.
Copyright	Specify the copyright information to be displayed on the custom authentication page.
Page Preview	Click the Login Page Preview button, and you can preview the customized authentication page
Authentication URL	Specify the URL for authentication page if you choose the Authentication Page as "External Links". The browser will redirect to this URL when the client starts the authentication.
Success Redirect URL	Specify the Success Redirect URL if you choose the Authentication Page as "External Links". The browser will redirect to this URL after the authentication succeeded.
Fail redirect URL	Specify the Fail Redirect URL if you choose the Authentication Page as "External Links". The browser will redirect to this URL if the authentication failed.

 **Note:**

If the web server is not deployed in the LAN, you need to create a Guest Resource entry to ensure the client can access the external web server before the authentication succeeded. For the configuration of Guest Resource, go to Guest Resources Configuration.

- 3) Specify the external Radius server and configure the corresponding parameters, then click **Save**.

Authentication Type	Choose the authentication type as Radius Authentication.
Primary Radius Server	Enter the IP address of the primary Radius server.
Secondary Radius Server	(Optional) Enter the IP address of the secondary Radius server. If the primary server is down, the secondary server will be effective.
Authentication Port	Enter the service port for Radius authentication. By default, it is 1812.
Authorized Share Key	Specify the authorized share key. This key should be the same configured in the Radius server.
Retry Times	Specify the number of times the gateway will retry sending authentication requests after the authentication failed.
Timeout Interval	Specify the timeout interval that the client can wait before the radius server replies.
Authentication Method	Specify the authentication protocol as PAP or CHAP.

4 Onekey Online Configuration

In Onekey Online authentication, users only need to click the “Onekey online” button on the authentication page, then can access the internet. The username and password are not required.

4.1 Configuring the Authentication Page

Choose the menu **Authentication > Authentication Settings > Web Authentication** to load the following page.

Figure 4-1 Configuring the Web Authentication

Follow these steps to configure Onekey Online Authentication:

- 1) In the **Settings** section, enable the authentication status, configure the idle timeout and portal authentication port.

Status	Check the box to enable portal authentication.
Interface	Specify the effective interface.
Idle Timeout	Specify the idle timeout. The client will be disconnected after the specified period (Idle Timeout) of inactivity, and is required to be authenticated again. Value 0 means the client will always keep online until the authentication timeout leased, even if the client remains inactive.

Portal Authentication Port	Enter the service port for portal authentication. The default setting is 8080.
----------------------------	--

- 2) In the **Authentication Parameters** section, configure the parameters of the authentication page and choose the authentication type, then click **Save**.

Authentication Page	Choose the type of authentication page as Custom Page. Note: External Links is not available for Onekey Online.
---------------------	--

Background Picture	Click the Upload button to choose a local image as the background picture of the custom authentication page.
--------------------	---

Welcome Information	Specify the welcome information to be displayed on the custom authentication page.
---------------------	--

Copyright	Specify the copyright information to be displayed on the custom authentication page.
-----------	--

Page Preview	Click the Login Page Preview button, and you can preview the customized authentication page
--------------	--

Authentication Type	Choose the authentication type as Onekey Online.
---------------------	--

Free Authentication Timeout	Specify the free duration for Onekey Online. When the free duration expired, users can click "Onekey Online" button on the authentication page to continue to visit the internet.
-----------------------------	---

5 LDAP Configuration

LDAP Authentication allows you to bind the device to an LDAP server and use that server to authenticate LAN clients.

5.1 Configuring the Authentication Page

Choose the menu **Authentication > Authentication Settings > Web Authentication** to load the following page.

Figure 5-1 Configuring the Web Authentication

Follow these steps to configure Onekey Online Authentication:

- 1) In the **Settings** section, enable the authentication status, configure the idle timeout and portal authentication port.

Status	Check the box to enable portal authentication.
Interface	Specify the effective interface..
Idle Timeout	Specify the idle timeout. The client will be disconnected after the specified period (Idle Timeout) of inactivity, and is required to be authenticated again. Value 0 means the client will always keep online until the authentication timeout leased, even if the client remains inactive.

Portal Authentication Port	Enter the service port for portal authentication. The default setting is 8080.
----------------------------	--

- 2) In the **Authentication Parameters** section, configure the parameters of the authentication page and choose the authentication type, then click **Save**.

Authentication Page	Choose the type of authentication page as Custom Page. Note: External Links is not available for Onekey Online.
---------------------	--

Background Picture	Click the Upload button to choose a local image as the background picture of the custom authentication page.
--------------------	---

Welcome Information	Specify the welcome information to be displayed on the custom authentication page.
---------------------	--

Copyright	Specify the copyright information to be displayed on the custom authentication page.
-----------	--

Page Preview	Click the Login Page Preview button, and you can preview the customized authentication page
--------------	--

Authentication Type	Choose the authentication type as LDAP Online.
---------------------	--

LDAP Profile	Select a profile from previously configured LDAP profiles.
--------------	--

6 Guest Resources Configuration

Guest resources are limited network resources provided for users before they pass the portal authentication.

You can configure the guest resources in two ways:

■ Five Tuple Type

Specify the client and the network resources the client can visit based on the settings of IP address, MAC address, VLAN ID, service port and protocol. It is recommended to select Five Tuple Type when the IP address and service port of the free network resource are already known.

■ URL Type

Specify the client and the network resources the client can visit based on the settings of the URL, IP address, MAC address and service port. It is recommended to select URL Type when the URL of the free network resource is already known.

Note:

By default, the Guest Resource table is empty, which means all the clients cannot visit any network resource before they pass the portal authentication.

6.1 Configuring the Five Tuple Type

Choose the menu **Authentication > Authentication Settings > Guest Resources** and click **Add** to load the following page.

Figure 6-1 Configuring the Five Tuple Type

<input type="checkbox"/>	ID	Name	Type	Source IP Range	Destination IP Range	Source Port	Destination Port	Status	Operation
--	--	--	--	--	--	--	--	--	--

Name: (1-50 characters)

Type: Five Tuple Type ▼

Source IP Range: / (Optional)

Destination IP Range: / (Optional)

Source MAC Address: (XX-XX-XX-XX-XX-XX, optional)

Source Port Range: – (1-65535, optional)

Destination Port Range: – (1-65535, optional)

Protocol: TCP ▼

Description: (1-50 characters)

Status: Enable

Specify the client and the network resources the client can visit by configuring the IP address, MAC address and service port, then click **OK**.

Name	Enter the name of the guest resource entry.
Type	Choose the guest resource type as Five Tuple Type.
Source IP Range	Specify the IP range of the client(s) by entering the network address and subnet mask bits. Only the specified clients can visit the guest resources.
Destination IP Range	Specify the IP range of the server(s) that provides the guest resources by entering the network address and subnet mask bits.
Source MAC Address	Enter the MAC address of the client.
Source Port Range	Enter the source service port range.
Destination Port Range	Enter the destination service port range.
Description	Enter a brief description for the Guest Resources entry to make it easier to search and manage.
Protocol	Specify the protocol as TCP or UDP for the Guest Resources.
Status	Check the box to enable the guest resource entry.

 **Note:**

In a Guest Resource entry, if some parameter is left empty, it means the gateway will not restrict that parameter. For example, if the source IP range is left empty, it means all the clients can visit the specified guest resources.

6.2 Configuring the URL Type

Choose the menu **Authentication > Authentication Settings > Guest Resources** and click **Add** to load the following page.

Figure 6-1 Configuring the URL

<input type="checkbox"/>	ID	Name	Type	Source IP Range	Destination IP Range	Source Port	Destination Port	Status	Operation
--	--	--	--	--	--	--	--	--	--

Name: (1-50 characters)

Type: URL Type ▼

URL Address: (1-128 characters)

Source IP Range: / (Optional)

Source MAC Address: (XX-XX-XX-XX-XX-XX, optional)

Source Port Range: - (1-65535, optional)

Description: (1-50 characters)

Status: Enable

Specify the client and the network resources the client can visit by configuring the URL of the network resource and the parameters of the clients, then click **OK**.

Name	Enter the name of the guest resource entry.
Type	Choose the guest resource type as URL Type.
URL Address	Enter the URL address or IP address of the network resource that can be visited for free.
Source IP Range	Configure the IP range of the client(s) by entering the network address and subnet mask bits.
Source MAC Address	Enter the MAC address of the client.
Source Port Range	Enter the source service port range.

Description	Enter a brief description for the Guest Resources entry to make it easier to search and manage.
--------------------	---

Status	Check the box to enable the guest resource entry.
---------------	---

 **Note:**

In a Guest Resource entry, if some parameter is left empty, it means the gateway will not restrict that parameter. For example, if the source IP range is left empty, it means all the clients can visit the specified guest resources.

7 Configuring LDAP Profiles

The Lightweight Directory Access Protocol (LDAP) is an industry standard protocol for maintaining and accessing directory information over a network. LDAP Authentication allows you to bind the device to an LDAP server and use that server to authenticate LAN clients.

Choose the menu **Authentication > LDAP > LDAP Profiles**, click **Add** to load the following page.

Figure 7-1 Configuring the Web Authentication




Name	Specify the name of the LDAP profile..
Status	Check the box to enable LDAP Authentication.
Bind Type	Select the LDAP Authentication mode: Anonymous Mode, Simple Mode, or Regular Mode.
Server Address	Enter the Host name or IP address of the LDAP server.
Destination Port	Enter the port ID of the LDAP server. By default, the port ID is 389 when SSL is disabled and 636 when SSL is enabled.
Use SSL	Determine whether to use SSL for LDAP communication.

