



🔁 trovaprezzi.it

User Guide

Omada Wireless Gigabit VPN Router

© 2023 TP-Link REV1.0.0 1910013449

CONTENTS

Intended Readers	1
Conventions	1
More Information	1
Determine the Management Method	3
Web Interface Access	4
System Status	7
Traffic Statistics	8
Viewing the Interface Statistics	8
Viewing the IP Statistics	9
Overview	12
Supported Features	12
Wireless Status	13
View Router's Wireless Settings	13
View Client Details	14
Wireless Settings	15
Wireless Settings Access	
Wireless VLAN	19
MAC Filtering	
Wireless Schedule	
Band Steering	
Mesh Management	25
Overview	
Supported Features	
WAN Configuration	
Configuring the Number of WAN Ports	
Configuring the WAN Connection	
LAN Configuration	
Configuring the IGMP Proxy	
Viewing the DHCP Client List	
Configuring the Address Reservation	
IPTV Configuration	
Configuring the IPTV	
MAC Configuration	
Configuring MAC Address	
Switch Configuration	
Viewing the Statistics	

Configuring Port Mirror	
Configuring Rate Control	
Configuring Port Config	51
Viewing Port Status	
Viewing DDM Status	
VLAN Configuration	
Creating a VLAN	54
Configuring the PVID of a Port	55
IPv6 Configuration	
Configure IPv6 for WAN / SFP WAN port(s)	57
Configuring the WAN Connection	
Configuring IPv6 for the LAN Port	64
Overview	71
USB Modem Configuration	
Configuring USB Modem automatically	72
Configuring the USB Modem manually	74
USB Storage	
Managing the USB Storage	76
Auto Backup	76
Firmware Upgrade via USB	77
Overview	
IP Group Configuration	
Adding IP Address Entries	80
Grouping IP Address Entries	81
IPv6 Group Configuration	
Adding IP Address Entries	82
Grouping IP Address Entries	83
Time Range Configuration	
VPN IP Pool Configuration	
Service Type Configuration	
Transmission	
Overview	
Supported Features	
NAT Configurations	
Configuring the One-to-One NAT	
Configuring the Virtual Servers	
Configuring the Port Triggering	
Configuring the NAT-DMZ	

Configuring the ALG	
Bandwidth Control Configuration	
Quality of Services Configurations	
Configuring Bandwidth Control	
Configuring Class Rule	
Configuring VoIP Prioritization	
Configuring Tag Prioritization	
Session Limit Configurations	
Configuring Session Limit	
Viewing the Session Limit Information	
Load Balancing Configurations	
Configuring the Load Balancing	
Configuring the Link Backup	
Configuring the Online Detection	
Routing Configurations	
Configuring the Static Routing	
Configuring the Policy Routing	
Viewing the Routing Table	
Configuring RIP	
Configuring OSPF	
Configuration Examples	119
Example for Configuring NAT	
Example for Configuring Load Balancing	
Example for Configuring Virtual Server	
Example for Configuring Policy Routing	
Firewall	
Overview	
Supported Features	
Firewall Configuration	
Anti ARP Spoofing	
Configuring Attack Defense	
Configuring MAC Filtering	
Configuring Access Control	
Configuration Examples	
Example for Anti ARP Spoofing	
Example for Access Control	
Behavior Control	
Overview	

Supported Features	
Behavior Control Configuration	
Configuring Web Filtering	
Configuring Web Security	
Configuration Examples	
Example for Access Control	
Example for Web Security	
VPN	
Overview	
Supported Features	
IPSec VPN Configuration	172
Configuring the IPSec Policy	
Verifying the Connectivity of the IPSec VPN tunnel	
GRE VPN Configuration	179
L2TP Configuration	
Configuring the VPN IP Pool	
Configuring L2TP Globally	
Configuring the L2TP Server	
Configuring the L2TP Client	
(Optional) Configuring the L2TP Users	
Verifying the Connectivity of L2TP VPN Tunnel	
PPTP Configuration	
Configuring the VPN IP Pool	
Configuring PPTP Globally	
Configuring the PPTP Server	
Configuring the PPTP Client	
(Optional) Configuring the PPTP Users	
Verifying the Connectivity of PPTP VPN Tunnel	
OpenVPN Configuration	
Configuring the OpenVPN Server	
Configuring the OpenVPN Client	
Viewing the OpenVPN Tunnel	
WireGuard VPN Configuration	
Configuring the WireGuard VPN Server	
Configuring the Peers Settings	
Users Configuration	
OpenVPN Configuration	
OpenVPN Configuration	

Configuration Examples	
Example for Configuring IPSec VPN	
Example for Configuring L2TP VPN	
Example for Configuring PPTP VPN	
Example for Configuring OpenVPN	
Overview	
Quick Setup	203
Status Configuration	204
Viewing the Status Information	
Viewing Locked Out User	
SSL VPN Server Configuration	
Configuring the SSL VPN Server	
Resource Management	
Configuring the Resources	
Grouping Tunnel Resources	
User Management	210
Adding the User List	210
Grouping Users	211
Authentication	212
Adding the Authentication Server List	212
Configuring the Radius Server	213
OpenVPN Configuration	
Configuration Examples	
Example for Configuring IPSec VPN	
Example for Configuring L2TP VPN	
Example for Configuring PPTP VPN	
Example for Configuring OpenVPN	
Overview	216
Typical Topology	216
Portal Authentication Process	217
Supported Features	217
Local Authentication Configuration	219
Configuring the Authentication Page	219
Configuring the Local User Account	
Radius Authentication Configuration	
Configuring Radius Authentication	
Onekey Online Configuration	
Configuring the Authentication Page	

LDAP Configuration	
Configuring the Authentication Page	
Guest Resources Configuration	232
Configuring the Five Tuple Type	
Configuring the URL Type	
Configuring LDAP Profiles	236
Viewing the Authentication Status	
Configuration Example	
Network Requirements	
Configuration Scheme	
Configuration Procedures	
Services	243
Overview	
Support Features	
Dynamic DNS Configurations	244
Configure and View Peanuthull DDNS	
Configure and View Comexe DDNS	
Configure and View DynDNS	
Configure and View NO-IP DDNS	
Custom DDNS	
UPnP Configuration	251
Configuration Example for Dynamic DNS	
Network Requirement	
Configuration Scheme	
Configuration Procedure	
mDNS Configuration	
Reboot Schedule	
DNS Proxy	
DNSSEC	
DOH	
DOT	
System Tools	
Overview	
Support Features	
Admin Setup	
Admin Setup	
Remote Management	
System Setting	

Controller Settings	265
Enable Cloud-Based Controller Management	265
Configure Controller Inform URL	266
Management	267
Factory Default Restore	
Backup & Restore	267
Reboot	
Firmware Upgrade	268
SNMP	269
Diagnostics	270
Diagnostics	270
Remote Assistance	272
LED Control	273
Time Settings	273
Setting the System Time	273
Setting the Daylight Saving Time	
System Log	278

About This Guide

This User Guide provides information for managing Omada VPN Router. 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 router.
- 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 Router

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 router based on your actual network situation. The router 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 router can be centrally configured and monitored via Omada SDN Controller.

To prepare the router 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 router using the GUI (Graphical User Interface, also called web interface in this text). The router uses two built-in web servers, HTTP server and HTTPS server, for user authentication.

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



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

2 Web Interface Access

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

- Connect to the router using the default SSID printed on the label at the bottom of the router or connect a PC to a LAN port of the router 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 http://tplinker.net or http://192.168.0.1 in the address field of the browser, then press the Enter key.

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

\oplus	192.168.0.1

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

Figure 2-2 Create a Username and a Password

For device security, pleas	se set an administrator account.
Username :	admin
Password:	•••••
Confirm the Password:	•••••
✓ I agree to TP-Link's Terr	ms of Use and Privacy Policy
password for login. These wi attempts. If you forget your	r administrator account name and II be required for subsequent login login details, you will need to reset the . To reset the device, power it on and et button for 5 seconds.
	Confirm