Regular DN	Specify the distinguished name (DN) of the administrator account. This parameter is required in Regular mode.
Regular Password	Specify the password of the administrator account. This parameter is required in Regular mode.
Common Name Identifier	Specify the common name for user authentication. It is usually "cn".
Base Distinguished Name	Specify the user identifier for user authentication. You can click the icon next to it to search and select from the LDAP directory tree.
Additional Filter	Specify the filter for user authentication. It is not supported in Simple Mode and is optional in other modes.
Group Distinguished Name	Specify the group identifier for user authentication. It is not supported in Simple Mode and is optional in other modes.

8 Viewing the Authentication Status

Choose the menu **Authentication > Authentication Status > Authentication Status** to load the following page.

Figure 8-1 Viewing the Authentication Status

Authenticated User List							
Entry Count: 1							 Refresh  Offline
<input type="checkbox"/>	ID	Type	Starting Time	IP Address	MAC Address	Operation	
<input type="checkbox"/>	1	Local Authentication	2017-1-1 1:10:54	192.168.0.197	74-D4-35-9F-DB-1C		

Here you can view the clients that pass the portal authentication.

Type	Displays the authentication type of the client.
Starting Time	Displays the starting time of the authentication.
IP Address	Displays the client's IP address.
MAC Address	Displays the client's MAC address.

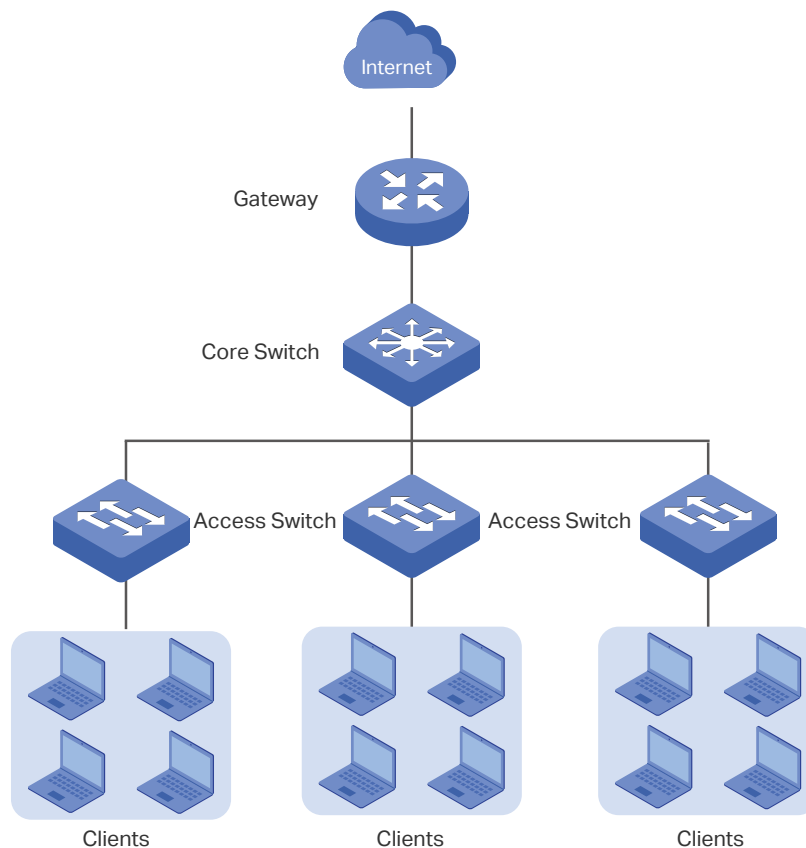
9 Configuration Example

Here we take the application of Local Authentication as an example.

9.1 Network Requirements

A hotel needs to offer internet service to the guests and push hotel advertisement. For network security, only the authorized guests can access the internet.

Figure 9-1 Network Topology



9.2 Configuration Scheme

For the hotel does not have an external Web server or Authentication server, it is recommended to choose Local Authentication to meet this requirement.

- To control the guests' internet access, you can create local user accounts for the guests. The guests need to use the accounts assigned to them to get authenticated, then can visit the internet. The other people cannot visit the internet through the hotel's network without authentication accounts.

- To push hotel advertisement, you can simply customize the authentication page by set the background picture and the welcome information.

9.3 Configuration Procedures

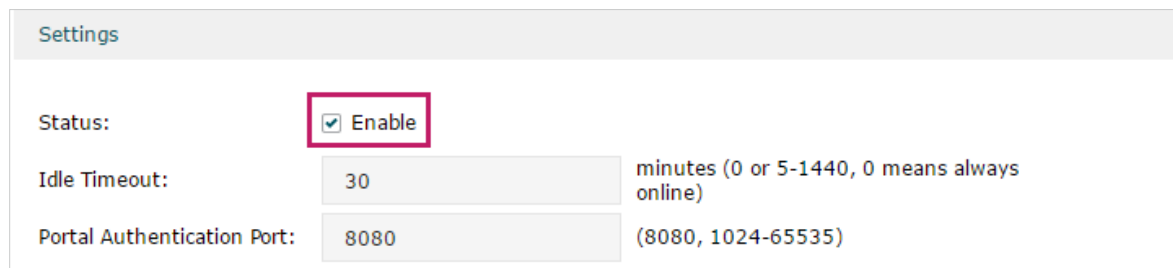
- 1) Enable Portal Authentication, choose the authentication type as Local Authentication, and customize the authentication page.
- 2) Create the authentication accounts for the guests.

9.3.1 Configuring the Authentication Page

Choose the menu **Authentication > Authentication Settings > Web Authentication** to load the following page.

- 1) Enable portal authentication, and keep the Idle Timeout and Portal Authentication Port as default settings.

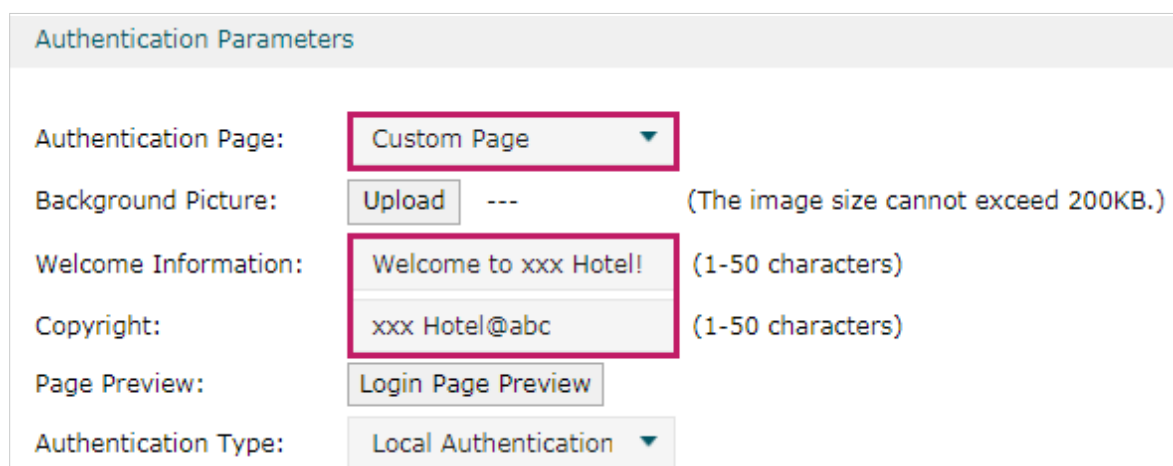
Figure 9-2 Enable Portal Authentication



Settings		
Status:	<input checked="" type="checkbox"/> Enable	
Idle Timeout:	30	minutes (0 or 5-1440, 0 means always online)
Portal Authentication Port:	8080	(8080, 1024-65535)

- 2) Choose the Authentication Page as Custom page, pick a picture of the hotel as the background picture on the authentication page, and specify the welcome information and copyright.

Figure 9-3 Customize the authentication page



Authentication Parameters		
Authentication Page:	Custom Page	
Background Picture:	Upload ---	(The image size cannot exceed 200KB.)
Welcome Information:	Welcome to xxx Hotel!	(1-50 characters)
Copyright:	xxx Hotel@abc	(1-50 characters)
Page Preview:	Login Page Preview	
Authentication Type:	Local Authentication	

- 3) Choose the Authentication Type as Local Authentication, and configure the parameters of expiration reminder. Then click **Save**.

Figure 9-4 Configure the authentication type and expiration reminder

9.3.2 Configuring Authentication Accounts for the Guests

Choose the menu **Authentication > User Management > User Management** to load the following page.

Here we take the configuration of Formal User account as an example. We create an account for the guests of room 101. The username is Room101 and the password is 123456, and at most three guests can use this account to authenticate. Then click **OK**.

Figure 9-5 Configure the Account for the guests

<input type="checkbox"/>	ID	User Type	Username	Authentication Timeout	MAC Address	Description	Status	Operation
--	--	--	--	--	--	--	--	--

User Type: Formal User ▼

Username: Room101 (1-100 Characters)

Password: 123456 (1-100 Characters)

Expiration Date: 2017-12-31 (YYYY-MM-DD)

Authentication Period: 00:00-24:00 (HH:MM-HH:MM)

MAC Binding Type: No Binding ▼

Maximum Users: 3 (1-1024)

Upstream Bandwidth: 0 Kbps (0 or 10-1,000,000. 0 means no limit)

Downstream Bandwidth: 0 Kbps (0 or 10-1,000,000. 0 means no limit)

Name: (1-50 characters, optional)

Telephone: (1-50 characters, optional)

Description: (1-50 characters, optional)

Status: Enable

OK Cancel

After all the configuration finished, the guest can use the account to authenticate and access the internet after the authentication succeeded.

Part 12

Managing Services

CHAPTERS

1. Services
2. Dynamic DNS Configurations
3. UPnP Configuration
4. Configuration Example for Dynamic DNS
5. mDNS Configuration
6. Reboot Schedule
7. DNS Proxy

1 Services

1.1 Overview

The Services module incorporates two functions, Dynamic DNS (DDNS) and UPnP (Universal Plug and Play) to provide convenient network services.

1.2 Support Features

Dynamic DNS

Nowadays, network protocols such as PPPoE and DHCP are widely employed by ISPs to assign public IP addresses to users. The use of these protocols can cause the user's public IP address to change dynamically. DDNS is an internet service that ensures a fixed domain name can be used to access a network with a varying public IP address. This means the user's network can be more easily accessed by internet hosts.

UPnP

With the development of networking and advanced computing techniques, greater numbers of devices feature in networks. UPnP is designed to solve the problem of communication between these network devices. UPnP function allows devices dynamically discover and communicate with each other without additional configurations. For example, it allows the download of P2P software without opening ports.

mDNS

mDNS (Multicast DNS) Repeater can help mDNS request/reply packets spread across different network segments. With this function, services published using the mDNS protocol can be discovered across network segments.

Reboot Schedule

In Reboot Schedule, you can set schedules to reboot the connected devices periodically based on needs. You can configure the reboot schedule flexibly by creating multiple entries.

DNS Proxy

DNS Proxy provides the LAN side clients with the DNS query service. It forwards the DNS request from the LAN side clients to the selected upstream DNS server and forwards the DNS reply accordingly.

2 Dynamic DNS Configurations

With Dynamic DNS configurations, you can:

- Configure and view Peanuthull DDNS
- Configure and view Comexe DDNS
- Configure and view DynDNS
- Configure and view NO-IP DDNS

2.1 Configure and View Peanuthull DDNS

Choose the menu **Service > Dynamic DNS > Peanuthull** and click **Add** to load the following page.

Figure 2-1 Configure Peanuthull DDNS

<input type="checkbox"/>	ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Service Type	Operation
--	--	--	--	--	--	--	--	--	--

Interface:

Account Name: [Go to register](#)

Password:

Update Interval:

Status: Enable

Follow these steps to configure Peanuthull DDNS.

- 1) Click **Go to register** to visit the official website of Peanuthull, register an account and a domain name.
- 2) Configure the following parameters and click **OK**.

Interface	Select the interface for the DDNS service.
Account Name	Enter the account name of your DDNS account. You can click Go to register to visit the official website of Peanuthull to register an account.
Password	Enter the password of your DDNS account.
Update Interval	Specify the Update Interval that the device dynamically updates IP addresses for registered domain names.
Status	Check the box to enable the DDNS service.

3) View the DDNS status.

Figure 2-2 View the Status of Peanuthull DDNS

Peanuthull

+ Add - Delete

<input type="checkbox"/>	ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Service Type	Operation
<input type="checkbox"/>	1	WAN1	user1	6 hours	Enabled ✖	Offline	---	---	

Status Displays whether the corresponding DDNS service is enabled.

Service Status Displays the current status of DDNS service.

Offline: DDNS service is offline.

Connecting: DDNS client is connecting to the server.

Online: DDNS is working normally.

Incorrect account name or password: The account name or password is incorrect.

Domain Name Displays the Domain Names obtained from the DDNS server.

Service Type Displays the DDNS service type, including Professional service and Standard service.

2.2 Configure and View Comexe DDNS

Choose the menu **Service > Dynamic DNS > Comexe** and click **Add** to load the following page.

Figure 2-3 Configure Comexe DDNS

<input type="checkbox"/>	ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Operation
--	--	--	--	--	--	--	--	--

Interface: ---

Account Name: [Go to register](#)

Password:

Update Interval: ---

Status: Enable

Follow these steps to configure Comexe DDNS.

- 1) Click **Go to register** to visit the official website of Comexe, register an account and a domain name.

2) Configure the following parameters and click **OK**.

Interface	Select the interface for the DDNS service.
Account Name	Enter the account name of your DDNS account. You can click Go to register to visit the official website of Comexe to register an account.
Password	Enter the password of your DDNS account.
Update Interval	Specify the Update Interval that the device dynamically updates IP addresses for registered domain names.
Status	Check the box to enable the DDNS service.

3) View the DDNS status.

Figure 2-4 View the Status of Comexe DDNS

Comexe + Add - Delete

<input type="checkbox"/>	ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Operation
<input type="checkbox"/>	1	WAN1	user1	6 hours	Enabled ✖	Connecting	---	

Status Displays whether the corresponding DDNS service is enabled.

Service Status Displays the current status of DDNS service.

Offline: DDNS service is offline.

Connecting: DDNS client is connecting to the server.

Online: DDNS is working normally.

Incorrect account name or password: The account name or password is incorrect.

Domain Name Displays the Domain Names obtained from the DDNS server.

2.3 Configure and View DynDNS

Choose the menu **Service > Dynamic DNS > DynDNS** and click **Add** to load the following page.

Figure 2-5 Configure DynDNS

<input type="checkbox"/>	ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Operation
--	--	--	--	--	--	--	--	--

Interface:

Account Name: [Go to register](#)

Password:

Domain Name:

Update Interval:

Status: Enable

Follow these steps to configure DynDNS.

- 1) Click **Go to register** to visit the official website of DynDNS and register an account and a domain name.
- 2) Configure the following parameters and click **OK**.

Interface	Select the interface for the DDNS service.
Account Name	Enter the account name of your DDNS account. You can click Go to register to visit the official website of DynDNS to register an account.
Password	Enter the password of your DDNS account.
Domain Name	Specify the domain name that you registered with your DDNS service provider.
Update Interval	Specify the Update Interval that the device dynamically updates IP addresses for registered domain names.
Status	Check the box to enable the DDNS service.

- 3) View the DDNS status.

Figure 2-6 View the Status of DynDNS

DynDNS + Add - Delete

<input type="checkbox"/>	ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Operation
<input type="checkbox"/>	1	WAN1	user1	6 hours	Enabled ✖	Connecting	domainname1.com	

Status	Displays whether the corresponding DDNS service is enabled.
---------------	---

Service Status	<p>Displays the current status of DDNS service.</p> <p>Offline: DDNS service is offline.</p> <p>Connecting: DDNS client is connecting to the server.</p> <p>Online: DDNS is working normally.</p> <p>Incorrect account name or password: The account name or password is incorrect.</p> <p>Incorrect domain name: The domain name is incorrect.</p>
Domain Name	<p>Displays the Domain Names obtained from the DDNS server.</p>

2.4 Configure and View NO-IP DDNS

Choose the menu **Service > Dynamic DNS > NO-IP** and click **Add** to load the following page.

Figure 2-7 View NO-IP DDNS

<input type="checkbox"/>	ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Operation
--	--	--	--	--	--	--	--	--

Interface:

Account Name: [Go to register](#)

Password:

Domain Name:

Update Interval:

Status: Enable

Follow these steps to configure NO-IP DDNS.

- 1) Click **Go to register** to visit the official website of NO-IP and register an account and a domain name.
- 2) Configure the following parameters and click **OK**.

Interface	Select the interface for the DDNS service.
Account Name	Enter the account name of your DDNS account. You can click Go to register to visit the official website of NO-IP to register an account.
Password	Enter the password of your DDNS account.
Domain Name	Specify the domain name that you registered with your DDNS service provider.

Update Interval	Specify the Update Interval that the device dynamically updates IP addresses for registered domain names.
Status	Check the box to enable the DDNS service.

3) View the DDNS status.