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

Figure 2-3 Login Authentication

Ptp-link	
Username	admin
Password	•••••
Log	g In Clear

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

Part 2

Viewing Status Information

CHAPTERS

- 1. System Status
- 2. Traffic Statistics

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.
```

System Status	s						
Device Info							
Hardware Vers	ion: EP7	06W v1.0		Firmware Vers	ion: 100B	uild 20230513 Rel.04	1826(4555)
CPU Temperatu		C(GOOD)		Thinking vers	1.0.0 5	und 20230313 Nello-	1020(4000)
CPO Temperatu	ire: 50 (.(6000)					
System Time							
System Time:	05/:	13/2023 00:07	:57 Saturday	Running Time	: 0 Day, 0	0 Hour, 8 Min, 16 Sec	5
WAN IPv4							
Interface Name	Connection Type	Connection Status	IP Address	Subnet Mask	MAC Address	Default Gateway	Primary DNS
SFP WAN/LAN1	Dynamic IP	Link Down	0.0.0.0	0.0.0.0	40-ED-00-52-BB-DE	0.0.0.0	0.0.0.0
WAN2	Static IP	Link Down	172.31.53.227	255.255.255.0	04-D4-C4-AE-6D-CF	172.31.53.1	172.29.1.1
Resource Utiliz	ation						
			100 Core1				
39%	3%		80 Core2	\wedge			
			60				
			40				
			20				
Memory	CPU		0		~~~~~		~

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.

Interface Statistics	IP Statistics								
ettings									0
Enable Interface	e Statistics								
Save									
tatistics List									
tatistics List									
tatistics List						🖥 Clear 🛛 🕼	Refresh 🕑	Auto Refresh	
itatistics List Interface	TX Rate (KB/s)	RX Rate (KB/s)	TX Packet Rate (Pkt/s)	RX Packet Rate (Pkt/s)	Total TX Bytes		Tabel TV	Auto Refresh Total RX Packets	
	TX Rate (KB/s)	RX Rate (KB/s)			Total TX Bytes		Total TX	Total RX	
Interface			(Pkt/s)	(Pkt/s)		Total RX Bytes	Total TX Packets	Total RX Packets	

Figure 2-1 Interface Statistics

Click the header to select or change the sorting preferences.

Enable **Interface Statistics**, then you can 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 	1							
IP Range :	192.16	8.0.0	/ 255.255.25	5.0				
Save								
Statistics List								
IP Address Number: 0						👕 Clear 🛛 🧔	Refresh 💽	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
			(FKL/S)	(FKL/S)			Packets	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.

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

Configuring Wireless Settings

CHAPTERS

- 1. Overview
- 2. Wireless Status
- 3. Wireless Settings
- 4. Mesh Management

1 Overview

The Wireless module provides basic wireless functions, including checking wireless connection details, configuring wireless parameters, setting up mesh network and more.

1.1 Supported Features

Status

You can check the parameters of the router's wireless network (SSID lists, radio settings, and radio traffic) and the details about the connected clients.

Wireless Settings

Wireless networks enable wireless clients to access the internet. Once a wireless network is set up, the router typically broadcast the network name (SSID) in the air, and wireless clients can connect to the network and access the internet. In this module, you can configure wireless settings, set up wireless VLAN, configure MAC filtering, set wireless schedule and enable Band Steering.

Mesh

Enable the Mesh feature and synchronize the mesh network settings to the Omada app.

2 Wireless Status

You can check the parameters of the router's wireless network (SSID lists, radio settings, and radio traffic) and the details about the connected clients.

2.1 View Router's Wireless Settings

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

SID	List								
									🙆 Refre
ID	SSID Name	Clients	Band	Security	Portal	VLAN ID	Guest Network	Down (Bytes)	Up (Bytes)
1	TP- Link_2.4GHz_52BBDC		2.4GHz	None	Disable	Disable	Disable	0	0
2	TP-Link_5GHz_52BBDD		5GHz	None	Disable	Disable	Disable	0	0
adio	Settings								2.4GHz 5GHz
.4GH	z Wireless Radio:	Enable							
hann	el Frequency:	11 / 2462MH	z						
		Auto	-						
		b/g/n/ax mixe	ed						
		573.5Mbps	20						
Max TX Rate:									
		20dBm							
x Pov									2.4GHz 5GHz
x Pov adio	ver: Traffic			т	x Packets:		0		2.4GHz 5GHz
x Pov adio x Pac	ver: Traffic :kets:	20dBm			x Packets: x Bytes:		0		2.4GHz 5GHz
adio x Pac x Byt	ver: Traffic ckets: tes:	20dBm 0		T		ckets:			2.4GHz 5GHz
tadio tx Pac tx Pac	ver: Traffic ckets: tes: opped Packets:	20dBm 0		רד רד	x Bytes:	ckets:	0		2.4GHz 5GHz
x Pov adio x Pac x Byl x Dro x Err	ver: Traffic ckets: tes: opped Packets:	20dBm 0 0 0 0 Displays		נד נד נד	x Bytes: x Dropped Par x Errors: SSIDs you	u have cre	0	r details. Clic	
x Pov adio x Pac x Byt x Dro x Err	ver: Traffic ckets: tes: opped Packets: ors:	20dBm 0 0 0 Displays get the la	atest stati er works	T: T: Hz/5GHz \$ us of the \$	x Bytes: x Dropped Par x Errors: SSIDs you SSID List. .4GHz an	u have cre d 5GHz b	0 0 0		k Refresh te

Figure 2-1 Viewing the Wirelesss Settings

2.2 View Client Details

Choose the menu Wireless > Status > Client to load the following page.

Figure 2-2 Viewing Client Details

											🙆 Refr
ID	Hostname	IP Address	MAC Address	Band	SSID	Active Time	Up (Bytes)	Down (Bytes)	RSSI (dBm)	Rate (Mbps)	Actio
											A • (
											🙆 Refi
ID		Hostname			MAC Addres	s		Jp tes)	Down (Bytes		Refi Action

parameters. Click Refresh to get the latest status of the Client List.

Block Client ListAllows you to view the information of the clients that have been blocked, and resume
the client's access. Click Refresh to get the latest status of the Block Client List.

3 Wireless Settings

Wireless networks enable wireless clients to access the internet. Once a wireless network is set up, the router typically broadcast the network name (SSID) in the air, and wireless clients can connect to the network and access the internet. In this module, you can configure wireless settings, set up wireless VLAN, configure MAC filtering, set wireless schedule and enable Band Steering.

3.1 Wireless Settings Access

Wireless Settings Access allows you to create wireless networks on the 2.4GHz or 5GHz band, view and edit the information of the wireless networks that have been created, and configure the wireless networks' advanced settings including Radio Settings, Load Balance, Airtime Fairness, etc.

To complete wireless settings access, follow these steps:

- 1) Click 2.4GHz | 5GHz to select a frequency band.
- 2) Configure the information and features of the wireless network.

Choose the menu **Wireless > Wireless Settings > Wireless Settings Access** to load the following page.

Figure 3-1 Configuring the Wireless Settings Access

	Wireless Radio						
2.4GHz V	Wireless Radio:	Enable					
Save							
2.4GHz S	SSIDs						
							O A
ID	SSID		VLAN ID	SSID Broadcast	Security Mode	Guest Network	Action
1	TP-Link_2.	4GHz_52BBDC	Disable	Enable	None	Disable	1 T
.4GHz V	Wireless Advance	ed Settings					
		ed Settings d Balance Airtime Fa	sirness More Settir	gs			
Radio	o Settings Load			gs			
Radio Wireless I	o Settings Load Mode:	l Balance Airtime Fa		gs			
Radio Wireless Channel	o Settings Load Mode: Width:	l Balance Airtime Fa 802.11b/g/n/a		gs			
Radio Wireless I Channel V Channel:	o Settings Load Mode: Width:	Balance Airtime Fa 802.11b/g/n/a Auto	ax mixed	gs dBm(5-20)			
Radio Wireless Channel V Channel: Tx Power Note:	o Settings Load Mode: Width: : r(EIRP):	Balance Airtime Fa 802.11b/g/n/a Auto Auto	ix mixed •				

Wireless Radio	the wireless parameters. Only when this option is enabled will the wireless radio on 2.4GHz or 5GHz band works.
0.4011-/5011-	Oliste Add to supply COID on the change hand and firms the management

2.4GHz/5GHz	Click Add to create a new SSID on the chosen band, configure the parameters, and
SSIDs	click OK.

2.4GHz/5GHz Wireless Advanced Settings

Radio Settings

Radio settings directly control the behavior of the radio in the router and its interaction with the physical medium; that is, how and what type of signal the router emits.

Load Balance

Load Balance allows you to limit the maximum number of clients who can access the router's wireless network. In this way, you can achieve a rational use of network resources.

Airtime Fairness

With Airtime Fairness enabled, each client connected to the router's wireless network can get the same amount of time to transmit data, avoiding low-data-rate clients occupying too much network bandwidth.

More Settings

To improve the network's stability, reliability, and communication efficiency, configure the following parameters based on your needs.

Configuring Advanced Settings

Radio Settings

Configure the following parameters of the chosen band, and click **Save**.

Wireless Mode	Select the IEEE 802.11 mode the radio uses.
	For 2.4GHz:
	802.11n only - Only 802.11n clients can connect to the router.
	802.11b/g mixed - Both 802.11b and 802.11g clients can connect to the router.
	802.11b/g/n mixed - All of 802.11b, 802.11g, and 802.11n clients operating in the 2.4GHz frequency can connect to the router.
	802.11b/g/n/ax mixed - All of 802.11b, 802.11g, 802.11n, and 802.11ax clients operating in the 2.4GHz frequency can connect to the router. Note that 802.11ax is only available for certain devices.
	For 5GHz:
	802.11n/ac mixed - Both 802.11n clients and 802.11ac clients operating in the 5GHz frequency can connect to the router.
	802.11a/n/ac mixed - All of 802.11a, 802.11n, and 802.11ac clients operating in the 5GHz frequency can connect to the router.
	802.11a/n/ac/ax mixed - All of 802.11a, 802.11n, 802.11ac, and 802.11ax clients operating in the 5GHz frequency can connect to the router. Note that 802.11ax is only available for certain devices.

Channel Width	Select the channel width of the router. For the 2.4GHz band, available options include Auto, 20MHz, and 40MHz. For the 5GHz band, available options include Auto, 20MHz, 40MHz, 80MHz, and 160MHz.				
Channel	Select the channel used by the router. For example, 1/2412MHz means that the channel is 1 and the frequency is 2412MHz. By default, the channel is selected as Auto, and we recommend that you keep the default setting.				
Tx Power (EIRP)	Specify the transmit power value. If this value is set to be larger than the maximum transmit power that is allowed by the local regulation, the regulated maximum transmit power will be applied in the actual situation.				
 Note: Note that in most cases, it is unnecessary to use the maximum transmit power. Specifying a larger transmit power than needed may cause interference to the neighborhood. Also, it consumes more power and reduces the longevity of the device. 					

Load Balance

Configure the following parameters of the chosen band, and click **Save**.

Load Balance	Check the box to enable Load Balance.
Maximum Associated Clients	Specify the maximum number of clients who can connect to a radio band (either 2.4GHz or 5GHz) of the router at the same time. While the number of connected clients has reached the limit and there are more clients requesting to access the network, the router will disconnect those with weaker signals. The value of Maximum Associated Clients is from 1-127, and the default is 50.

Airtime Fairness

We recommend you check the box to enable Airtime Fairness under multi-rate wireless networks. In this way, the faster clients can get more time for the data transmission and the network's overall throughput can be improved.

More Settings

Configure the following parameters of the chosen band, and click **Save**.

Beacon Interval Beacons are transmitted periodically by the router to announce the presence of a wireless network for the clients. Beacon Interval determines the time interval of the beacons sent by the router. You can specify a value between 40 and 100ms. The default is 100ms.

DTIM Period	The DTIM (Delivery Traffic Indication Message) is contained in some Beacon frames. It indicates whether the router has buffered data for client devices. The DTIM Period indicates how often the clients served by this router should check for buffered data still on the router awaiting pickup. You can specify the value between 1-255 Beacon Intervals. The default value is 1, indicating that clients check for buffered data at every beacon. An excessive DTIM interval may reduce the performance of multicast applications, so we recommend you keep the default value.
RTS Threshold	 RTS/CTS (Request to Send/Clear to Send) is used to improve the data transmission efficiency of the network with hidden nodes, especially when there are lots of large packets to be transmitted. When the size of a data packet is larger than the RTS Threshold, the RTS/CTS mechanism will be activated. As a result, before sending a data packet, the client will send an RTS packet to the router to request data transmitting. And then the router will send a CTS packet to inform other clients to delay their data transmitting. In this way, packet collisions can be avoided. For a busy network with hidden nodes, a low threshold value will help reduce interference and packet collisions. But for a not-so-busy network, a too low threshold value will cause bandwidth wasting and reduce the data throughput. The recommended and default value is 2347 bytes.
Fragmentation Threshold	The fragmentation function can limit the size of packets transmitted over the network. If the size of a packet exceeds the Fragmentation Threshold, the fragmentation function is activated and the packet will be fragmented into several packets. Fragmentation helps improve network performance if properly configured. However, a too low fragmentation threshold may result in poor wireless performance caused by the extra work of dividing up and reassembling of frames and increased message traffic. The recommended and default value is 2346 bytes.
OFDMA	OFDMA enables multiple users to transmit data simultaneously, and thus greatly improves speed and efficiency. Only when your clients also support OFDMA, can you fully enjoy the benefits.

3.2 Wireless VLAN

Wireless VLAN is used to set VLANs for wireless networks. With this feature, the router can work together with the switches supporting 802.1Q VLAN. Traffic from the clients in different wireless networks is added with different VLAN tags according to the VLAN settings of the wireless networks. Then the wireless clients in different VLANs cannot directly communicate with each other. Note that the traffic from the wired clients will not be added with VLAN tags.

To complete wireless VLAN, select the specific SSID in the VLAN ID list to configure the VLAN parameters and click **Save**.

Choose the menu **Wireless** > **Wireless Settings** > **VLAN** to load the following page.

Figure 3-2 Configuring the Wireless VLAN

ID	SSID Name	Band	VLAN	VLAN ID
1	TP-Link_2.4GHz_52BBDC	2.4GHz	Disable 🔹	
2	TP-Link_5GHz_52BBDD		Disable 🔹	
Save	e VLAN, please select the corresp	onding LAN net	work.	
			verk. Ie the VLAN function on the S	SID.
Save 'LAN 'LAN ID	Select Enal Specify the	ole to enab	le the VLAN function on the S	SID. y VLAN ID represents a differe

3.3 MAC Filtering

MAC Filtering is used to allow or block clients with specific MAC addresses to access the network. With this feature, you can effectively control clients' access to the wireless network according to your needs.

To complete MAC filtering settings, follow these steps:

- 1) In Settings, check the box of Enable MAC Filtering.
- 2) In **Station MAC Group**, click **Create Groups**, create a new MAC group, and add the MAC address of the hosts to be filtered to the MAC group.
- 3) In MAC Filtering Association, configure the filtering rule

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



Settings	Settings						
Enable MAC	Enable MAC Filtering: 🕑 Enable						
Save	Save						
Station MA	C Group						
	Create Groups						
MAC Filterin	ng Association						
ID	SSID	Band	MAC Group Name	Action			
1	TP-Link_2.4GHz_52BBDC	2.4GHz	None	Deny 💌			
2	TP-Link_5GHz_52BBDD	5GHz	None 🔻	Deny 💌			
	Deny: Block access from the stations in the MAC Group list. Allow: Only allow access from the stations in the MAC Group list.						

In Settings section, Check the box to enable MAC Filtering, and click Save.

In **Station MAC Group** section, click **Create Groups**, and two pop-up windows will appear, which allow you to create a MAC group first, and add the MAC addresses to the MAC group.

Add (above the Operation column)	Click Add , and a pop-up window will appear, on which you can create a new MAC group.
MAC Group	Specify a name for the MAC Group, and click OK .
MAC Group Name	Displays all the MAC groups you have created.
Add (above the Modify column)	Select a MAC group in the group list, and click Add . On the pop-up window, add the MAC address to be filtered.
MAC Address	Enter the MAC address to be filtered in the format XX-XX-XX-XX-XX, and OK. In the same way, you can add more MAC addresses to the selected MAC group. And you can also view all the added MAC addresses here.
Modify	Edit or delete the selected MAC address.
In MAC Filtering	Association section, specify the filtering rule, then click Save.

SSID	Displays the SSIDs that you can set the filtering rule.	

Band	Displays the SSIDs that you can set the filtering rule.
MAC Group Name	Select a MAC group to be filtered from the drop-down list.
Action	Specify the filtering rule (Allow/Deny) for the selected MAC group from the drop- down list, and click Save.

3.4 Wireless Schedule

The Scheduler feature allows the router's wireless network to automatically turns on or off at the time you set. As a time-based function, Scheduler takes effect according to the router's system time. You can set or view the system time in **System Tools > Time Settings**.

To complete wireless schedule settings, follow these steps:

- 1) In **Settings**, check the box to enable **Scheduler**, and select the **Association Mode**.
- 2) In **Profile**, click **Create Profiles**, create a new scheduler profile, and add time range items to the profile. Note that if there are several time range items in one profile, the time range of this profile is the sum of all of these time ranges.
- 3) In Scheduler Association, configure the scheduler rule.

Choose the menu Wireless > Wireless Settings > Scheduler to load the following page.

Scheduler:	✓ Enable				
Association Mode: Associated with SSID 🔻					
Save					
Save					
Profile					
			Create Profiles		
Scheduler A	ssociation				
Scheduler A	ssociation				
Scheduler A	ssociation	Band	Profile Name	Action	
		Band 2.4GHz	Profile Name	Action Radio Off	
	SSID				
ID 1	SSID TP-Link_2.4GHz_52BBDC	2.4GHz	None	Radio Off 🔹	

Figure 3-4 Configuring Schduler

In Settings section, Check the box to enable Scheduler, and select the Association Mode.

Associated with SSID	The scheduler profile will be applied to the specific SSID.
Associated with Router	The profile will be applied to all SSIDs on the router.

In **Profile**, click **Create Profiles**, and two pop-up windows will appear, which allow you to create a scheduler profile first, and add time range items to the profile.

Add (of the scheduler profile window)	Click Add , and a pop-up window will appear, on which you can create a new scheduler profile.
Profile	Specify a name for the scheduler profile, and click OK .
Profile Name	Displays all the scheduler profiles you have created.
Operation	Edit or delete the selected scheduler profile's information
Add (of the time range items window)	Select a profile in the profile list (the color of the selected one will turn green), and click Add on the time range items window. On the pop-up window, configure the parameters, and click OK .
Day	Select on which day(s) (Weekday/Weekend/Everyday/Custom) the scheduler will take effect.
Time	If you check the box of 24 hours, the scheduler rule will take effect for 24 hours on each selected day.
Start Time	Specify when the scheduler rule will take effect.
End Time	Specify when the scheduler rule will end.
In Scheduler Ass	ociation section, specify the rule, then click Save .
SSID	Displays the SSIDs that you can set the scheduler rule.
Band	Displays which frequency band the SSID belongs to.
Profile Name	Select a scheduler profile for the SSID.
Action	Select the scheduler rule (Radio On/Radio Off), and click Save.

3.5 Band Steering

With Band Steering enabled, dual-band clients will be steered to the 5GHz band according to the configured parameters. Band Steering adjusts the number of clients on 2.4GHz and 5GHz bands. As the 5GHz band supports a larger number of non-overlapping channels and is less noisy, the network performance can be improved.

To run the Band Steering function on an SSID, you need to create the SSIDs on both the 2.4GHz and 5GHz bands and make sure they have the same name, security mode, and wireless password.

To complete the Band Steering settings, check the box to enable **Band Steering**, and configure the parameters to balance the clients on both frequency bands, then click **Save**.

Band Steering					
Band Steering:	Enable				
Connection Threshold:	20	(2-40)			
Different Threshold:	4	(1-8)			
Max Failures:	10	(0-100)			
Note: To run the Band Steering function on an SSID, please create the SSIDs on both of the 2GHz and 5GHz band and make sure they have the same name, security mode and wireless password. Save					
Connection Threshold		um number of clients connected to the 5GHz band. The value of nold is from 2 to 40, and the default is 20.			
Different Threshold	Defines the maximum difference between the number of clients on the 5GHz band and 2.4GHz band. The value of Different Threshold is from 1 to 8, and the default is 4. When the following two conditions are both met, the router prefers to refuse the connection request on 5GHz band and no longer steer other clients to the 5GHz band:				
	1. The number of clients on the 5GHz band reaches the Connection Threshold value.				
	2. The difference between the number of clients on the 2.4GHz band and 5GHz band reaches the Different Threshold value.				
Max Failures	associate with the	s 5GHz band is overloaded, if a client repeatedly attempts to router on the 5GHz band and the number of rejections reaches illures, the router will accept the request.			
	The value is from 0 to 100, and the default is 10.				

4 Mesh Management

Log in with your TP-Link ID to add and manage APs, and synchronize the mesh network settings to the Omada app.

Choose the menu **Wireless** > **Mesh** to load the following page.To complete Mesh Management, follow these steps:

1) Click Go to Login to configure mesh network and log in with TP-Link ID

	Log in with Tp-Link ID
Log in with your T	P-Link ID to add and manage APs, and synchronize the mesh network settings to the Omada app.
	Go to Login
Note: To enjoy	the mesh function, please go to System Tools > Controller Settings, enable Cloud-Based Controller Management and tick the Privacy Policy checkbox.

2) Click Let's Get Started to start setting up the mesh network.



3) The system will scan for the EAPs available to build a mesh network.



4) Click **Add Device** to add the selected device to the mesh network. The router will be the mesh root.

anned Devic	ces: 2		@ Resc
	Name	MAC Address	Role
	EAP620 HD 3.0	30-DE-4B-2B-95-28	MeshMaster
	EAP621 HD 2.0	30-DE-4B-2B-95-74	MeshNode

5) Adding device to the mesh network.



6) Configure the Device Account Settings.

Devices Account Setting	gs	
Username:	admin	
Password:	•••••	אר ^ג
Next		

7) Configure the network settings.

4			
Network Config	uration		
SSID:			
Password:		Syst.	
Band:	2.4GHz	5GHz	
Next			

8) Done. The mesh network is set up. To manage the device wirelessly, connect to the extended network.

Network Config	uration		
SSID:	t	Sinish!	
assword:			
Band: Next	2.4GHz 🕑 5GHz	To manage the device wirelessly, please connect to the extended Wi-Fi.	
		Extended 2.4Ghz SSID: t	
		Extended 5Ghz SSID: t	
		ок	

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 router 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 router connect to your local network devices, the router 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 router 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 router if your ISP supports IPv6. IPv6 network won't cause conflict with your current IPv4 network.


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.

To complete WAN configuration, follow these steps:

- 1) In WAN Mode, determine the number of WAN ports according to your needs.
- 2) Configure WAN connection for the WAN / SFP WAN port(s).

2.1 Configuring the Number of WAN Ports

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

WAN Mode:	USB Modem	SFP WAN/LAN1	WAN2	WAN/LAN3
	LTE 1 2		AN 6	
Save	Note: 🔲 Available	📕 WAN Connection 🏾 🌄	LAN Connection	
ote: . Any change to the nun roceeding.	nber of WAN ports may lead y	your current configurations to b	e lost. Make sure you hav	e backed up your configurations before
. Any change to the nun	Determine the as WAN port, enable the po	e number of WAN pe check the box of the	orts according to desired port. To	e backed up your configurations before your needs. To enable a por configure multiple WAN ports (for certain devices) and USI

Figure 2-1 Configuring the WAN Mode

2.2 Configuring the WAN Connection

The router supports five connection types: **Static IP, Dynamic IP, PPPoE, L2TP, PPTP,** you can choose one according to the requirements of your ISP.

Static IP: Select this type if your ISP has offered you a fixed IP address.

Dynamic IP: Select this type if your ISP automatically assigns the IP address.

PPPoE: Select this type if your ISP provides you with a PPPoE account.

L2TP: Select this type if your ISP provides you with an L2TP account.

PPTP: Select this type if your ISP provides you with a PPTP account.

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 > SFP WAN/LAN1** to load the following page.

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:	🗌 Enable			
Vlan ID:	4094	(1-4094)		
	Get IP using Unicast DHCP			
Save Connect Disc	onnect			

Figure 2-2 Configuring the Dynamic IP

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 has offered you a fixed IP address
Host Name	(Optional) Enter a name for the router. It is null by default.
Upstream Bandwidth	Specify the upstream bandwidth of the WAN port. This value is the upper limit of the Maximum Upstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of each WAN port after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
Downstream Bandwidth	Specify the downstream bandwidth of the WAN port. This value is the upper limit of the Maximum Downstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of each WAN port after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.

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.
VLAN ID	If VLAN for the WAN port is enabled, you need to enter a VLAN ID. Then the WAN port is automatically assigned to the VLAN. By default, 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 configure its egress rule as TAG. To configure 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 in the normal DHCP process. 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 > SFP WAN/LAN1** to load the following page.

Figure 2-3	Configuring the Static IP

Connection Configuration			Connection Status	
Connection Type: IP Address: Subnet Mask: Default Gateway: Upstream Bandwidth: Downstream Bandwidth: MTU: Primary DNS:	Static IP	(Optional) Kbps (100-1000000) Kbps (100-1000000) (576-1500) (Optional)	Connection Status IP Address Subnet Mask Default Gateway Primary DNS Secondary DNS	Disconnected 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0 0.0.0.0
Secondary DNS:		(Optional)		
Vlan:	Enable			
Vlan ID:	4094	(1-4094)		

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 upstream bandwidth of the WAN port. This value is the upper limit of the Maximum Upstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of each WAN port after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
Downstream Bandwidth	Specify the downstream bandwidth of the WAN port. This value is the upper limit of the Maximum Downstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of each WAN port after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port.
	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.
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, Generally, you don't need to enable VLAN for the WAN port unless required by your ISP.
VLAN ID	If VLAN for the WAN port is enabled, you need to enter a VLAN ID. Then the WAN port is automatically assigned to the VLAN. By default, 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 configure its egress rule as TAG. To configure VLANs, go to Network > VLAN > VLAN .

Configuring the PPPoE

Choose the menu **Network > WAN > SFP WAN/LAN1** to load the following page.

Figure 2-4	Configuring the PPPoE	
i igui c z =		

Connection Configuration Connection Status				
Connection Type:	РРРоЕ	•	Connection Status	Disconnected
Username:			IP Address	0.0.0.0
Password:		r.r.k	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
Downstream bandwidth:	100000	Kbps (100-1000000)		
MTU:	1492	(576-1492)	Secondary Connection	on
MRU:	1492	(576-1492)	IP Address	0.0.0.0
Service Name:		(1-128 characters, optional)	Subnet Mask	0.0.0.0
Primary DNS:		(Optional)		
Secondary DNS:		(Optional)		
Vlan:	🗌 Enable			
Vlan ID:	4094	(1-4094)		
Secondary Connection:	None Opynamic IP	Static IP		
Save Connect Disc	connect			

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	Choose the connection mode, including Connect Automatically , Connect Manually and Time-Based.
	Connect Automatically: The router will activate the connection automatically when the router reboots or the connection is down.
	Connect Manually: You can manually activate or terminate the connection.
	Time-Based: During the specified period, the router will automatically activate the connection.
Time	Choose the time range for automatic connection. To create the time range, go to Preferences > Time Range > Time Range .

Upstream Bandwidth	Specify the upstream bandwidth of the WAN port. This value is the upper limit of the Maximum Upstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of each WAN port after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
Downstream Bandwidth	Specify the downstream bandwidth of the WAN port. This value is the upper limit of the Maximum Downstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of each WAN port after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
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.
MRU	Specify the MRU (Maximum Receive Unit) of the WAN port.
	MRU is the largest packet size the router will allow a computer on the network to receive. When PPPoE is selected, MRU 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, Generally, you don't need to enable VLAN for the WAN port unless required by your ISP.
VLAN ID	If VLAN for the WAN port is enabled, you need to enter a VLAN ID. Then the WAN port is automatically assigned to the VLAN. By default, 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 configure its egress rule as TAG. To configure 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.

Configuring the L2TP

Choose the menu **Network > WAN > SFP WAN/LAN1** 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:		rt.	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
	1460			
MTU:	1460	(576-1460)	Secondary Connection	on
Primary DNS:		(Optional)	IP Address	0.0.0.0
Secondary DNS:		(Optional)	Subnet Mask	0.0.0.0
Vlan:	Enable		Default Gateway	0.0.0.0
Vlan ID:	4094	(1-4094)	Primary DNS	0.0.0.0
Secondary Connection:	Oynamic IP O Static	IP	Secondary DNS	0.0.0.0
VPN Server IP/Domain Name:				
IP Address:				
Subnet Mask:				
Default Gateway:		(Optional)		
Primary DNS:		(Optional)		
Secondary DNS:		(Optional)		
Save Connect Disc	connect			

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	Choose the connection mode, including Connect Automatically , Connect Manually and Time-Based.
	Connect Automatically: The router will activate the connection automatically when the router reboots or the connection is down.
	Connect Manually: You can manually activate or terminate the connection.
	Time-Based: During the specified period, the router will automatically activate the connection.
Time	Choose the time range for automatic connection. To create the time range, go to Preferences > Time Range > Time Range .

Upstream BandwidthSpecify the upstream bandwidth of the WAN port. This value is the upper limit of the Maximum Upstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth rule of each WAN port after Bandwidth Basics Settings page.Downstream BandwidthSpecify the downstream Bandwidth on Transmission > Load Balancing > Basic Settings page.MTUSpecify the downstream Bandwidth on Transmission > Load Balancing > Basic Settings page.MTUSpecify the MTU (Maximum Transmission Unit) of the WAN port. This value is the upper limit of Basic Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.MTUSpecify 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.VLANAdd the WAN port to a VLAN. Generally. Generally, you don't need to enable VLAN for the WAN port to a VLAN. Generally. Generally, you don't need to oonfigue its usutmatically assigned to the VLAN. By default, the geress rule of the VLAN is upstream the WAN port to a submatically assigned to the VLAN. By dofault, the geress rule of the VLAN is upstream the WAN port to arransmitted by the WAN port units.Secondary DNSSelect the secondary connection type according to the requirements of your ISP. To secondary connection is required for L2TP connection. The router will get some necessary information after the secondary connection.SecondarySelect the secondary connection type as Static IP, you need to configure IP Address. Subhet Mask, Default G		