Figure 2-8 View the Status of NO-IP DDNS

NO-IP

+ Add - Delete

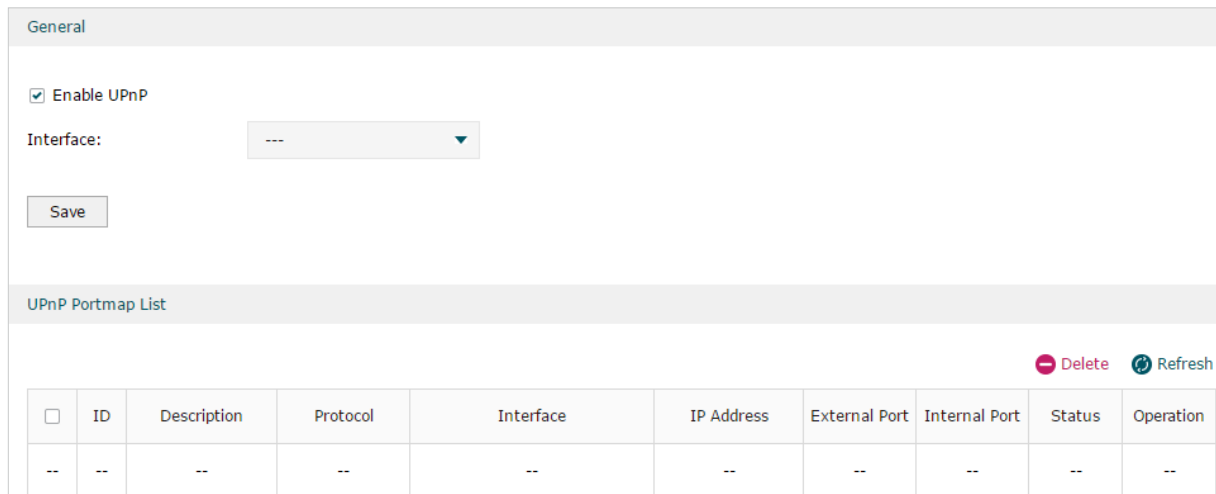
<input type="checkbox"/>	ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Operation
<input type="checkbox"/>	1	WAN1	user1	6 hours	Enabled ✘	Connecting	domainname1.com	

Status	Displays whether the corresponding DDNS service is enabled.
Service Status	<p>Displays the current status of DDNS service.</p> <p>Offline: DDNS service is offline.</p> <p>Connecting: DDNS client is connecting to the server.</p> <p>Online: DDNS is working normally.</p> <p>Incorrect account name or password: The account name or password is incorrect.</p> <p>Incorrect domain name: The domain name is incorrect.</p>
Domain Name	Displays the Domain Names obtained from the DDNS server.

3 UPnP Configuration

Choose the menu **Service > UPnP** to load the following page.

Figure 3-1 Configure UPnP Function



Follow these steps to configure UPnP function:

- 1) In the **General** section, enable the UPnP function and select the interface. Then click **Save**.

Enable UPnP	Check the box to enable the UPnP function.
Interface	Select the interface for the UPnP function.

- 2) (Optional) In the **UPnP Portmap List** section, view the portmap list.

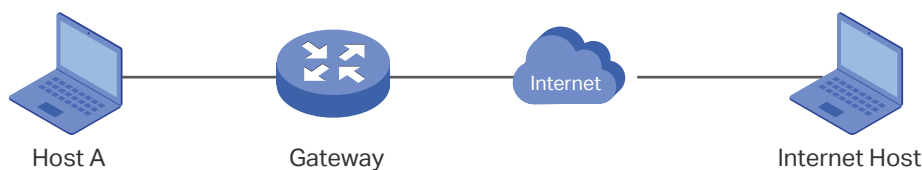
Description	Displays the description of the application using UPnP protocol.
Protocol	Displays the protocol type used in the process of UPnP.
Interface	Displays the interface used in the process of UPnP.
IP Address	Displays the IP address of the local host.
External Port	Displays the external port that is opened for the application by the gateway.
Internal Port	Displays the internal port that is opened for the application by the local host.
Status	Displays the status of the corresponding UPnP entry. Enabled: The mapping is active. Disabled: The mapping is inactive.

4 Configuration Example for Dynamic DNS

4.1 Network Requirement

Host A gets internet services from an ISP (Internet Service Provider) via a PPPoE dial-up connection. The user wants to visit the gateway's web management interface using another host on the internet.

Figure 4-1 Network Topology



4.2 Configuration Scheme

For security management, the internet hosts attempting to manage the gateway must be permitted by the gateway. Remote Management is used to manage the IP addresses of these hosts.

Because the user uses PPPoE to access the network, the public IP address of the gateway may be changed each time the dial-up connection is established. When the public IP address of the gateway changes, DDNS service ensures the DNS server rebinds the current domain name to the new IP address. This means the user can always reach the gateway using the same domain name, even if the public IP address has been changed.

4.3 Configuration Procedure

4.3.1 Specifying the IP Address of the Host

Before configuring DDNS, it is required to specify the IP address of the internet host for remote management. For details, go to **System Tools > Admin Setup > Remote Management** page.

4.3.2 Configuring the DDNS function

There are four DDNS servers supported by the gateway, we take Peanuthull DNS as an example here.

- 1) Choose the menu **Services > Dynamic DNS > Peanuthull** and click **Add** to load the following page. Click **Go to register** to register a domain name on the official website of Peanuthull.

Figure 4-2 Registering a Domain Name

Peanuthull

+ Add - Delete

<input type="checkbox"/>	ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Service Type	Operation
--	--	--	--	--	--	--	--	--	--

Interface:

Account Name: [Go to register](#)

Password:

Update Interval:

Status: Enable

- 2) Set the Interface as WAN1, set the Update Interval as 6 hours, and enter the Account Name and Password previously registered before. Click **OK**.

Figure 4-3 Specifying Peanuthull DDNS Parameters

Peanuthull

+ Add - Delete

<input type="checkbox"/>	ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Service Type	Operation
--	--	--	--	--	--	--	--	--	--

Interface:

Account Name: [Go to register](#)

Password:

Update Interval:

Status: Enable

5 mDNS Configuration

Enable Multicast DNS Repeater and specify the Forward Rules to determine the network segments that mDNS request/reply packets can cross, that is, the range of services that can be found across network segments. Bonjour is Apple’s open zero-configuration network standard based on the mDNS protocol, which can automatically discover computers, devices and services on the IP network.

Choose the menu **Services > mDNS**, click **Add** to load the following page.

Figure 5-1 Configure mDNS Function

- Multicast DNS Repeater Check the box to enable the function.
- Forward Rules Select one or multiple mDNS (Bonjour) rules for forwarding mDNS request/reply packets.
- Description Give a name to the rule.
- Service Network Select a network, then its mDNS reply packets will be forwarded by the gateway.
- Client Network Select a network, then its mDNS request packets will be forwarded by the gateway.
- Service Select the service type, then the traffic of these services can be forwarded by the gateway.

In **Services** section, click **Add** and manage the service types supported by mDNS.

Services

+ Add - Delete

<input type="checkbox"/>	ID	Name	Domain	Type	Operation
--	--	--	--	--	--
<div style="display: flex; justify-content: space-between;"> <div style="width: 60%;"> <p>Name: <input style="width: 100%;" type="text"/></p> <p>Domain: <input style="width: 100%;" type="text"/></p> </div> <div style="width: 35%; text-align: right;"> <input type="button" value="OK"/> <input type="button" value="Cancel"/> </div> </div>					
--	1	any	any	Default	
--	2	AirPlay	_airplay_tcp,_raop_tcp,_appletv-v2_tcp	Default	
--	3	AFP	_afpovertcp_tcp	Default	
--	4	BitTorrent	_bittorrent_tcp	Default	
--	5	FTP	_ftp_tcp,_sftp-ssh_tcp	Default	
--	6	iChat	_presence_tcp,_ichat_tcp	Default	
--	7	iTunes	_daap_tcp,_home-sharing_tcp,_apple-mobdev_tcp,_daap_tcp	Default	
--	8	Printers	_ipp_tcp,_pdl-datastream_tcp,_printer_tcp,_http_tcp,_http_alt_tcp,_ipp-tls_tcp,_fax-ipp_tcp,_riousbprint_tcp,_ica-networking_tcp,_ica-networking2_tcp,_ptp_tcp,_canon-bjnp1_tcp,_ipps_tcp	Default	
--	9	Samba	_smb_tcp,_smbdirect_tcp	Default	
--	10	Scanners	_ipp_tcp,_pdl-datastream_tcp,_scanner_tcp,_http_tcp,_http_alt_tcp,_ipp-tls_tcp,_fax-ipp_tcp,_riousbprint_tcp,_ica-networking_tcp,_ica-networking2_tcp,_ptp_tcp,_canon-bjnp1_tcp,_ipps_tcp	Default	

Name Enter a name to identify the service

Status Enter the domain of the service.

6 Reboot Schedule

In Reboot Schedule, you can set schedules to reboot the connected devices periodically based on needs. You can configure the reboot schedule flexibly by creating multiple entries.

Choose the menu **Services > Reboot Schedule**, click **Add** to load the following page.

Figure 6-1 Configure Reboot Schedule

<input type="checkbox"/>	ID	Name	Status	Next Execution	Operation
--	--	--	--	--	--

Name:

Status: Enable

Occurrence: Every on at : in Pacific Time.

Name Enter a name to identify the reboot schedule entry.

Status Click the checkbox to enable the reboot schedule entry.

Occurrence Specify the date and time for the devices to reboot.

7 DNS Proxy

DNS Proxy provides the LAN side clients with the DNS query service. It forwards the DNS request from the LAN side clients to the selected upstream DNS server and forwards the DNS reply accordingly.

DNSSEC (DNS Security Extensions), DoT (DNS over TLS), and DoH (DNS over Https) are three security options for DNS Proxy. DNSSEC will verify the integrity of DNS records, and DoT / DoH will encrypt the query.

All of the three options need an upstream DNS server that supports them.

7.1 DNSSEC

Choose the menu **Services > DNS Proxy > DNSSEC** to load the following page.

Figure 7-1 Configure DNSSEC

DNSSEC

DNSSEC: Enable

DNS Server: + Add

- Minus

Action for Bogus Replies: Pass Drop

Diagnose

Domain:

Type: IPv4 IPv6

DNS Server:

Result

ID	Domain Name	Type	IP Address	Verify Result
--	--	--	--	--

In **DNSSEC**, configure the following parameters.

DNSSEC Check the box to enable the function.