Bandwidththe Maximum Downstream Bandwidth on Transmission > Bandwidth Dased Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.MTUSpecify 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.VLANAdd the WAN port to a VLAN. Generally, Generally, you don't need to enable VLAN for the WAN port to a VLAN. Benerally, Generally, you don't need to enable VLAN is UNTAG, so the packets are transmitted by the WAN port without YLAN tags. If you want the WAN port to transmit packets with VLAN. By default, the egress rule of the VLAN is global as at G. To configure VLANs, go to Network > VLAN > VLANSecondary ConnectionSelect the secondary connection type according to the requirements of your ISP.ConnectionSelect the secondary connection process.Dynamic IP: If you select the secondary connection type as Static IP, you need to configure IP AddressVPN Server/ Domain NameEnter the VPN Server/Domain Name provided by your ISP.Static IP: If you select the secondary connection type as Static IP, you need to configure IP AddressPrimary/ Secondary connection.Enter the elected as provided by your ISP.PrimaryEnter the IP address provided by your ISP for the secondary connection.PrimaryEnter the default gateway provided by your ISP for the secondary connection.Connect/Enter the IP address provided by your ISP for the secondary connection.Primary/ Secondary Con		Maximum Upstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of each WAN port after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings
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.VLANAdd the WAN port to a VLAN. Generally, Generally, you don't need to enable VLAN for the WAN port unless required by your ISP.VLAN IDIf VLAN for the WAN port is enabled, you need to enter a VLAN ID. Then the WAN port is automatically assigned to the VLAN. By default, 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 configure its egress rule as TAG. To configure VLANs, go to Network > VLAN > VLAN Secondary Connection is required for L2TP connection. The router will get some necessary information after the secondary connection type as Dynamic IP, the router set up the secondary connection dynamically.Settic IP: If you select the secondary connection type as Static IP, you need to configure IP. Hodress, Subnet Mask, Default Gateway, Primary/Second DNS for the secondary connection.VPN Server/ Domain NameEnter the VPN Server/Domain Name provided by your ISP for the secondary connection.UP AddressEnter the default gateway provided by your ISP for the secondary connection.Subnet MaskEnter the default gateway provided by your ISP for the secondary connection.Primary/ Secondary DNSEnter the primary/Secondary DNS provided by your ISP for the secondary connection.		the Maximum Downstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of each WAN port after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic
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.VLANAdd the WAN port to a VLAN. Generally, Generally, you don't need to enable VLAN for the WAN port unless required by your ISP.VLAN IDIf VLAN for the WAN port is enabled, you need to enter a VLAN ID. Then the WAN port is automatically assigned to the VLAN. By default, the egress rule of the VLAN by the UAN. By default, the egress rule of the VLAN tags. is UNTAG, so the packets are transmitted by the WAN port without VLAN tags. you want the WAN port to transmit packets with VLAN tag, you need to configure its 	MTU	Specify the MTU (Maximum Transmission Unit) of the WAN port.
Secondary DNSVLANAdd the WAN port to a VLAN. Generally, Generally, you don't need to enable VLAN for the WAN port unless required by your ISP.VLAN IDIf VLAN for the WAN port is enabled, you need to enter a VLAN ID. Then the WAN port is automatically assigned to the VLAN. By default, 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 configure its egress rule as TAG. To configure VLANs, go to Network > VLAN > VLAN.SecondarySelect the secondary connection type according to the requirements of your ISP. The secondary connection is required for L2TP connection. The router will get some necessary information after the secondary connection type as Dynamic IP, the router set up the secondary connection process.Dynamic IP: If you select the secondary connection type as Dynamic IP, the router set up the secondary connection dynamically.Static IP: If you select the secondary connection type as Static IP, you need to configure IP Address, Subnet Mask, Default Gateway, Primary/Second DNS for the secondary connection.VPN Server/ Domain NameEnter the VPN Server/Domain Name provided by your ISP for the secondary connection.VPN Server/ Domain NameEnter the default gateway provided by your ISP for the secondary connection.Default GatewayEnter the default gateway provided by your ISP for the secondary connection.Primary/ Secondary DNSEnter the primary/secondary DNS provided by your ISP for the secondary connection.		
for the WAN port unless required by your ISP.VLAN IDIf VLAN for the WAN port is enabled, you need to enter a VLAN ID. Then the WAN port is automatically assigned to the VLAN. By default, 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 configure its egress rule as TAG. To configure VLANs, go to Network > VLAN > VLAN.SecondarySelect the secondary connection type according to the requirements of your ISP. The secondary connection is required for L2TP connection. The router will get some necessary information after the secondary connection succeeded. The information will be used in the L2TP connection process. Dynamic IP: If you select the secondary connection type as Dynamic IP, the router set up the secondary connection dynamically. Static IP: If you select the secondary connection type as Static IP, you need to configure IP Address, Subnet Mask, Default Gateway, Primary/Second DNS for the secondary connection.VPN Server/ Domain NameEnter the IP address provided by your ISP for the secondary connection.Default GatewayEnter the default gateway provided by your ISP for the secondary connection.Primary/ Secondary DNSEnter the primary/secondary DNS provided by your ISP for the secondary connection.		(Optional) Enter the IP address of the DNS server provided by your ISP.
port is automatically assigned to the VLAN. By default, 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 configure its egress rule as TAG. To configure VLANs, go to Network > VLAN > VLAN.Secondary ConnectionSelect the secondary connection type according to the requirements of your ISP. The secondary connection is required for L2TP connection. The router will get some necessary information after the secondary connection type as Dynamic IP, the router set up the secondary connection dynamically.VPN Server/ Domain NameEnter the VPN Server/Domain Name provided by your ISP. for the secondary connection.Subnet MaskEnter the lP address provided by your ISP for the secondary connection.Default GatewayEnter the default gateway provided by your ISP for the secondary connection.Primary/ Secondary DNSEnter the primary/secondary DNS provided by your ISP for the secondary connection.Connect/Click the button to active/terminate the connection.	VLAN	
ConnectionThe secondary connection is required for L2TP connection. The router will get some necessary information after the secondary connection succeeded. The information will be used in the L2TP connection process.Dynamic IP: If you select the secondary connection type as Dynamic IP, the router set up the secondary connection dynamically.Static IP: If you select the secondary connection type as Static IP, you need to configure IP Address, Subnet Mask, Default Gateway, Primary/Second DNS for the secondary connection.VPN Server/ Domain NameEnter the VPN Server/Domain Name provided by your ISP.IP AddressEnter the IP address provided by your ISP for the secondary connection.Subnet MaskEnter the default gateway provided by your ISP for the secondary connection.Pefault GatewayEnter the default gateway provided by your ISP for the secondary connection.Primary/ Secondary DNSEnter the primary/secondary DNS provided by your ISP for the secondary connection.Connect/Click the button to active/terminate the connection.	VLAN ID	port is automatically assigned to the VLAN. By default, 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 configure its
set up the secondary connection dynamically.Static IP: If you select the secondary connection type as Static IP, you need to configure IP Address, Subnet Mask, Default Gateway, Primary/Second DNS for the secondary connection.VPN Server/ Domain NameEnter the VPN Server/Domain Name provided by your ISP.IP AddressEnter the IP address provided by your ISP for the secondary connection.Subnet MaskEnter the lP address provided by your ISP for the secondary connection.Default GatewayEnter the default gateway provided by your ISP for the secondary connection.Primary/ Secondary DNSEnter the primary/secondary DNS provided by your ISP for the secondary connection.Connect/Click the button to active/terminate the connection.		The secondary connection is required for L2TP connection. The router will get some necessary information after the secondary connection succeeded. The information
configure IP Address, Subnet Mask, Default Gateway, Primary/Second DNS for the secondary connection.VPN Server/ Domain NameEnter the VPN Server/Domain Name provided by your ISP.IP AddressEnter the IP address provided by your ISP for the secondary connection.Subnet MaskEnter the subnet mask provided by your ISP for the secondary connection.Default GatewayEnter the default gateway provided by your ISP for the secondary connection.Primary/ Secondary DNSEnter the primary/secondary DNS provided by your ISP for the secondary connection.Connect/Click the button to active/terminate the connection.		
Domain NameIP AddressEnter the IP address provided by your ISP for the secondary connection.Subnet MaskEnter the subnet mask provided by your ISP for the secondary connection.Default GatewayEnter the default gateway provided by your ISP for the secondary connection.Primary/ Secondary DNSEnter the primary/secondary DNS provided by your ISP for the secondary connection.Connect/Click the button to active/terminate the connection.		configure IP Address, Subnet Mask, Default Gateway, Primary/Second DNS for the
Subnet MaskEnter the subnet mask provided by your ISP for the secondary connection.Default GatewayEnter the default gateway provided by your ISP for the secondary connection.Primary/ Secondary DNSEnter the primary/secondary DNS provided by your ISP for the secondary connection.Connect/Click the button to active/terminate the connection.		Enter the VPN Server/Domain Name provided by your ISP.
Default GatewayEnter the default gateway provided by your ISP for the secondary connection.Primary/ Secondary DNSEnter the primary/secondary DNS provided by your ISP for the secondary connection.Connect/Click the button to active/terminate the connection.	IP Address	Enter the IP address provided by your ISP for the secondary connection.
Primary/ Secondary DNSEnter the primary/secondary DNS provided by your ISP for the secondary connection.Connect/Click the button to active/terminate the connection.	Subnet Mask	Enter the subnet mask provided by your ISP for the secondary connection.
Secondary DNS connection. Connect/ Click the button to active/terminate the connection.	Default Gateway	Enter the default gateway provided by your ISP for the secondary connection.
		Click the button to active/terminate the connection.

Configuring the PPTP

Choose the menu **Network > WAN > SFP WAN/LAN1** to load the following page.

- : 0 0	o c · · ·	
Figure 2-6	Configuring t	The PPTP

Connection Configuration			Connection Status	
Connection Type:	РРТР		Connection Status	Disconnected
Username:			IP Address	0.0.0.0
Password:	> ₁	c .	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 (100-100000)	Secondary DNS	0.0.0.0
MTU:	1420	(576-1420)	Secondary Connection	on
Primary DNS:		(Optional)	IP Address	0.0.0.0
Secondary DNS:		(Optional)	Subnet Mask	0.0.0.0
Vlan:	Enable		Default Gateway	0.0.0.0
Vlan ID:	4094	(1-4094)	Primary DNS	0.0.0.0
Secondary Connection:	Oynamic IP O Static I	Ρ	Secondary DNS	0.0.0.0
VPN Server IP/Domain Name:				
IP Address:				
Subnet Mask:				
Default Gateway:		(Optional)		
Primary DNS:		(Optional)		
Secondary DNS:		(Optional)		
Save Connect Disc	onnect			

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	Choose the connection mode, including Connect Automatically , Connect Manually and Time-Based.
	Connect Automatically: The router will activate the connection automatically when the router reboots or the connection is down.
	Connect Manually: You can manually activate or terminate the connection.
	Time-Based: During the specified period, the router will automatically activate the connection.
Time	Choose the time range for automatic connection. To create the time range, go to Preferences > Time Range > Time Range .

Upstream Bandwidth	Specify the upstream bandwidth of the WAN port. This value is the upper limit of the Maximum Upstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of each WAN port after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
Downstream Bandwidth	Specify the downstream bandwidth of the WAN port. This value is the upper limit of the Maximum Downstream Bandwidth on Transmission > Bandwidth Control page. Also, this value determines the bandwidth ratio of each WAN port after Bandwidth Based Balance Routing is enabled on Transmission > Load Balancing > Basic Settings page.
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 enable VLAN for the WAN port unless required by your ISP.
VLAN ID	If VLAN for the WAN port is enabled, you need to enter a VLAN ID. Then the WAN port is automatically assigned to the VLAN. By default, 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 configure its egress rule as TAG. To configure VLANs, go to Network > VLAN > VLAN .
Secondary Connection	Select the secondary connection type according to the requirements of your ISP. The secondary connection is required for PPTP connection. The router will get some necessary information after the secondary connection succeeded. The information will be used in the PPTP connection process.
	Dynamic IP: If you select the secondary connection type as Dynamic IP, the router set up the secondary connection dynamically.
	Static IP: If you select the secondary connection type as Static IP, you need to configure IP Address, Subnet Mask, Default Gateway, Primary/Second DNS for the secondary connection.
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.
- Reserve IP addresses for certain LAN clients

3.1 Configuring the IGMP Proxy

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

Figure 3-1 Configuring the LAN IP Address

LAN	DHCP Clie	nt List	Address Reser	vation				
Settings								
IGMP Prox	y:	✓ El	nable					
IGMP Versi	ion:	V2	!	•				
IGMP Inter	rface:	W	AN/LAN4	•				
Save Note: IGMP only	takes effe	ct when WAN	I mode is enat	oled for port WAN.				
Network Li	ist							
								🔂 Add
	ID	Name	Vlan	IP Address	Subnet Mask	DHCP Server	DHCP Relay	Operation
	1	LAN	1	192.168.0.1	255.255.255.0	Enabled	Disabled	Ø

In the **Settings** section, enable IGMP Proxy, select the corresponding parameters and click **Save**.

IGMP Proxy If you want the local network devices to receive multicast data from the Internet, check the box to enable IGMP Proxy. This feature is used to detect whether there is any multicast member connected to the LAN ports.

IGMP Version	Configure the IGMP version as V2 or V3 according to your ISP.
IGMP Interface	Select the interface on which the IGMP Proxy takes effect.
 Note: IGMP only takes effect when WAN mode is enabled for port WAN. 	

Figure 3-2 Configuring the LAN network

Network	List							
								🕁 Add
	ID	Name	Vlan	IP Address	Subnet Mask	DHCP Server	DHCP Relay	Operation
	1	LAN	1	192.168.0.1	255.255.255.0	Enabled	Disabled	ø

In the **Network List** section, set up the LAN network or click **Add** to add new networks, and configure the related parameters.

Name	set up the LAN network or click Add to add new networks, and configure the related parameters.
IP Address	Enter the IP address of the LAN port. To make your local network devices connect to the internet, you need to set the IP address of the LAN port as the default gateway of those devices.
Subnet Mask	Enter the subnet mask of the LAN port (255.255.255.0 by default). The IP addresses of all devices which connect to the LAN ports should be in the same subnet as the IP address of the LAN port.
VLAN	Specify the VLAN of the LAN port, only the devices in the specified VLAN can access and manage the gateway.

DHCP Mode DHCP Server	If you select DPCP Server as DHCP Mode, the DHCP server of the gateway will assign IP addresses to the LAN clients. Configure the following parameters.
	Status: Check the box to enable DHCP Server.
	Starting IP Address / Ending IP Address: Enter the starting IP address and ending IP address of the DHCP server's IP pool. The IP pool defines the range of IP addresses that can be assigned to the LAN clients. Note that the starting IP address and ending IP address should be in the same subnet as 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 fails, the client will have to stop using that IP address when the lease finally expired, and try to get a new IP address from another DHCP server.
	Default Gateway: (Optional) Enter the default gateway which is assigned by the DHCP server. It is recommended to enter the IP address of the LAN port.
	Default Domain: (Optional) Enter the domain name of your network.
	Primary DNS / Secondary DNS: (Optional) Enter the DNS server address provided by your ISP. If you are not clear, please consult your ISP.
	Option60: (Optional) Enter the value for DHCP Option 60. DHCP clients use this field to optionally identify the vendor type and configuration of a DHCP client. Mostly, it is used in the scenario where the APs apply for different IP addresses from different servers according to the needs. For detailed information, please consult the vendor. For TP-Link, this entry should be TP-Link.
	Option66: (Optional) Enter the value for DHCP Option 66. It specifies the TFTP server information and supports a single TFTP server IP address.
	Option67: (Optional) Enter the value for DHCP Option 67. It specifies the boot file name.
	Option138: (Optional) Enter the value for DHCP Option 138. It is used in discovering the devices by the Omada controller.
	Option150: (Optional) Enter the value for DHCP Option 150. It specifies the TFTP server information and supports multiple TFTP server IP addresses.
	Option159: (Optional) Enter the value for DHCP Option 159. This option is used to configure a set of ports bound to a shared IPv4 address.
	Option160: (Optional) Enter the value for DHCP Option 160. This option is used to configure DHCP captive portal.
	Option176: (Optional) Enter the value for DHCP Option 176. This option is used to configure parameters for IP phones.
	Option242: (Optional) Enter the value for DHCP Option 242. This option is used to provide the TMS address automatically.

DHCP Mode DHCP Relay	If you select DHCP Relay as DHCP Mode, the gateway will relay DHCP requests from LAN clients to the DHCP server in another network. Then the DHCP server will assign IP addresses to the LAN clients. Configure the following parameters.
	Status: Check the box to enable DHCP Relay.
	Server Address: Enter the IP address of the DHCP server.

3.2 Viewing the DHCP Client List

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

Figure 3-3 Viewing the DHCP Client List

DHCP Clier	nt List				
Total Clien	ts: 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 host name of the DHCP client. It should be composed of digits, English letters, dashes and underscores only.
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.

3.3 Configuring the Address Reservation

Configuring the Address Reservation

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

Figure 3-4 Configuring the Address Reservation

	ID	М	IAC Address		IP Address	Description	Status	Operation
	C Address:							
	Address: scription:				(Optional)			
Exp	port to IP-MAC	Binding:	Enable					
IP-	MAC Binding I	nterface:	LAN	•				
Sta	atus:		 Enable 					
	ОК Са	ancel						

Configure the parameters for the address reservation entry, including MAC address, IP Address, and so on, 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.

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) Enable IPTV globally.
- 2) Chose the Wan Port according to your ISP.
- 3) Select the appropriate Mode 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	
Settings		
IPTV:	Enable IPTV	
Wan Port:	SFP WAN/LAN1	•
Mode:	Bridge	•
WAN/LAN3:	Internet	•
WAN/LAN4:	Internet	•
WAN/LAN5:	Internet	•
WAN/LAN6:	Internet	•
Save		
Note:		

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

In the **Settings** section, 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 config WAN port	ure Internet VLAN ID, please go to WAN Configuration and configure on the corresponding t.

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 router, you can just set the MAC address of this router'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.

Interface Name	Current MAC Address	MA	C Clone
SFP WAN/LAN1	40-ED-00-52-BB-DE	Restore Factory MAC	Clone Current PC's MAC
WAN2	04-D4-C4-AE-6D-CF	Restore Factory MAC	Clone Current PC's MAC
LAN	40-ED-00-52-BB-DC		
		Current MAC A	uddress

Figure 5-1 Configuring MAC Address

Configure the MAC address of the WAN 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	MAC Clone provides a shortcut to changing the MAC Address.
	Restore Factory MAC : Click this button to restore the MAC address to the factory default value.
	Clone Current PC's MAC : Click this button to clone the MAC address of the PC you are currently using to configure the router. It's only available for the WAN ports.

Note:

When cloning curent 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 router provides some basic switch port management function, including **Statistics**, **Port Mirror**, **Rate Control**, **Port Config**, **Port Status** and **DDM Status**.

6.1 Viewing the Statistics

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

Figure 6-1 Viewing the Statistics

Packet Type		Port1	Port3	Port4	Port5	Port6
	Unicast	0	13020	0	0	0
	Broadcast	0	77	0	0	0
	Pause	0	0	0	0	0
Received	Mulitcast	0	3850	0	0	0
Received	Total	0 B	3.0 MB	0 B	0 B	0 B
	Undersize	0	0	0	0	0
	Normal	0	16947	0	0	0
	Oversize	0	0	0	0	0
	Unicast	0	15920	0	0	0
	Broadcast	3	5276	0	0	0
Transmitted	Pause	0	0	0	0	0
	Mulitcast	0	0	0	0	0
	Total	1038 B	9.8 MB	0 B	0 B	0 B

You can view the detailed traffic information of each port, which facilitates you to monitor the traffic and manage the network effectively.

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).
Refresh	Click Refresh to view the latest traffic statistics of each port.
Clear	Click Clear to clear all the traffic statistcs.
Note: Error Fra	ame: The frames that have a false checksum.

Maximum frame length: The maximum frame length supported by the router. 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 router to forward packet copies of the monitored ports 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.

Enable Port Mirror		
Mirror Mode:	Ingress and Egress	
Monitor List		
	Mirroring Port	Mirrored Port
	O Port1	✓ Port1
	O Port3	Port3
	O Port4	Port4
	O Port5	Port5
	Port6	Port6

Figure 6-2 Configuring Port Mirror

Follow these steps to configure Port Mirror:

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

2)

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.
In the Monitor L Save.	L ist section, set the mirroring port and the mirrored port(s), then click
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

Rate Control enables you to set limit to the traffic rate for the specific packets on each port to manage the traffic flow of your network.

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

Figure 6-3	Configuring Rate Control

Port	Ingress Limit	Ingress Frame Type	Ingress Rate(Mbps)	Egress Limit	Egress Rate(Mbp
Port1	Enable	All Frames 💌	1000	Enable	1000
Port3	Enable	All Frames 🔻	1000	Enable	1000
Port4	Enable	All Frames 💌	1000	Enable	1000
Port5	Enable	All Frames 🔻	1000	Enable	1000
Port6	Enable	All Frames 🔹	1000	Enable	1000

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	Specify the ingress frame type to be limited. It is All Frames by default.				
Туре	All Frames: The ingress rate of all frames is limited.				
	Broadcast: The ingress rate of broadcast frames is limited.				
	Broadcast and Multicast : The ingress rate of broadcast and multicast 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	Enable	Auto 🔻
Port2	Enable	Auto 🔻
Port3	Enable	Auto 💌
Port4	Enable	Auto 💌
Port5	Enable	Auto 💌
Port6	🗌 Enable	Auto 🔻

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 select Auto (Auto-negoation), or manually select the speed and duplex mode.

6.5 Viewing Port Status

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

Figure 6-5 Viewing Port Status

Port	Status	Speed(Mbps)	Duplex Mode	Flow Control
Port1	Link Down			
Port2	Link Down			
Port3	Link Up	1000M	Full-duplex	Disabled
Port4	Link Down			
Port5	Link Down			
Port6	Link Down			
resh				

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.

6.6 Viewing DDM Status

The DDM (Digital Diagnostic Monitoring) function is used to monitor the status of the SFP modules inserted into the SFP ports on the switch. The user can choose to shut down the monitored SFP port automatically when the specified parameter exceeds the alarm threshold or warning threshold. The monitored parameters include: Temperature, Voltage, Bias Current, Tx Power and Rx Power.

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

Figure 6-6 Viewing Port Status

DDM Status								
Total: 0								
Port	Temperature (°C)	Voltage (V)	Bias Current (mA)	TX Power (mW)	RX Power (mW)	Transmit Fault	Loss of Signal	Data Ready

7 VLAN Configuration

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.

For VLAN configuration, you can:

- Create VLANs and add the desired ports to the VLANs.
- Configure the PVID of the ports.

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

VLAN List

					🔂 Add	🗢 Delete
ID	VLAN ID	Name		Ports	Description	Operation
VLAN ID:				(1-4086)		
Name:				(1-50 characters)		
Ports:			TAG	•		
		3	TAG	•		
		□ 4	TAG	•		
		5	TAG	-		
			TAG	•		
Description:				(1-50 characters, optional)		
OK	Can	cel				
1	1	vlan1	3(UNTAG) 4(UI	NTAG) 5(UNTAG) 6(UNTAG)	LAN1	0
2	4094	vlan4094		1(UNTAG)		0

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
 Check the box to add the desired port to the VLAN and specify the port type in the specified VLAN. The port can be divided into two types: TAG or UNTAG.

 TAG: The egress rule of the packets transmitted by the port is tagged.

 UNTAG: The egress rule of the packets transmitted by the port is untagged. If the desired egrees the packet is greated by the port is untagged. If the desired egrees the packet is greated by the port is untagged.

UNIAG: The egress rule of the packets transmitted by the port is untagged. If the device connected to the port is an end device, like a PC or a server, the port type should be UNTAG, because end devices don't recognize tagged packets.

Description (Optional) Enter a brief description for easy management and searching.

VLAN List						
					Ø	Add 😑 Delete
	ID	VLAN ID	Name	Ports	Description	Operation
	1	1	vlan1	3(UNTAG) 4(UNTAG) 5(UNTAG) 6(UNTAG)	LAN1	2
	2	4094	vlan4094	1(UNTAG)		2

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

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.

Mote:

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

7.2 Configuring the PVID of a Port

PVID indicates the default VLAN for the corresponding port. Untagged packets which are received by the port are tagged with the PVID and then transmitted within the corresponding VLAN.

For example, if Port 2 is in both VLAN 10 and VLAN 20, and the PVID of the port is 10, when Port 2 receives an untagged packet from a PC, the packet is transmitted within VLAN 10, but cannot reach VLAN 20 directly.

To Configure the PVID of the port, choose the menu Network > VLAN > Ports to load the following page.

Figure 7-2 Configuring the PVID

Port	PVII	D	VLAN
Port1	4094	•	4094(UNTAG)
Port3	1	•	1(UNTAG)
Port4	1	•	1(UNTAG)
Port5	1	•	1(UNTAG)
Port6	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 following IPv4. You can configure IPv6 network for the router 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 LANs.
- Configure IPv6 for the WAN/SFP WAN port(s). You can configure IPv6 for multiple WANs, and each WAN port has its own Internet Connection Type and parameters.

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

Choose the menu Network > IPv6 > SFP WAN/LAN1 to load the following page.

In the General section, enable IPv6 and click Save.

Figure 8-2 Select Internet Connection Type

General	
10 <i>c</i>	
IPv6:	Enable
Save	
Internet	
Internet Connection Type:	•
	Static IP
	Dynamic IP (SLAAC/DHCPv6)
	PPPoE
	6to4 Tunnel
	Pass-Through (Bridge)

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

InternetChoose the proper Internet Connection Type according to the requirements of yourConnection TypeISP.

8.2 Configuring the WAN Connection

The router 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 > SFP WAN/LAN1** to load the following page.

Figure 8-3 Configuring the Static IP

General		
IPv6:	Enable	
Save		
Internet		
Internet Connection Type:	Static IP	•
IPv6 Address:		
Prefix Length:		(1-128)
Default Gateway:		
Primary DNS:		
Secondary DNS:		
Save		

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

IPv6 Address/Enter these parameters as provided by the ISP.Prefix Length/Default Gateway/Primary DNS/Secondary DNS

Configuring the Dynamic IP (SLAAC/DHCPv6)

Choose the menu **Network > IPv6 > SFP WAN/LAN1** to load the following page.

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

General		
IPv6:	✓ Enable	
Save		
Internet		
Internet Connection Type:	Dynamic IP (SLAAC/DHCPv6)	•
IPv6 Address:		
Primary DNS:		
Secondary DNS:		
Secondary DNS:		
Renew Release		
Advanced		
. Advanced		
Save		

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.
Auto	Select Auto to get an IPv6 address automatically.
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.
Prefix Delegation Size	With Prefix Delegation enabled, enter the Prefix Delegation Size to determine the length of the address prefix. You can get this value from your ISP.
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 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 > SFP WAN/LAN1** to load the following page.

Figure 8-5 Configuring the PPPoE

General	
IPv6:	✓ Enable
Internet	
Internet Connection Type:	PPPoE Image: The second seco
Username:	
Password:	
IPv6 Address:	
 Advanced 	
Connect Disconnect	
Save	

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.
Auto	Select Auto to get an IPv6 address automatically.

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.
Prefix Delegation Size	With Prefix Delegation enabled, enter the Prefix Delegation Size to determine the length of the address prefix. You can get this value from your ISP.
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.
Connect	Click this button to connect to the internet.
Disconnect	Click this button to disconnect from the internet.

Configuring the 6to4 Tunnel

Choose the menu **Network > IPv6 > SFP WAN/LAN1** to load the following page.

Figure 8-6 Configuring the 6to4 Tunnel

General	
IPv6:	🕑 Enable
Save	
Internet	
Internet Connection Type:	6to4 Tunnel 🔹
IPv4 Address:	0.0.0.0
IPv4 Subnet Mask:	0.0.0.0
IPv4 Default Gateway:	0.0.0.0
,	
Tunnel Address:	
Advanced	
0	

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	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	Click 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 > SFP WAN/LAN1** to load the following page.

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

General	
IPv6:	✓ Enable
Save	
Internet	
Internet Connection Type:	Pass-Through (Bridge)
Save	

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

eneral					
	ID	Name(Vlan)	Assigned Type	Address	Operation
	1	LAN(1)	None	fe80::42ed:ff:fe52:bbdc/64	ø

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 T	ype 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.
Not	e:
•	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.