DNS Server Specify the IP address of the DNSSEC server. Up to 2 IP addresses can be configured.

Action for Bogus Replies Specify the action for processing DNS reply packets whose signature verification fails.

In **Diagnose** section, configure the following parameters.

Domain Specify the domain name you want to query.

Type Query the IPv4/IPv6 address corresponding to the domain name.

DNS Server Specify the upstream DNS server used.

Diagnose Click to diagnose the domain name and check the results.

There may be three diagnostic results:

Secure: The queried domain name has passed the DNSSEC signature verification.

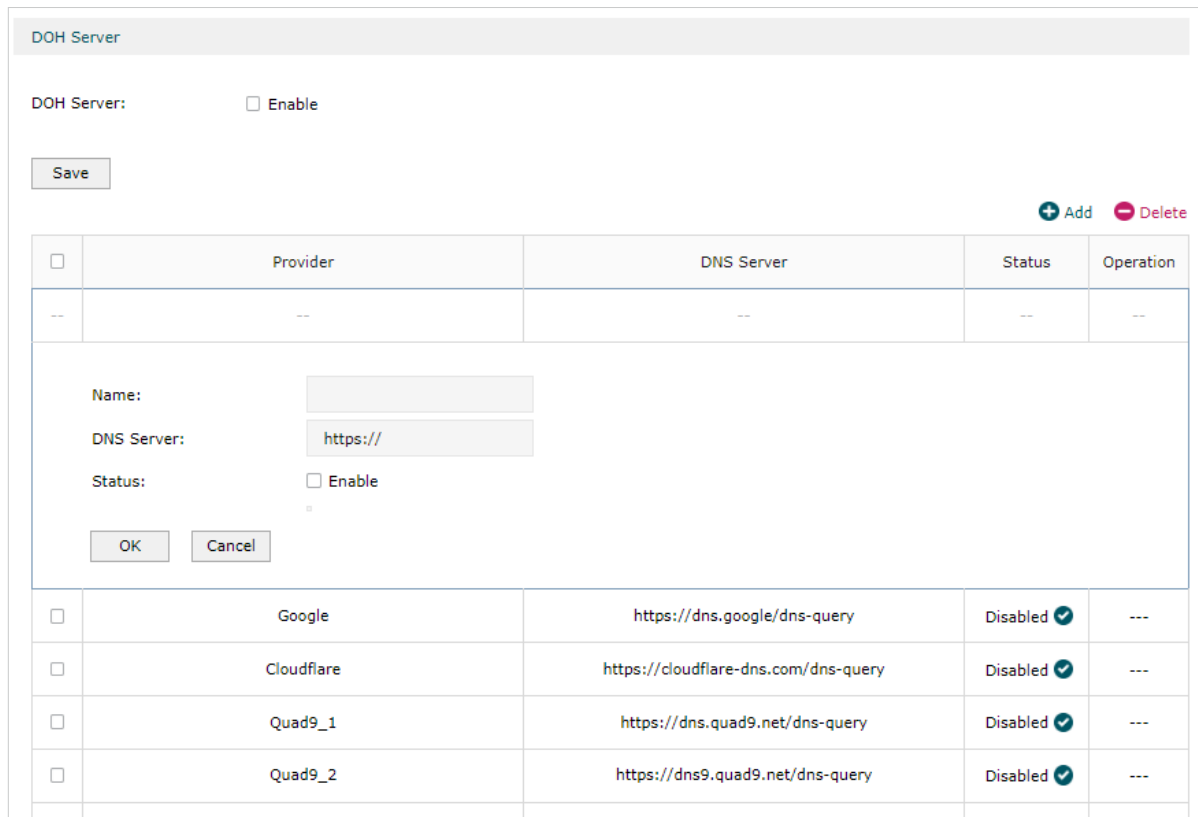
Bogus: The queried domain name has not passed the DNSSEC signature verification. The domain name authentication failed.

Insecure: The device cannot verify the DNSSEC signature of the queried domain name.

7.2 DOH

Choose the menu **Services > DNS Proxy > DOH** to load the following page.

Figure 7-2 Configure DOH



Enable the feature and click **Add** to create a new server entry.

DOH Server	Check the box to enable the DoH (DNS over Https) server.
Name	Specify the name of the server.
DNS Server	Specify the domain name of DNS Server. Only one server can be added.
Status	Specify whether to enable this server entry. Up to two server entries can be enabled at the same time.

7.3 DOT

Choose the menu **Services > DNS Proxy > DOT** to load the following page.

Figure 7-3 Configure DOT

The screenshot shows the 'DOT Server' configuration interface. At the top, there is a 'DOT Server' section with an 'Enable' checkbox and a 'Save' button. Below this is a table of existing server entries. A modal dialog is open for adding a new entry, with fields for Name, DNS Server, and Status, and 'Add', 'OK', and 'Cancel' buttons.

Provider	DNS Server	Status	Operation
--	--	--	--
Google	8.8.8.8 8.8.4.4	Disabled ✓	---
Quad9	9.9.9.9 9.9.9.10	Disabled ✓	---
Cloudflare	1.1.1.1 1.0.0.1	Disabled ✓	---
CleanBrowsing	185.228.168.9 185.228.169.9	Disabled ✓	---
OpenDNS	208.67.222.222 208.67.220.220	Disabled ✓	---

Enable the feature and click **Add** to create a new server entry.

DOT Server	Check the box to enable the DoT (DNS over TLS) server.
Name	Specify the name of the server.
DNS Server	Specify the IP address of DNS Server. Up to two servers can be added.

Status

Specify whether to enable this server entry. Up to two server entries can be enabled at the same time.

Part 13

System Tools

CHAPTERS

1. System Tools
2. Admin Setup
3. Controller Settings
4. Management
5. SNMP
6. Diagnostics
7. Time Settings
8. System Log

1 System Tools

1.1 Overview

The System Tools module provides several system management tools for users to manage the gateway.

1.2 Support Features

Admin Setup

Admin Setup is used to configure the parameters for users' login. With this function, you can modify the login account, specify the IP subnet and mask for remote access and specify the HTTP and HTTPS server port.

Management

The Management section is used to manage the firmware and the configuration file of the gateway. With this function, you can reset the gateway, backup and restore the configuration file, reboot the gateway and upgrade the firmware.

SNMP

SNMP (Simple Network Management Protocol) is a standard network management protocol. It helps network managers to configure and monitor network devices. With SNMP, network managers can view and modify network device information, detect and analyze network error, and so on. The gateway supports SNMPv1 and SNMPv2c.

Diagnostics

Diagnostics is used to detect network errors and equipment failures. With this function, you can test the connectivity of the network with ping or traceroute command and inspect the gateway under the help of technicians.

Time Settings

Time Settings is used to configure the system time and the daylight saving time.

System Log

System Log is used to view the system log of the gateway. You can also configure the gateway to send the log to a server.

2 Admin Setup

In Admin Setup module, you can configure the following features:

- Admin Setup
- Remote Management
- System Settings

2.1 Admin Setup

Choose the menu **System Tools > Admin Setup > Admin Setup** to load the following page.

Figure 2-1 Modifying the Admin Account

The screenshot shows a web form titled "Account" with the following fields and labels:

- Old Username:** (1-15 letters, digits or special characters)
- Old Password:** (6-15 letters, digits or special characters)
- New Username:** (1-15 letters, digits or special characters)
- New Password:** (6-15 letters, digits or special characters). Below this field are three radio buttons labeled "Low", "Middle", and "High".
- Confirm New Password:** (6-15 letters, digits or special characters)

A "Save" button is located at the bottom left of the form.

In the **Account** section, configure the following parameters and click **Save** to modify the admin account

Old Username	Enter the old username.
Old Password	Enter the old password.
New Username	Enter a new username.
New Password	Enter a new password.
Confirm New Password	Re-enter the new password for confirmation.

2.2 Remote Management

Choose the menu **System Tools > Admin Setup > Remote Management** and click **Add** to load the following page.

Figure 2-2 Configuring Remote Management

Remote Management

+ Add - Delete

<input type="checkbox"/>	ID	Subnet/Mask	Status	Operation
--	--	--	--	--

Subnet/Mask: /

Status: Enable

In the **Remote Management** section, configure the following parameters and click **OK** to specify the IP subnet and mask for remote management.

Subnet/Mask	Enter the IP Subnet and Mask of the remote host.
Status	Check the box to enable the remote management function for the remote host.

2.3 System Setting

Choose the menu **System Tools > Admin Setup > System Settings** to load the following page.

Figure 2-3 Configuring System Settings

Settings

HTTP Server Port: (80, 1024-65535)

Redirect HTTP to HTTPS

HTTPS Server Port: (443, 1024-65535)

HTTPS Server Status: Enable

Web Idle Timeout: minutes (5-60)

In the **Settings** section, configure the following parameters and click **Save**.

HTTP Server Port	Enter the http server port for web management. The port number should be different from other servers'. The default setting is 80. After changing the http server port, you should access the interface by using IP address and the port number in the format of 192.168.0.1:1600.
Redirect HTTP to HTTPS	Check the box to enable the function, then you will access the web management interface by HTTPS protocol instead of HTTP protocol.
HTTPS Server Port	Enter the https server port for web management. The port number should be different from other servers'. The default setting is 443. After changing the https server port, you should access the interface by using IP address and the port number in the format of https://192.168.0.1:1800.
HTTPS Server Status	Check the box to enable HTTPS Server.
Web Idle Timeout	Enter a session timeout time for the device. The web session will log out for security if there is no operation within the session timeout time.