٠	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

G	General					
		ID	Name(Vlan)	Assigned Type	Address	Operation
		1	LAN(1)	None	fe80::214:78ff:fe00:0/64	
	Assi IPve DHC Lea: DNS Add	I(VLAN): igned Type: 5 Address: CP Range se Time: 5 Address: iress: OK Ca	1 DHC • Aut	minutes. (The defaul	/	

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

IPv6 Address Enter the IPv6 address and prefix length (subnet mask).			
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.		
DHCP Range	Enter the starting and ending IPv6 address to define a range for the DHCPv6 server to assign dynamic IPv6 addresses.		
Lease Time	The duration time in minutes when the assigned IPv6 address remains valid. Either keep the defualt 1440 minutes or change it if required.		
DNS Address	Select a method to configure the DNS server for the LAN, with Auto selected, the DNS server addresses are automatically obtained. With Manual DNS selected, manually enter the primary and secondary DNS server addresses provided by your ISP.		
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 8-10 Configuring the SLAAC+Stateless DHCP

General					
	ID	Name(Vlan)	Assigned Type	Address	Operation
	1	LAN(1)	None	fe80::214:78ff:fe00:0/64	
Ass Prei Add DNS	I(VLAN): igned Type: fix: lress Prefix: S Address: lress:		+Stateless DHCP I Prefix Get from Pref Manual DNS	fix Delegation /64	
OK Cancel					

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

Prefix	Configure the IPv6 address prefix for each client in the local network. WIth Manual Prifix selected, enter the prefix in the Address Prefix field. With Get from Prefix Delegation selected, select hte IPv6 Prefix Delegation WAN port, and enter the IPv6 Prefix ID to get a prefix delegation from the ISP.
IPv6 Prefix Delegation WAN	Enter the IPv6 Prefix Delegation WAN port and the IPv6 Prefix ID to get a prefix delegation from the ISP.
IPv6 Prefix ID	With Get from Prefix Delegation selected, enter the Prefix ID, which will be addred to the prefix to obtain a /64 subnet. The range of IPv6 Prefix ID is determined by Prefix Delegation Size and Prefix Length.
DNS Address	Select a method to configure the DNS server for the LAN. With Auto selected, the DNS server addresses are automatically obtained. With Manual DNS selected, manually enter the primary and secondary DNS server addresses provided by your ISP.
Address	Displays the IPv6 address automatically generated by Prefix.

Configuring the SLAAC+RDNSS

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

Figure 8-11 Configuring the SLAAC+RDNSS

General							
	ID	Name(Vlan)	Assigned Type	Address	Operation		
	1		None	fe80::214:78ff:fe00:0/64			
Ass Pre Add	1 LA LAN(VLAN): Assigned Type: Prefix: Address Prefix: DNS Address: Address: OK Cancel		C+RDNSS ual Prefix O Get from Pref O Manual DNS	fix Delegation /64			

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

Prefix	Configure the IPv6 address prefix for each client in the local network. WIth Manual Prifix selected, enter the prefix in the Address Prefix field. With Get from Prefix Delegation selected, select hte IPv6 Prefix Delegation WAN port, and enter the IPv6 Prefix ID to get a prefix delegation from the ISP.
IPv6 Prefix Delegation WAN	Enter the IPv6 Prefix Delegation WAN port and the IPv6 Prefix ID to get a prefix delegation from the ISP.
IPv6 Prefix ID	With Get from Prefix Delegation selected, enter the Prefix ID, which will be addred to the prefix to obtain a /64 subnet. The range of IPv6 Prefix ID is determined by Prefix Delegation Size and Prefix Length.
DNS Address	Select a method to configure the DNS server for the LAN. With Auto selected, the DNS server addresses are automatically obtained. With Manual DNS selected, manually enter the primary and secondary DNS server addresses provided by your ISP.
Address	Displays the IPv6 address automatically generated by Prefix.

Configuring the pass-through

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

Figure 8-12 Configuring the pass-through

General					
	ID	Name(Vlan)	Assigned Type	Address	Operation
	1 LAN(1		None	fe80::214:78ff:fe00:0/64	
LAN(VLAN): 1					
Assi	gned Type:	passi	through 🔻		
IPv6 Passthrough WAN:		WAN:			
	OK Car	ncel			

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

IPv6 Passthro WAN	ough Select the WAN port using Pass-Through (Bridge) for the IPv6 connection.
Note	
	f 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.
	f 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.

3) In the **Prefix Delegation Server** section, check the box to enable **Prefix Delegation**, click **Add** to add a Prefix Delegation Server. Then click **OK**.

Prefix Delegation Server prefix Delegation									
Prefix Delegation: Enable Ena									
	ID	LAN	WAN	Address Prefix	Prefix Length	Prefix ID	New Prefix	DUID	Action
							In a complex netwo	rk where-all the d	levices are ARP
LAN: WAN: Prefix: Prefix Length: Prefix ID:									
New Prefix: Link-local Address: DUID: OK Cancel			separating e	256 hexadecima each two numb 5:00:14:78:00.	ers by colon, such				

Specify the LAN port to which the requesting router will connect.

WAN	Select the WAN port to obtain the delegated prefix.
Prefix	Displays the prefix delegated by the selected WAN port. (Note: You need to enable Prefix Delegation for the corresponding WAN port. Follow the steps: Go to Network > IPV6 > WAN, set Internet Connection Type to Dynamic IP, and enable Prefix Delegation in Advanced.)
Prefix Length	Displays the length of the prefix to be applied. (Note: To set the prefix length, go to Network > IPV6 > WAN, set Internet Connection Type to Dynamic IP, and set the Prefix Delegation Size in Advanced.)
Prefix ID	Specify the value of the remaining bits if the configured Prefix Length is greater than the Prefix Length allocated by the original WAN port.
New Prefix	Displays the prefix to be applied.
Link-local Address	Specify the link-local IPv6 address of the device to apply the prefix.
DUID	The ID of the device to be apply the prefix.

Part 5 USB

CHAPTERS

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

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.

3G/4G						
USB Modem: No USB modem connected.						
Config Type:	Auto	•				
Location:	Argentina	•				
Mobile ISP:	Claro	•				
Connection Mode:	Connect Automatically					
	O 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. 				
PDP Type:	IPv4	•				
MTU Size(in bytes):	1480 The default is 1480, do not chan (If you use a USB-to-RJ45 device MTU to 1500)	ge unless necessary. e, please modify the				
Use The following Enable DNS Servers:						
Connect Disconnected						
Save						

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.

USB Modem	Displays the status of the 3G/4G USB modem.
Location	Automatically selects and displays the region when the USB modem and SIM carc 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 ISF 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 Dia Number, APN (Access Point Name), Username and Password that are provided by the ISP.
Connection Mode	Select the connection mode and configure the parameters according to the requirements of your ISP.
	Connect Automatically: In this mode, the Internet connection reconnects automatically anytime it gets disconnected.
	Connect Manually: In this mode, you can click the Connect or Disconnect button to control the Internet connection manually.
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 Contro 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	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.
	Auto: If Auto (default), the router automatically determines the authentication type used by the ISP.
	PAP: If PAP (Password Authentication Protocol), the router authenticates with the peer using two handshakes. Select this option if the ISP requires this authentication type.
	CHAP: If CHAP (Challenge Handshake Authentication Protocol), the router authenticates with the peer using three handshakes and validates the peer's identify periodically. Select this option if the ISP requires this authentication type.
MTU Size	The default MTU (Maximum Transmission Unit) size is 1480 bytes. Do not change i unless required by the ISP.

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

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..

3G/4G		
USB Modem:	No USB modem connected.	
Config Type:	Auto 💌	
Location:	Argentina 🔹	
Mobile ISP:	Claro 🔻	
Connection Mode:	Connect Automatically	
	O 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.
PDP Type:	IPv4 💌	
	1480	
MTU Size(in bytes):	The default is 1480, do not change u (If you use a USB-to-RJ45 device, pl MTU to 1500)	
Use The following DNS Servers:	🗌 Enable	
Connect Disconnect	8 Disconnected	
Save		

Figure 2-2 Configuring the USB Modem manually

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	Select the connection mode and configure the parameters according to the requirements of your ISP.
	Connect Automatically: In this mode, the Internet connection reconnects automatically anytime it gets disconnected.
	Connect Manually: In this mode, you can click the Connect or Disconnect button to control the Internet connection manually.
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	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.
	Auto: If Auto (default), the router automatically determines the authentication type used by the ISP.
	PAP: If PAP (Password Authentication Protocol), the router authenticates with the peer using two handshakes. Select this option if the ISP requires this authentication type.
	CHAP: If CHAP (Challenge Handshake Authentication Protocol), the router authenticates with the peer using three handshakes and validates the peer's identify periodically. Select this option if the ISP requires this authentication type.
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.

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 stor	age device.			
Scan				
Disk Drivers		Partition	Total	Operation
Backup				
Click Backup to save a copy	y of your curre	nt settings. It is recomm	nended to back up your settings before changing configurations or upgrad	ding firmware.
Backup:	Config			
	Log			
Choose USB:				
Backup				
Restore				
Restore saved settings fron	n a file.			
Choose USB:				
Restore				

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 upgarding 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 Vf	at 00	▼ : 00 ▼ in UTC.	
Maximum Number of Files:		1-50)		
Data Retention Days:	•			
Saving Path:		Br	owse	
Apply				
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:			Browse
Upgrade			

- 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

In IP Group, you can preset IP 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 IP Group configuration, follow these steps:

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

2.1 Adding IP Address Entries

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

IP Addr	ess List						
						c	🗗 Add 🛛 😑 Delete
	ID	Name	IP Address Type	IP Address Range	IP Address/Mask	Description	Operation
	Name: IP Add Descrip OK	ress Type: otion:	 IP Addre 	ess Range O IP Address/Mask - (Optional)			
	1	IP_LAN	IP Address/Mask		192.168.0.0/24	IP_LAN	

Figure 2-1 Add an IP Address Entry

Follow these steps to add an IP address entry:

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

NameEnter a name for the IP address entry. Only letters, digits or underscores are
allowed.

IP Address Type	Specify the type of the IP address entry. Two types are provided:
	IP Address Range : Specify a starting IP address and an ending IP address. A rule that references the IP address entry will be applied to the IP addresses within the range in the entry.
	IP Address/Mask : Specify a network address and a subnet mask. A rule that references the IP address entry will be applied to the IP 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.

2.2 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

Group Name:				
Address Name:		•		
Description:		(Optional)		
OK Cance	I			

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.

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

2) Click **OK**.

Note:

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

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

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.

IPv6 Addre	ss List				
					<table-cell-rows> Add 🛛 😑 Delete</table-cell-rows>
	ID	Name	IPv6 Address/Mask	Description	Operation
	me: 6 Address/	Mask:		1	
	OK	Cancel	(Optional)		
	1	IPV6_LAN	fe80::0/64,/64	IPV6_LAN	

Figure 3-1 Add an IPv6 Address Entry

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 IP v6address 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.

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

roup List					
					🔂 Add 🛛 🗢 Dele
	ID	Group Name	Address Name	Description	Operation
Add Des	oup Name: dress Name: scription: OK Ca	•	(Optional)	1	
	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 na	ame and configure	e the range to	add an IPv6	address range.
					J.

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

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.

Time Ran	nge List					Add 😑 Delete
	ID	Time R	ange Name	Working Time	Description	Operation
T V	Time Range Time Setting Norking Cale Description: OK	ıs: endar:	 Working Caler Image: A start of the start of	ndar (Optional)		
	1		Any		Any time	

Figure 4-1 Add a Time Range Entry

Follow these steps to add a time range entry:

1) Enter a name for the time range entry.

Time RangeEnter 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.

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
00:00							
01:00							
02:00							
03:00							
04:00							
05:00							
06:00							
07:00							
08:00							
09:00							
10:00							
11:00							
12:00							
13:00							
14:00							
15:00							
16:00							
17:00							
18:00							
19:00							
20:00							
21:00							
22:00							
23:00							
24:00							
4:00	Time						

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
i iguio i o	ivial la l

Time Settings:	O Working Calendar						
Week:	🗌 Mon	🗌 Tue	U Wed	🗌 Thu	🗆 Fri	🗌 Sat	🗌 Sun
Time range:	:	-	:	+			

Week Select the effective days in a week.

Time RangeEnter 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

In VPN IP Pool, you can preset VPN IP pools that will appear as options for you to choose when configuring L2TP VPN and PPTP VPN. After creating the entries, you can apply them to different rules, which saves you from repeatedly setting up the same information.

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

Figure 5-	1 Ad	d an IP Pool Entry			
IP Pool Lis	t				
					🕂 Add 🗧 Delete
	ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
	Pool Nan				
	tarting IP nding 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:

The range of the newly created IP pool cannot overlap with the IP range of the DHCP pool and other existing VPN IP pools.

_ _ _ _ _ _ _ _ _ _

The VPN IP pool entry that has been referenced by a rule cannot be deleted unless the rule no longer references the entry.

6 Service Type Configuration

In Service Type, you can define service type entries that will appear as matching conditions for you to choose when configuring the rules of Access Control in Firewall. The entries in gray are system predefined service types, and they cannot be edited or deleted. You can add other entries if your service type is not in the list.

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

Figure 6-1 Service Type List

Service Type List

					🕂 Add 🛛 😑 Delete
ID	Service Type Name	Protocol	Detail	Description	Operation
 1	ALL	0-255		ALL	
 2	FTP	ТСР	Source Port = 0-65535; Destination Port = 21-21	FTP	
 3	SSH	ТСР	Source Port = 0-65535; Destination Port = 22-22	SSH	
 4	TELNET	ТСР	Source Port = 0-65535; Destination Port = 23-23	TELNET	
 5	SMTP	ТСР	Source Port = 0-65535; Destination Port = 25-25	SMTP	
 6	DNS	UDP	Source Port = 0-65535; Destination Port = 53-53	DNS	
 7	HTTP	ТСР	Source Port = 0-65535; Destination Port = 80-80	НТТР	
 8	POP3	ТСР	Source Port = 0-65535; Destination Port = 110-110	POP3	
 9	SNTP	UDP	Source Port = 0-65535; Destination Port = 123-123	SNTP	
 10	H.323	ТСР	Source Port = 0-65535; Destination Port = 1720-1720	H.323	
 11	ICMP_ALL	ICMP	Type =255; Code = 255	icmp	
 12	HTTPS	ТСР	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 Lis	t				
						🕂 Add 🗢 Delete
	ID	Service Type Name	Protocol	Detail	Description	Operation
	Protocol Source	Port Range:	• TCP OUD	DP O TCP/UDP O ICMP O Other		