3 Controller Settings

To make your controller adopt your gateway, make sure the gateway can be discovered by the controller. Controller Settings enable your gateway to be discovered in either of the following scenarios.

- If you are using Omada Cloud-Based Controller, [Enable Cloud-Based Controller Management](#).
- If your gateway and controller are located in the same network, LAN and VLAN, the controller can discover and adopt the gateway without any controller settings. Otherwise, you need to inform the gateway of the controller's URL/IP address, and one possible way is to [Configure Controller Inform URL](#).

For details about the whole procedure, refer to the User Guide of Omada SDN Controller. The guide can be found on the download center of our official website: <https://www.tp-link.com/support/download/>.

3.1 Enable Cloud-Based Controller Management

Choose the menu **System Tools > Controller Settings** page. In the Cloud-Based Controller Management section, enable Cloud-Based Controller Management and click **Save**. You can check the connection status on this page.

Figure 3-1 Cloud-Based Controller Management

 Enable'. A 'Save' button is located at the bottom left." data-bbox="151 556 913 757"/>

Cloud-Based Controller Management

Connection Status: Disabled

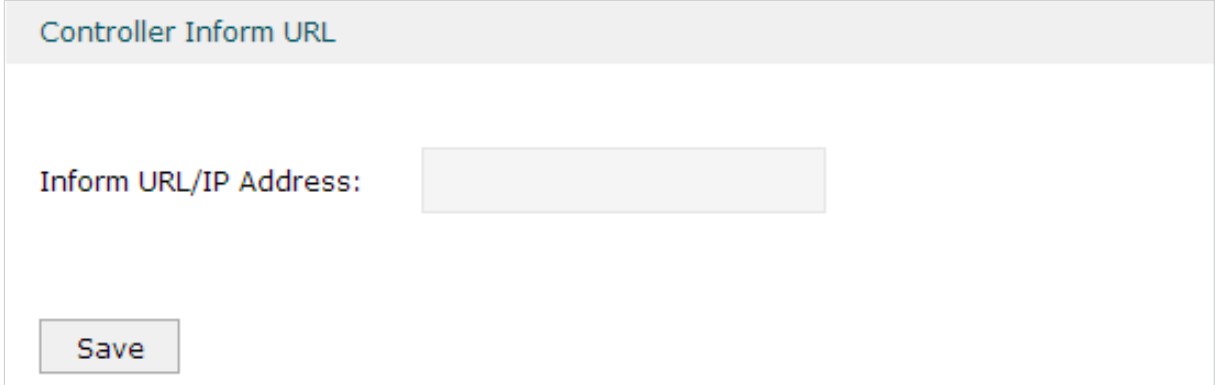
Cloud-Based Controller Management: Enable

Save

3.2 Configure Controller Inform URL

Choose the menu **System Tools > Controller Settings** page. In the Controller Inform URL section, inform the gateway of the controller's URL/IP address, and click **Save**. Then the gateway makes contact with the controller so that the controller can discover the gateway.

Figure 3-2 Cloud-Based Controller Management



The screenshot shows a web interface for configuring the Controller Inform URL. At the top, there is a header bar with the text "Controller Inform URL". Below this, the label "Inform URL/IP Address:" is followed by a text input field. At the bottom left of the form area, there is a "Save" button.

4 Management

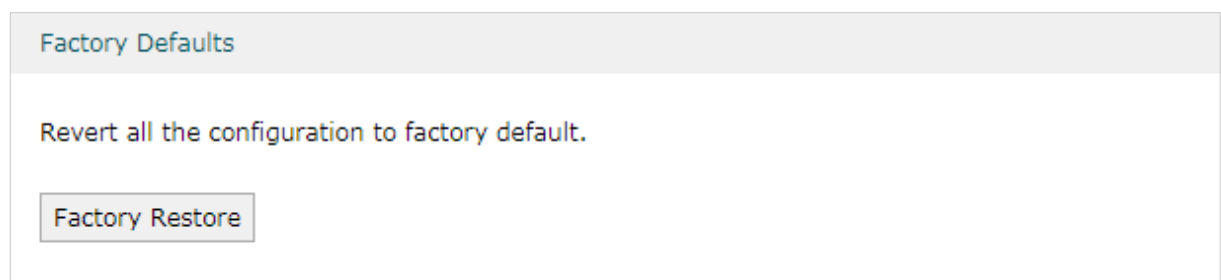
In Management module, you can configure the following features:

- Factory Default Restore
- Backup & Restore
- Reboot
- Firmware Upgrade

4.1 Factory Default Restore

Choose the menu **System Tools > Management > Factory Default Restore** to load the following page.

Figure 4-1 Resetting the Device

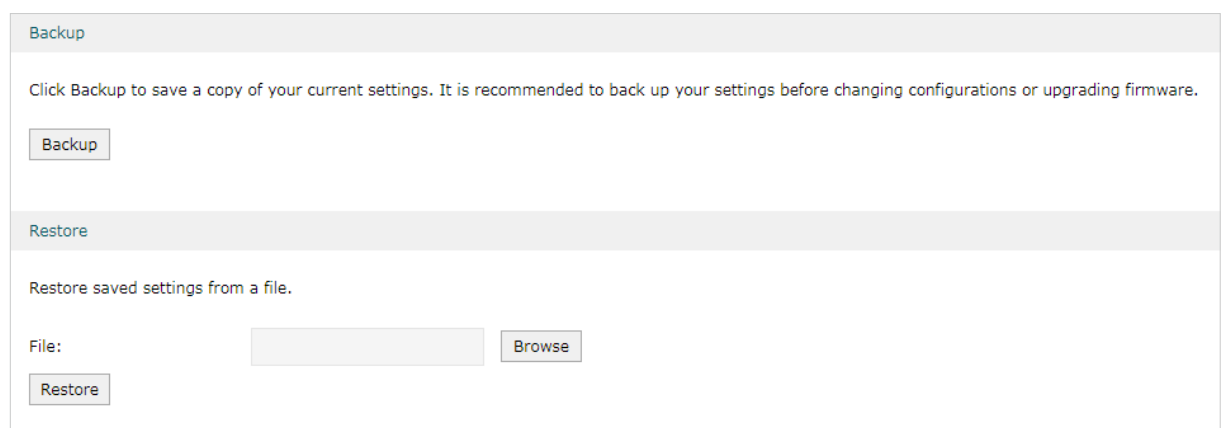


Click **Factory Restore** to reset the device.

4.2 Backup & Restore

Choose the menu **System Tools > Management > Backup & Restore** to load the following page.

Figure 4-2 Backup & Restore Page



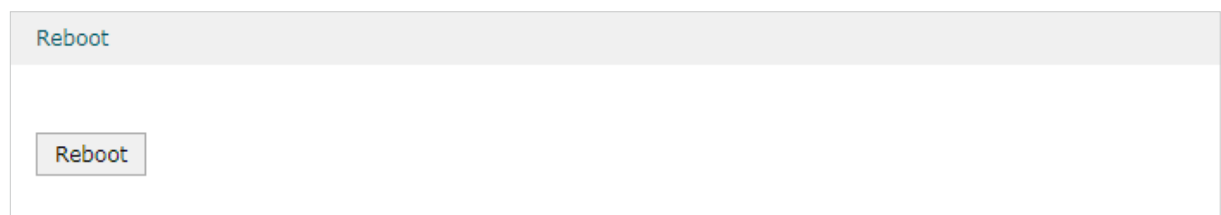
Choose the corresponding operation according to your need:

- 1) In the **Backup** section, click **Backup** to save your current configuration as a configuration file and export the file to the host.
- 2) In the **Restore** section, select one configuration file saved in the host and click **Restore** to import the saved configuration to your gateway.

4.3 Reboot

Choose the menu **System Tools > Management > Reboot** to load the following page.

Figure 4-3 Rebooting the Device

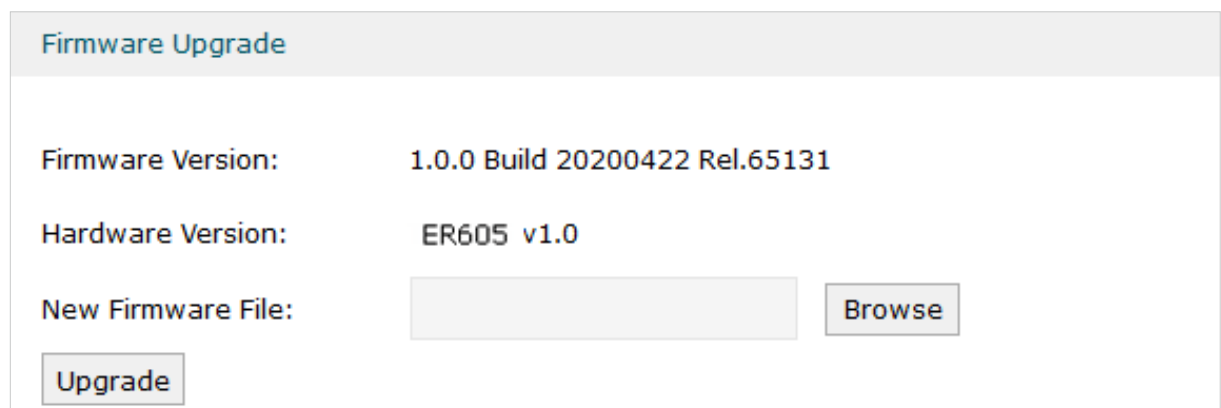


Click **Reboot** to reboot the device.

4.4 Firmware Upgrade

Choose the menu **System Tools > Management > Firmware Upgrade** to load the following page.

Figure 4-4 Configure System Settings



Select one firmware file and click **Upgrade** to upgrade the firmware of the device.

5 SNMP

Choose the menu **System Tools > SNMP > SNMP** to load the following page.

Figure 5-1 Configuring SNMP

The screenshot shows the SNMP configuration interface. At the top, the title 'SNMP' is displayed. Below it, there are several configuration fields:

- SNMP:** A checkbox labeled 'Enable' is checked.
- Contact:** A text input field containing 'www.tp-link.com'.
- Device Name:** A text input field containing 'ER605'.
- Location:** A text input field containing 'TP-Link'.
- Get Community:** A text input field containing 'public'.
- Get Trusted Host:** A text input field containing '0.0.0.0'.
- Set Community:** A text input field containing 'private'.
- Set Trusted Host:** A text input field containing '0.0.0.0'.

At the bottom left of the form, there is a 'Save' button.

Follow these steps to configure the SNMP function:

- 1) Check the box to enable the SNMP function.
- 2) Configure the following parameters and click **Save**.

Contact	Enter the textual identification of the contact person for this the device, for example, contact or e-mail address.
Device Name	Enter a name for the device.
Location	Enter the location of the device. For example, the name can be composed of the building, floor number, and room location.
Get Community	Specify the community that has read-only access to the device's SNMP information.
Get Trusted Host	Enter the IP address that can serve as Get Community to read the SNMP information of this device.
Set Community	Specify the community who has the read and write right of the device's SNMP information.
Set Trusted Host	Enter the IP address that can serve as Set Community to read and write the SNMP information of this device.

6 Diagnostics

In Diagnostics module, you can configure the following features:

- Diagnostics
- Remote Assistance

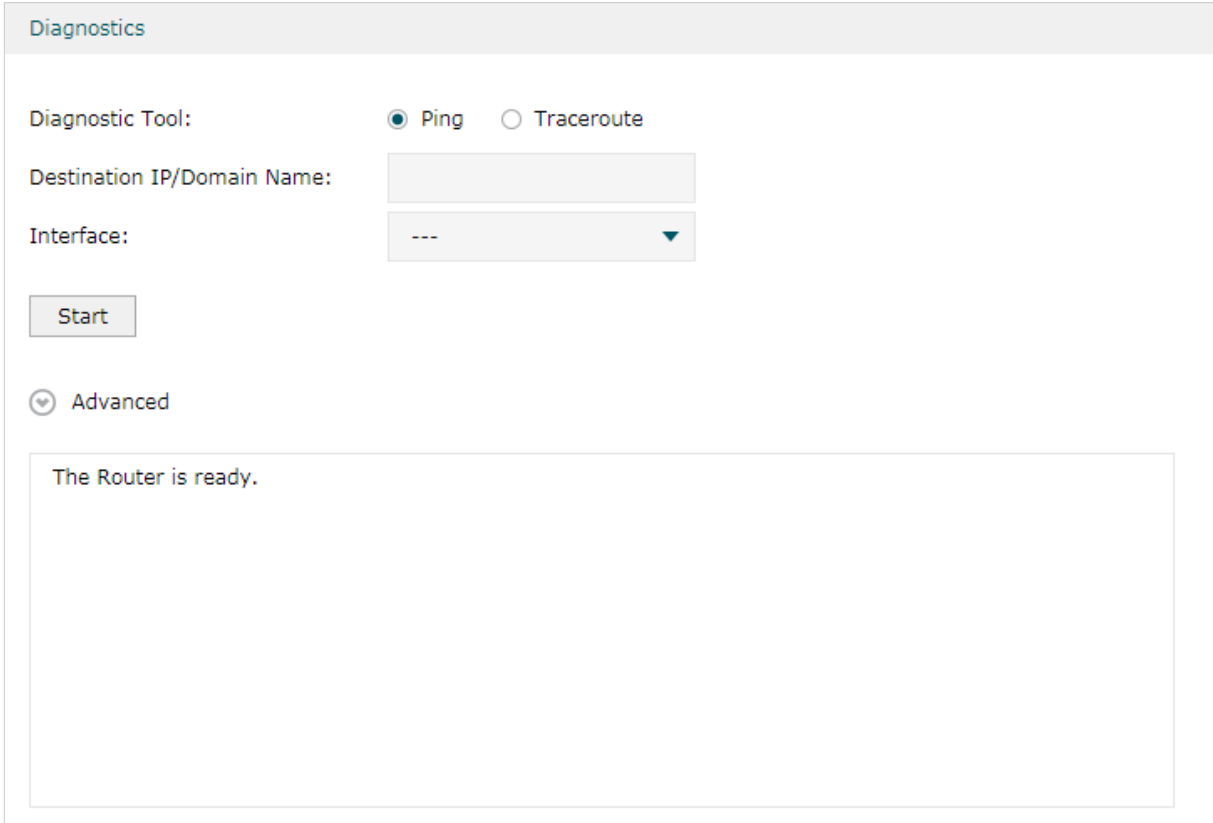
6.1 Diagnostics

Ping and traceroute are both used to test the connectivity between two devices in the network. In addition, ping can show the roundtrip time between the two devices directly and traceroute can show the IP address of gateways along the route path.

6.1.1 Configuring Ping

Choose the menu **System Tools > Diagnostics > Diagnostics** to load the following page.

Figure 6-1 Configuring Diagnostics



Diagnostics

Diagnostic Tool: Ping Traceroute

Destination IP/Domain Name:

Interface:

Start

Advanced

The Router is ready.

Follow these steps to configure Diagnostics:

- 1) In **Diagnostics** section, select **Ping** and configure the following parameters.

Diagnostics Tool Select **Ping** to test the connectivity between the gateway and the desired device.

Destination IP/ Domain Name	Enter the IP address or the domain name that you want to ping or tracet.
Interface	Select the interface that sends the detection packets.

2) (Optional) Click **Advanced** and the following section will appear.

Figure 6-2 Advanced Parameters for Ping Method

⊕

Ping Count: (1-50)

Ping Packet Size: (4-1472 Bytes)

Ping Count	Specify the count of the test packets to be sent during the ping process.
Ping Packet Size	Specify the size of the test packets to be sent during the ping process.

3) Click **Start**.

6.1.2 Configuring Traceroute

Choose the menu **System Tools > Diagnostics > Diagnostics** to load the following page.

Figure 6-3 Configuring Diagnostics

Diagnostics

Diagnostic Tool: Ping Traceroute

Destination IP/Domain Name:

Interface: ▼

⊖ Advanced

The Router is ready.

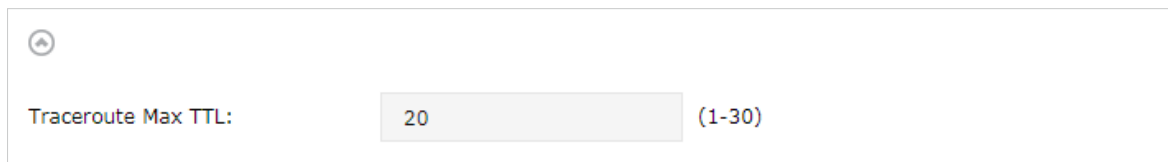
Follow these steps to configure Diagnostics:

- 1) In **Diagnostics** section, select **Traceroute** and configure the following parameters.

Diagnostic Tool	Select Traceroute to test the connectivity between the gateway and the desired device.
Destination IP/ Domain Name	Enter the IP address or the domain name that you want to ping or tracet.
Interface	Select the interface that sends the detection packets.

- 2) (Optional) Click **Advanced** and the following section will appear.

Figure 6-4 Advanced Parameters for Traceroute Method



Traceroute MAX TTL	Specify the traceroute max TTL (Time To Live) during the traceroute process. It is the maximum number of the route hops the test packets can pass through.
---------------------------	--

- 3) Click **Start**.

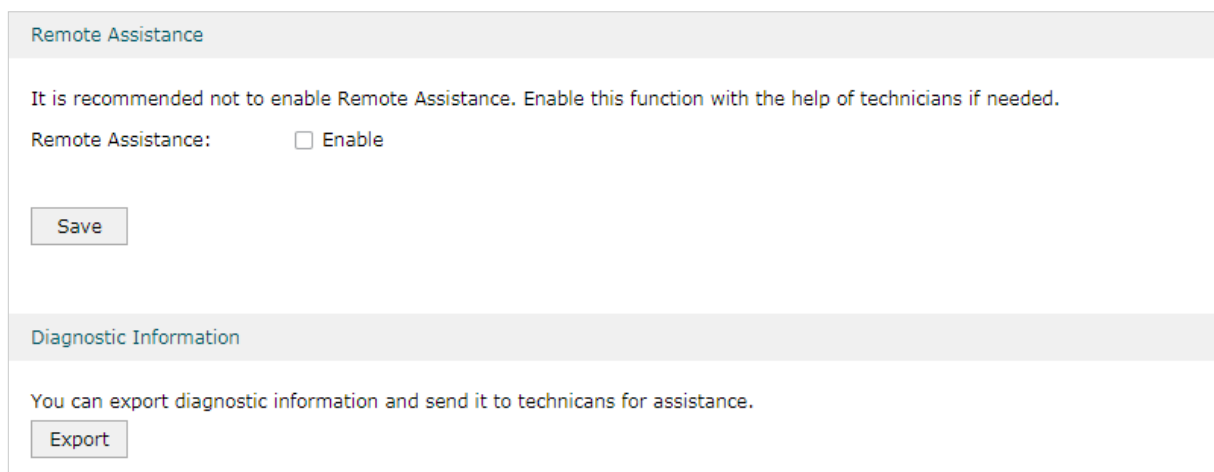
6.2 Remote Assistance

Note:

Please make contact with the technicians before trying to use this function.