	Descript OK	tion Port Range: tion: Cancel		(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.

 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	O UDP	⊖ TCP/UDP	○ ICMP	O 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.

the type and code fields matched are considered as the target packets.

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

Figure 6-4 IC	CMP Protocol					
Protocol:		⊖ TCP			ICMP	○ Other
Type:						
Code:						
Type/Code		Specif	fy the type	e and code o	f the ICMP p	backets. ICM

User Guide = 88

_ _

_ _

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

	Figure 6-5 Other Protocol	S						
	Protocol:	⊖ TCP ⊖	UDP O T	CP/UDP	○ ICMP	Other		
	Protocol Number:							
	Protocol Number	1 5				ets. Packets e target pack	s with the proto kets.	ocol
3)	(Optional) Enter a brie	f descriptio	n of this se	ervice ty	pe to mal	ke identify	ving it easier.	
4)	Click OK .							

Note: A service type entry that is being referenced by a rule cannot be deleted unless the rule no longer references the entry.

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 router 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 router can record the IP address of the host, when the data from the internet returns to the external ports, the router 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

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

Quality of Services

Quality of Services allows you to configure rules to limit various data flows.

Session Limit

Session limit feature limits the number of sessions that specific sources can use. This feature can prevent the network resources and bandwidth from being exhausted by some hosts which use too many sessions at one time, and therefore optimizes network performance.

Load Balancing

You can configure the traffic sharing mode of the WAN ports to optimize the resource utilization and processing capability of servers. The router will switch all the new sessions from dropped lines automatically to the others to keep an always on-line network.

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 router 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.

ID	Name	Interface	Original IP	Translated IP	DMZ Forwarding	Description	Status	Operation
Name:			_					
Interface: Original IP:			•					
Translated IP:								
DMZ Forwarding:		🗌 Enab	le					
Description:				(Optional)				
Status:		💌 Enab	le					
OK	Cancel]						

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 only when the connection type is Static IP. If you choose multiple ports, the entry will be applied to all selected ports simultaneously.
Original IP	Specify the private IP address for the rule. The original IP address cannot be the broadcast address and the IP address of the LAN interface.

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

	Translated IP	Specify the public IP address for the rule. The translated IP address cannot be the broadcast address and the IP address of the WAN 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	(Optional) Enter a brief description for the rule 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.

When setting open ports for NAT, do not select the reserved ports (1723/1701 is reserved for PPTP/ L2TP, 1194 is reserved for OpenVPN, and the specific ports you reserved).

2.2 Configuring the Virtual Servers

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

Figure 2-2 Conliguring the virtual Serve	Figure 2-2	Configuring the Virtual Servers
--	------------	---------------------------------

ID	Name		Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
Name:									
Interface:				•					
External Port:					(XX or XX-X	X ,1-65535)			
Internal Port:					(XX or XX-X	X,1-65535)			
Internal Server IP:									
Pro	Protocol: ALL			•					
Sta	itus:	💌 Enab	le						
	OK Cancel								

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 of the router for external network access. The ports or port ranges cannot overlap with those of other virtual server rules.

Internal Port	Enter the service port or port range of the router for external network access. The ports or port ranges cannot overlap with those of other virtual server rules.
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 rule.
	ALL: Data packets are transmitted based on TCP or UDP protocols.
	TCP: Data packets are transmitted based on TCP protocol.
	UDP: Data packets are transmitted based on UDP protocol.
Status	Check the box to enable the rule.

2.3 Configuring the Port Triggering

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

Figure 2-5 Configuring the Fort mygening	Figure 2-3	Configuring the Port Triggering
--	------------	---------------------------------

ID	Interface	Name	Trigger Port	Trigger Protocol	Incoming Port	Incoming Protocol	Status	Operation
Interfac	e:		•					
Name:								
Trigger Port:				(XX or XX-XX)				
Trigger Protocol:		TCP/UDP	•					
Incoming Port:				(XX or XX-XX)				
Incoming Protocol: TCP/UDP		•						
Status:		Enable						
OK	Cancel							

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 from which the data flows out. Each entry supports at most 5 groups of trigger ports. For example, you can enter 1 or 1-2. Note that the ports or port ranges cannot overlap with those of other port triggering rules.

Trigger Protocol	Specify the protocol for the trigger port.
	ALL: Data packets are transmitted based on TCP or UDP protocols.
	TCP: Data packets are transmitted based on TCP protocol.
	UDP: Data packets are transmitted based on UDP protocol.
Incoming Port	Enter the incoming port or port range from which the data is received. Each entry supports at most 5 groups of incoming ports. For example, you can enter 1-2 or 11-12. Note that the ports or port ranges cannot overlap with those of other port triggering rules.
Incoming Protocol	Specify the protocol for the incoming port.
	ALL: Data packets are transmitted based on TCP or UDP protocols.
	TCP: Data packets are transmitted based on TCP protocol.
	UDP: Data packets are transmitted based on UDP protocol.
Status	Check the box to enable the rule.
Click OK	

2.4 Configuring the NAT-DMZ

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

	ID	Nan	ne Interf		rface	Host IP Address	Status	Operation
				-	-			
In	ame: iterface: ost IP Ado	fress:		•				
St	tatus:		 Enable 					
	ОК	Cancel						

Figure 2-4 Configuring the NAT-DMZ

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.
Host IP Address	Specify the host IP address for NAT-DMZ.
Status	Check the box to enable the rule.

2.5 Configuring the ALG

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

Figure 2-5 Configuring the ALG

ALG
✓ FTP ALG
✓ H.323 ALG
PPTP ALG
✓ SIP ALG
✓ IPSec ALG
Save

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.

Bandwidth (Bandwidth Control Config								
🗌 Enable B	andwidth Control								
Enable Bandwidth Control when bandwidth usage reaches 0 %									
Save									
Bandwidth (Bandwidth Control Rule List								
								•	
								🔂 Add	Delete
	D Name	Direction	Group	Maximum Upstream Bandwidth	Maximum Downstream Bandwidth	Mode	Effective Time	Status	Operation

Figure 3-1 Configuring the Bandwidth Control

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.
Bandwidth Control Threshold	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.

	ID	Name	Direction	Group	Maximum Upstream Bandwidth	Maximum Downstream Bandwidth	Mode	Effective Time	Status	Operation
	Name:									
	Direction	1:		•						
	Group:		IPGROUP_	ANY 🔻						
	Maximum Upstream 1000			Kbps(100-10	000000)					
	Maximum Downstream 1000 Bandwidth:			Kbps(100-10	000000)					
	Mode: Shared Individual									
	Effective Time: Any			•						
	Description:			(Optional)						
	ID:			(Optional)						
Status: 🕑 Enable										
	ОК	Cancel								

Figure 3-2 Add Bandwidth Control rules

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	Select the IP groups you have created from the drop-down list. With IPGROUP_ ANY selected, the rule will apply to all clients. If no desired IP groups have been created, go to Preferences > IP Group page to create one.
Maximum Upstream Bandwidth	Specify the limit of upstream bandwidth for the specific user to transmit traffic to the internet through the router.
Maximum Downstream Bandwidth	Specify the limit of downstream bandwidth for the specific user to receive traffic from the internet through the router.
Mode	Select the bandwidth control mode for the controller users.
	Shared: The total bandwidth for all users is equal to the specified values in upstream and downstream bandwidth.
	Individual: The bandwidth for each user is equal to the specified value in upstream and downstream bandwidth.
Effective Time	Specify the time for the rule to take effect. Any means it always takes effect. If no desired time ranges have been configured, go to Preferences > Time Range page to create one.
Description	Enter a brief description for the rule.
ID	Assign a number to the rule to reorder the list.
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.

Bandwidth Control								
Index	Status	Direction	Inbound/Outbound Bandwidth	Class 1	Class 2	Class 3	Others	Operation
SFP WAN/LAN1	Enabled ଃ	Out	🖶 1000000Kbps 🛧 1000000Kbps	25 %	25 %	25 %	25 %	ି ଦ
WAN2	Enabled ଃ	Out	🖶 1000000Kbps 🛧 1000000Kbps	25 %	25 %	25 %	25 %	<u>s</u> 8
	Disabled	Out	🖶 1000000Kbps 🛧 1000000Kbps	25 %	25 %	25 %	25 %	<u>s</u> S
	Disabled	Out	🖶 1000000Kbps 🛧 1000000Kbps	25 %	25 %	25 %	25 %	<u></u>
	Disabled	Out	🖶 1000000Kbps 🛧 1000000Kbps	25 %	25 %	25 %	25 %	<u>s</u> 8
	Disabled	Out	🖶 1000000Kbps 👚 1000000Kbps	25 %	25 %	25 %	25 %	C Q

Figure 4-1 Configuring the Bandwidth Control

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.
| Bandwidth Control | | | | | | | | | |
|-------------------------|-----------------|--------------|--------|-----------------------|---------|---------|---------|--------|-----------|
| | | | | | | | | | |
| Index | Status | Direction | Inboun | d/Outbound Bandwidth | Class 1 | Class 2 | Class 3 | Others | Operation |
| SFP WAN/LAN1 | Enabled | Out | ➡10000 | 000Kbps 摿 1000000Kbps | 25 % | 25 % | 25 % | 25 % | 0 G |
| | | | | | | | | | |
| Index: | | SFP WAN/LAN | N1 | | | | | | |
| UDP Band | width Control: | Enable | | | | | | | |
| Limited Ba | andwidth Ratio: | | | % | | | | | |
| Outbound
Prioritize: | TCP ACK | 🗌 Enable | | | | | | | |
| Status: | | Enable | | | | | | | |
| Direction: | | Out | • | | | | | | |
| Inbound B | andwidth: | 1000000 | | Kbps(100-1000000) | | | | | |
| Outbound | Bandwidth: | 1000000 Kbps | | Kbps(100-1000000) | | | | | |
| | | | | | | | | | |
| | | Class 1: | | 25 | % | | | | |
| | | | | 25 | % | | | | |
| | | | | 25 | % | | | | |
| | | Others: | | 25 | % | | | | |
| ОК | Cancel | | | | | | | | |
| | | | | | - | | | | |

Figure 4-2 Edit Bandwidth Control rules

Configure the related parameters. Then click $\ensuremath{\textit{OK}}$.

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.

							0	Add 😑 D
	Rule	Qos Class	Status	Local Address	Remote Address	DSCP	Service Type	Operati
-								
	Status: IP Version:		 Enable IPv4 IPv6 					
	Local	Address:		•				
	Remote Address: DSCP: Service Type:			•				
				•				
				•				
	Servio							

Figure 4-3 Configuring the Class Rule

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 > VolP 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

Tag Prioritization		
Class 1:	□ Add DSCP or Precedence value	 •
Class 2:	Add DSCP or Precedence value	 •
Class 3:	Add DSCP or Precedence value	 •
Others:	□ Add DSCP or Precedence value	 •
Save		

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

General						
🗌 Enabl	le Sessio	n Limit				
Save						
Session I	Limit Rul	le List				
						🔂 Add 🛛 🖨 Delete
	ID	Name	Group	Max Sessions	Status	Operation

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

	ID	Name	e Group		Max Sessions	Status	Operation
r	Name:						
Group: Max Sessions:			•				
Status: 🕑 Enable							
	ОК	Cancel					

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 page.
Max Sessions	Enter the maximum number of sessions that a LAN host can use. The router will limit the sessions of the source when its number exceeds the maximum value.
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 Moni	tor List			
Entry Count:				(2) Refresh
	ID	IÞ	Max Sessions	Current Sessions
	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

General
Enable Load Balancing
Save
Basic Settings
Enable Application Optimized Routing
Enable Bandwidth Based Balance Routing on port(s):
Save

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 router 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 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	Select the WAN port from the drop-down list on which bandwidth-
Balance Routing on port(s)	based balance routing is enabled.

6.2 Configuring the Link Backup

With Link Backup function, the router 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.

	ID	Primary WAN		Backup WAN	Mode	Effective Time	Status	Operation
I	Primary WAN: Backup WAN: Mode:			g er(Enable backup link whe er(Enable backup link whe				
6	Effective Time:		Any	•				
5	Status:	atus: 🗹 Enable						
	OK	Cancel						

Figure 6-2 Configuring the Link Backup Rule

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. Load balancing will be enabled on the backup WAN. The traffic on the backup WAN will switch to the primary WAN when the failed primary WANs works properly.
	Failover(Enable backup link when all primary WANs fail) : Link Backup will be enabled only when all primary WANs fail. All the traffic on the primary WAN will switch to the backup WAN. The traffic on the backup WAN will switch to the primary WAN when all the primary WANs works properly.
Effective Time	Specify the time for the rule to take effect. Any means it takes effect at any time. If no desired time ranges have been configured, go to Preferences > Time Range page to create one.

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 it to load the following page.

ID	Port	Port Status	Operation
1	WAN1	Offline	
Port: Mode:	WAN1 Auto O Manual O Always Online		
Ping:	0.0.0.0		
DNS Lookup:			
OK Can	cel		
2	WAN2	Offline	ß

Figure 6-3 Configuring the Online Detection

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
- Configure RIP
- Configure OSPF

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

ID	Name	Destination IP	Subne	et Mask	Next Hop	Interface	Metric	Status	Operation
Name		market							
Destin	ation IP:	192.168.10.0							
Subne	t Mask:	255.255.255.0							
Next H	lop:	192.168.2.0							
Interfa	ace:	WAN1 🔻							
Metric	:	0		(0-15)					
Descri	ption:			(Optional)					
Status	:: 6	Enable							
Ok	Cancel								

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.

ID	Name	Service Type	Source IP	Destination I	WAN	Effective Time	Mode	Description	Status	Operation
Name:										
Service	Type:	Д	LL.	•						
Source	IP:	I	PGROUP_ANY	•						
Destina	ation IP:	I	PGROUP_ANY	•						
WAN:		-		•						
Effectiv	e Time:	Д	ny	•						
Mode:		P	Priority	•						
Descrip	tion:				tional)					
ID:					tional)					
Status:			Enable							
OK	C	ancel								

Figure 7-2 Configuring the Policy Routing

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 outcoming 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.

7.4 Configuring RIP

RIP(Routing Information Protocol) is a dynamic router protocol with Distance Vector Algorithms. You could config the protocol below to active as you like.

Choose the menu Transmission> Routing > RIP.

- 1) Check the box to enable the **RIP** function.
- 2) In the **Global Config** section to configure the following parameters, then click **Save**.

Figure 7-4 Configuring the Global Set	tinas

Global Config			
RIP Version:	Default		
		(1.055)	
RIP Distance:	120	(1-255)	
Auto Summary:	Enable		
Update Timer:	30	sec (5-100, default:30)	
Timeout Timer:	180	sec (5-300, default:180)	
Garbage Timer:	120	sec (5-500, default: 120)	
Save			
RIP Version	Choose the global RIP version 1 and 2	RIP version. Default: send with RIP version 2 and receive with both 2.	
	RIPv1: send and re	ceive RIP version 1 formatted packets via broadcast.	
	RIPv2: send and receive RIP version 2 packets using multicast.		
RIP Distance	Specify RIP route distance. When more than two protocols have routes to the same destination, only the route which have smallest distance will be inserted to IP routing table. The valid value ranges from 1 to 255 and the default is 120.		
Auto Summary	Summarize entries to their main class boundary.		
Update Timer	The timer interval to generate a complete response to every neighboring gateway		