Choose the menu **System Tools > Diagnostics > Remote Assistance** to load the following page.

Figure 6-5 Remote Assistance Page



- 1) In the **Remote Assistance** section, check the box and click **Save** to enable the remote assistance function and then the technicians can access your gateway and help to solve the problems by SSH.
- 2) In the **Diagnostic Information** section, click **Export** to download a binary (.bin) file containing helpful information, and send it to the technicians for help.

7 Time Settings

In Time Settings module, you can configure the following features:

- System Time
- Daylight Saving Time

7.1 Setting the System Time

Choose one method to set the system time.

7.1.1 Getting time from the Internet Automatically

Choose the menu **System Tools > Time Settings > Time Settings** to load the following page.

Figure 7-1 Getting Automatically from the Internet

The screenshot shows the 'Time Settings' configuration interface. It includes the following fields and options:

- Current Time :** 01/01/2017 03:31:00
- Time Config:** Get automatically from the Internet Manually
- Time Zone:** (GMT-08:00) Pacific Time (dropdown menu)
- Primary NTP Server:** 0.0.0.0
- Secondary NTP Server:** 0.0.0.0 (X.X.X.X, optional)
- Save** button

In the **Time Settings** section, configure the following parameters and click **Save**.

Current Time	Displays the current system time.
Time Config	Select Get automatically from the Internet to get the system time from the NTP server.
Time Zone	Select the time zone the device is in.
Primary NTP Server	Enter the IP address of the Primary NTP server.
Secondary NTP Server	Enter the IP address of the Secondary NTP server.

7.1.2 Setting the System Time Manually

Choose the menu **System Tools > Time Settings > Time Settings** to load the following page.

Figure 7-2 Setting the System Time Manually

The screenshot shows the 'Time Settings' configuration interface. At the top, it displays the 'Current Time' as 01/01/2017 03:44:07. Below this, the 'Time Config' section has two radio buttons: 'Get automatically from the Internet' (unselected) and 'Manually' (selected). The 'Date' field is a text input containing '01/01/2017' with a '(MM/DD/YYYY)' label. The 'Time' field consists of three dropdown menus for hours (03), minutes (26), and seconds (44), with a '(HH/MM/SS)' label. At the bottom, there is a checkbox labeled 'Synchronize with PC's Clock' and a 'Save' button.

In the **Time Settings** section, configure the following parameters and click **Save**.

Current Time	Displays the current system time.
Time Config	Select Manually to set the system time manually.
Date	Specify the date of the system.
Time	Specify the time of the system.
Synchronize with PC's Clock	Synchronize the system time of the gateway with PC's clock.

7.2 Setting the Daylight Saving Time

Choose one method to set the daylight saving time.

7.2.1 Predefined Mode

Choose the menu **System Tools > Time Settings > Time Settings** to load the following page.

Figure 7-3 Predefined Mode Page

Daylight Saving Time

DST Status: Enable

Mode: Predefined Mode Recurring Mode Date Mode

Predefined Country: Europe ▼

Save

In the **Daylight Saving Time** section, select one predefined DST schedule and click **Save**.

DST Status	Check the box to enable the DST function.
Mode	Select Predefined Mode to choose a predefined daylight saving time.
USA	Select the Daylight Saving Time of the USA. It is from 2:00 a.m. on the Second Sunday in March to 2:00 a.m. on the First Sunday in November
Europe	Select the Daylight Saving Time of Europe. It is from 1:00 a.m. on the Last Sunday in March to 1:00 a.m. on the Last Sunday in October.
Australia	Select the Daylight Saving Time of Australia. It is from 2:00 a.m. on the First Sunday in October to 3:00 a.m. on the First Sunday in April.
New Zealand	Select the Daylight Saving Time of New Zealand. It is from 2:00 a.m. on the Last Sunday in September to 3:00 a.m. on the First Sunday in April.

7.2.2 Recurring Mode

Choose the menu **System Tools > Time Settings > Time Settings** to load the following page.

Figure 7-4 Recurring Mode Page

Daylight Saving Time

DST Status: Enable

Mode: Predefined Mode Recurring Mode Date Mode

Time Offset: 60 minutes (1-180)

Starting Time: Last ▼ Sun ▼ in Mar ▼ at 01 ▼ : 00 ▼

Ending Time: Last ▼ Sun ▼ in Oct ▼ at 01 ▼ : 00 ▼

Save

In the **Daylight Saving Time** section, configure the following parameters and click **Save**.

DST Status	Check the box to enable the DST function.
Mode	Select Recurring Mode to specify a cycle time range for the daylight saving time. This configuration will take effect every year.
Time Offset	Specify the time added in minutes when Daylight Saving Time takes effect.
Starting Time	Specify the starting time of Daylight Saving Time. The starting time is relative to standard time.
Ending Time	Specify the ending time of Daylight Saving Time. The ending time is relative to daylight saving time.

7.2.3 Date Mode

Choose the menu **System Tools > Time Settings > Time Settings** to load the following page.

Figure 7-5 Date Mode Page

Daylight Saving Time

DST Status: Enable

Mode: Predefined Mode Recurring Mode Date Mode

Time Offset: minutes (1-180)

Starting Time: - - at :

Ending Time: - - at :

In the **Daylight Saving Time** section, select one predefined DST schedule and click **Save**.

DST Status	Check the box to enable the DST function.
Mode	Select Date Mode to specify an absolute time range for the daylight saving time.
Time Offset	Specify the time added in minutes when Daylight Saving Time takes effect.
Starting Time	Specify the starting time of Daylight Saving Time. The starting time is relative to standard time.
Ending Time	Specify the ending time of Daylight Saving Time. The ending time is relative to daylight saving time.

8 System Log

Choose the menu **System Tools > System Log > System Log** to load the following page.

Figure 8-1 System Log Page

Log Settings

Enable Auto-refresh
 Severity

All Level ▼

Send Log
 Server IP:

0.0.0.0

Save

Log List

↻ Refresh
 ✖ Delete All

ID	Time	Module	Level	Content
1	2017-01-01 16:48:45	WEB	NOTICE	192.168.0.200 Has logged in to web management system successfully!
2	2017-01-01 16:47:37	WEB	NOTICE	192.168.0.200 Has logged in to web management system successfully!
3	2017-01-01 15:37:23	WEB	NOTICE	192.168.0.200 Has logged in to web management system successfully!
4	2017-01-01 15:27:04	WEB	NOTICE	192.168.0.200 Has logged in to web management system successfully!
5	2017-01-01 01:47:17	WEB	NOTICE	192.168.0.200 Has logged in to web management system successfully!
6	2017-01-01 00:10:12	WEB	NOTICE	192.168.0.200 Has logged in to web management system successfully!
7	2017-01-01 00:07:12	WEB	NOTICE	192.168.0.200 Has logged in to web management system successfully!
9	2017-01-01 00:01:39	WEB	NOTICE	192.168.0.200 Has logged in to web management system successfully!
10	2017-01-01 00:01:38	WEB	NOTICE	192.168.0.200 Has logged in to web management system successfully!
11	2017-01-01 00:00:30	DHCP Client	NOTICE	WAN2:DHCP releasing IP address 192.68.12.32 succeeded.
12	2017-01-01 00:00:30	DHCP Client	NOTICE	WAN1:DHCP releasing IP address 0.0.0.0 succeeded.
13	2017-01-01 00:00:04	DHCP Client	NOTICE	WAN2:DHCP releasing IP address 192.68.12.32 succeeded.

Save Log

Follow these steps to view the system log:

- 1) In the **Log Settings** section, configure the following parameters and click **Save**.

Enable Auto-refresh

Check the box to enable this function and the page will refresh automatically every 10 seconds.

Severity	<p>Enable Severity and specify the importance of the logs you want to view in the log list.</p> <p>ALL Level: Logs of all levels.</p> <p>EMERGENCY: Errors that render the gateway unusable, such as hardware errors.</p> <p>ALERT: Errors that must be resolved immediately, such as flash write errors.</p> <p>CRITICAL: Errors that put the system at risk, such as a failure to release memory.</p> <p>ERROR: Generic errors.</p> <p>WARNING: Warning messages, such as WinNuke attack warnings.</p> <p>NOTICE: Important notifications, such as IKE policy mismatches.</p> <p>INFO: Informational messages.</p> <p>DEBUG: Debug-level notifications, such as when the gateway receives a DNS packet.</p>
Send Log	<p>Enable the Send Log function and then the newly generated logs will be sent to the specified server.</p>
Server IP	<p>Specify the IP address of the server that the logs will be sent to.</p>

- 2) (Optional) Click **Save Log** to save the current logs to the host.