Timeout Timer	Upon expiration of	the timeout, the route is no longer valid and set to unreachable.	
Garbage Timer	Upon expiration of the garbage-collection timer, the route is finally removed from the tables.		

3) In the **RIP Network List** section, click **Add** to add the network to enable RIP protocol, so the interface in the network would enable RIP protocol.

Figure 7-5	Configuring the RIP Network List
------------	----------------------------------

RIP Ne	etwork List			
			• Ad	d 😑 Delete
	Netwo	ork IP Address	Mask	Operation
	Network IP Address: Mask: OK Cancel	(Forma	t: 255.255.255.0)	
		(Forma	(; 200,200,200,0)	

Network IP Enter the IP address of the network. Address Mask

Enter the subnet mask of the network.

4) In the **Interface Config** section, click the edit button to configure the RIP parameters of the interface.

Figure 7-6 Configuring the Interface

ID	Interface	IP A	ddress	Split Horizon Mode	Status	Send Version	Receive Version	Authen Mode	Operati
1	LAN	192.	168.0.1	Split-horizon	down	RIPv2	Both	None	
Send Version: Receive Version: Split Horizon Mode: Authen Mode: Key ID:		RIPv2	•						
		Both	•						
		Split-ho	rizon 🔹						
		None	•						
				(1-255)					
	Key:			> ₁₇ <					

IP Address	The interface IP address. You can't change it here.
Status	The interface RIP status(up or down) is decided by the network status. You can't change it here.
Send Version	Select the version of RIP control packets the interface should send from the pulldown menu.
	RIPv1: Send RIP version 1 formatted packets via broadcast.
	RIPv2: Send RIP version 2 packets using multicast.
Receive Version	Select what RIP control packets the interface will accept from the pulldown menu.
	RIPv1: Accept only RIP version 1 formatted packets.
	RIPv2: Accept only RIP version 2 formatted packets.
	Both: Accept both RIP version 1 and RIP version 2 formatted packets.
Split Horizon Mode	Choose the Split Horizon Mode.
Mode	None: No special processing for this case.
	Split-horizon: A route will not be included in updates sent to the router from which it was learned.
	Poison Reverse: A route will be included in updates sent to the router from which it was learned, but the metric will be set to infinity.

Authen Mode	Select an authentication type.
	None: This is the initial interface state. If you select this option from the pulldown menu no authentication protocols will be run.
	Simple: If you select 'Simple' you will be prompted to enter an authentication key. This key will be included, in the clear, in the RIP header of all packets sent on the network. All routers on the network must be configured with the same key.
	MD5: If you select 'MD5' you will be prompted to enter both an authentication key and an authentication ID. All routers on the network must be configured with the same key and ID.
Key ID	Enter the RIP Authentication Key ID for the specified interface. If you choose not to use authentication or to use 'simple' you will not be prompted to enter the key ID.
Key	Enter the RIP Authentication Key for the specified interface. If you do not choose to use authentication you will not be prompted to enter a key. If you choose 'simple' or 'MD5' the key may be up to 16 octets long.

7.5 Configuring OSPF

OSPF (Open Shortest Path First) is an Interior Gateway Protocol (IGP) used to make routing decisions in a single autonomous system (AS).

Choose the menu Transmission> Routing > OSPF.

- 1) Check the box to enable the **OSPF** function, and set the **Router ID**.
- 2) In the **OSPF Config** section to configure the following parameters, then click **Save**.

Figure 7-7	Configuring the OSPF
------------	----------------------

OSPF Config		
Distance:	100	(0-255)
RFC 1583 Compatibility:	🔿 Enable 💿 Disable	
SPF Delay Time:	5000	msec (0-600000)
SPF Hold Init Time:	10000	msec (0-600000)
SPF Hold Max Time:	10000	msec (0-600000)
Maximum Paths:	16	(1-16)
Passive Default:	🔿 Enable 💿 Disable	
Save		
Distance	destination, only t	e distance. When more than two protocols have routes to the same he route which have smallest distance will be inserted to IP routing ue ranges from 0 to 255 and the default is 100.

RFC 1583 Compatibility	Select the preference rules that will be used when choosing among multiple AS- external LSAs advertising the same destination. If you select Enable, the preference rules will be those defined by RFC 1583. Else the preference rules will be those defined in RFC 2328, which will prevent routing loops when AS-external LSAs for the same destination have been originated from different areas. All routers in the OSPF domain must be configured the same. The default value is 'Disable'.
SPF Delay Time	The number of seconds from when OSPF receives a topology change to the start of the next SPF calculation. The valid value ranges from 0 to 600 000 msec and the default is 5000.
SPF Hold Init Time	Initial hold time (msec) between consecutive SPF calculations. The valid value ranges from 0 to 600000 msec and the default is 10000.
SPF Hold max Time	Maximum hold time (msec). The valid value ranges from 0 to 600000 msec and the default is 10000.
Maximum Paths	Set the number of paths that OSPF can report for a given destination. The valid value ranges from 1 to 16 and the default is 16.
Passive Default	Configure the default passive mode setting for the OSPF interfaces which do not specify the interface passive mode setting. OSPF does not form adjacencies on passive interfaces, due to that the routing updates on passive interfaces would be suppressed. The default value is 'Disable'.

3) In the **Network Table** section, click **Add** to add the network to enable OSPF protocol, so the interface in the network would enable OSPF protocol.

				🔁 Add 🛛 😑 Dele
IP Address		Wildcard Mask	Area ID	Operation
IP Address: Wildcard Mask:		(Format: 100.100.0.0) (Format: 0.0.255.255)		
Area ID:		(0-4294967295)		

Figure 7-8 Configuring the Network Table

IP Address	Enter the IP address of the network.
11 / 1001000	

Wildcard Mask	Enter the wildcard mask of the network. Normal subnet mask is also supported.

- Area IDThe 32 bit unsigned integer that uniquely identifies the area to which a router interface
connects. If you assign an Area ID which does not exist, the area will be created with
default values. It can be in decimal format or dotted decimal format.
- 4) In the **Interface Config** section, click the edit button to configure the OSPF parameters of the interface.

Figure 7-9 Configuring the Interface

interface	IP Address/Mask	Working	Router Priority	Retransmit Interval	Hello Interval	Dead Interval	Transmit Delay	Cost	Network Type	Passive Mode	MTU Ignore	Authentic ation Type	Operation
LAN	192.168.0.1/24	off	1	5	10	40	1	100	Broadcast	Disable	Disable	None	
Int	terface:	LAN											
Router Priority: Retransmit Interval: Hello Interval: Dead Interval: Transmit Delay: Cost:		1	1			5)							
		5			sec (1-65535)								
		10	10 40 1 100			-65535)							
		40				-65535)							
		1				-65535)							
		100				535)							
Ne	twork Type:	Broa	adcast	•									
Pa	ssive Mode:	Disa	ble	•									
МТ	"U Ignore:	Disa	ble	•									
Au	thentication Type:	Non	e	•									
Sir	mple Key:				1-8 ch	aracters							
ME	05 Key ID:				(1-255	5)							
MD	D5 Key:				1-16 c	haracters							

Interface	The interface for which data is to be displayed or configured.
IP Address/ Mask	The IP address and subnet mask of the interface.
Router Priority	The router priority for the selected interface. The priority of an interface is specified as an integer from 0 to 255. A value of '0' indicates that the router is not eligible to become the designated router on this network. The default is 1.
Hello Interval	The hello interval for the specified interface in seconds. This parameter must be the same for all routers attached to a network. The valid value ranges from 1 to 65535 seconds and the default is 10 seconds.
Dead Interval	The dead interval for the specified interface in seconds. This specifies how long a router will wait to see a neighbor router's Hello packets before declaring that the router is down. This parameter must be the same for all routers attached to a network. The valid value ranges from 1 to 65535 seconds and the default is 40.
Transmit Delay	The Transit Delay for the specified interface. This specifies the estimated number of seconds it takes to transmit a link state update packet over the selected interface. The valid value ranges from 1 to 65535 seconds and the default is 1 second.
Cost	The link cost. OSPF uses this value in computing shortest paths. The valid value ranges from 1 to 65535.

Network Type	The OSPF network type on the interface. The default network type for Ethernet interfaces is broadcast.
Passive Mode	Make an interface passive to prevent OSPF from forming an adjacency on an interface. The routing updates on passive interface would be suppressed. Interfaces are not passive by default.
MTU Ignore	Disables OSPF MTU mismatch detection on received database description packets. Default value is Disable(MTU mismatch detection is enabled).
Authentication Type	Displays the authentication type of the interface. One of the following: none: No authentication. simple: Use simple password. md5: Use md5 message-digest algorithm.
Simple Key	Displays the key used for simple authentication.
MD5 Key ID	Displays the key ID used for md5 authentication.

5) View the **Neighbor Table**.

Figure 7-10 Viewing the Neighbor Table

Neighbor Table

									🕖 Refresh
Interface	Neighbor IP Address	Router ID	Area ID	Options	Router Priority	State	Events	Retransmission Queue length	Dead Time

Interface	Displays the interface for which neighbor list is to be displayed.
Neighbor IP Address	The IP address of the neighboring router's interface to the attached network.
Router ID	A 32 bit integer in dotted decimal format representing the neighbor.
Area ID	The area ID of the OSPF area associated with the interface.
Router Priority	The router priority of the neighbor.
Options	An integer value that indicates the optional OSPF capabilities supported by the neighbor. The neighbor's optional OSPF capabilities are also listed in its Hello packets.

Dead Time	The amount of time, in seconds, to wait before the router assumes the neighl unreachable.
Retransmission Queue length	An integer representing the current length of the retransmission queue of specified neighbor router ID of the specified interface.
Events	The number of times this neighbor relationship has changed state, or an erro occurred.
	Full: In this state, the neighboring routers are fully adjacent. These adjacencie now appear in Router LSAs and Network LSAs.
	Loading: In this state, Link State Request packets are sent to the neighbor a for the more recent LSAs that have been discovered (but not yet received) i Exchange state.
	Exchange: In this state the router is describing its entire link state database sending Database Description packets to the neighbor. In this state, Link Request Packets may also be sent asking for the neighbor's more recent LSA adjacencies in Exchange state or greater are used by the flooding procedure. The adjacencies are fully capable of transmitting and receiving all types of OSPF re- protocol packets.
	ExStart: This is the first step in creating an adjacency between the two neighbrouters. The goal of this step is to decide which router is the master, and to d upon the initial DD sequence number. Neighbor conversations in this state or grare called adjacencies.
	2-Way: In this state, communication between the two routers is bidirectional has been assured by the operation of the Hello Protocol. This is the most adva state short of beginning adjacency establishment. The (Backup) Designated Rou selected from the set of neighbors in state 2-Way or greater.
	Init: In this state, a Hello packet has recently been seen from the neighbor. How bidirectional communication has not yet been established with the neighbor (i.e router itself did not appear in the neighbor's Hello packet). All neighbors in this sta greater) are listed in the Hello packets sent from the associated interface.
	Attempt: This state is only valid for neighbors attached to NBMA networks. It indi that no recent information has been received from the neighbor, but that a concerted effort should be made to contact the neighbor. This is done by sendir neighbor Hello packets at intervals of Hello Interval.
	Down: This is the initial state of a neighbor conversation. It indicates that ther been no recent information received from the neighbor. On NBMA networks, packets may still be sent to 'Down' neighbors, although at a reduced frequency.

6) View the Link State Database

Figure 7-11 Viewing the Link State Database	Figure 7-11	Viewing the Link State Database
---	-------------	---------------------------------

							Ø Refr		
Area ID	Advertising Router	LSA Type	Link State ID	Age	Sequence	Checksum	Options		
Area ID	Displa	ys the ID of tl	ne area to whi	ch the LSA be	longs.				
Advertising Router	Displa	ys the ID of tl	ne router that	advertising th	e LSA.				
LSA Type		The format and function of the link state advertisement. One of the following: Router, Network, Network-Summary, ASBR-Summary, External (Type 5), NSSA-External (Type 7).							
Link State ID		The Link State ID identifies the piece of the routing domain that is being described by the advertisement. The value of the LS ID depends on the advertisement's LS type.							
Age	The tir	The time since the link state advertisement was first originated, in seconds.							
Sequence The sequence number field is a signed 32-bit integer. It is used to detect of duplicate link state advertisements. The larger the sequence number, the more return advertisement.									
Checksum	can oo memo	cur while an	advertisemen is the checks	t is being floo	on of an adver ded, or while it mplete conte	is being held	l in a router		
Options				ite advertiser he advertiser	ment header nent.	indicates wh	ich optiona		

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 router.
- 2) The company has a web server which needs to be accessed by the users on the internet.

8.1.2 Network Topology



8.1.3 Configuration Scheme

To meet the first requirement, configure static routing on the gateway to make sure the router 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 router, 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 router:

- 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**.

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:	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	
Description:		
Status:	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**.
- 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 orignal 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.

	ID	Name	Interface	Original IP	Translated IP	DMZ Forwarding	Description	Status	Operation
			web						
	Name: Interface		WAN1	•					
	Original IP:			58.0.20					
-	Translate	ed IP:	123.1	.1.3					
I	DMZ For	warding:	Enabl	e					
I	Descripti	ion:			(Optional)				
:	Status:		💽 Enabl	e					
[ОК	Cancel]						

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

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



8.2.3 Configuration Scheme

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

8.2.4 Configuration Procedure

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

• 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

General	
Enable Load Balancing Save	
Basic Settings	
 Enable Application Optimized Routing Enable Bandwidth Based Balance Routing on port(s): WAN1, WAN2 Save 	

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



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 router 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 router:

- 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**.

ID	Name		Interface	External Port	Internal Port	Internal Server IP	Protocol	Status	Operation
Nar	me:	ftp							
Int	erface:	WAN:	1	•					
Ext	ternal Port:	21			(XX or XX-X	X ,1-65535)			
Int	ernal Port:	21			(XX or XX-X	X ,1-65535)			
Int	ernal Server IP:	192.1	68.0.100						
Pro	otocol:	ALL		•					
Sta	atus:	💌 Enab	le						
	OK Cancel								

Figure 8-8 Configuring the Virtual Server

8.4 Example for Configuring Policy Routing

8.4.1 Network Requirements

The network administrator has a router 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 router. 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 router:

- 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

	ID	Primary	WAN	Backup WAN	Mode	Effective Time	Status	Operation
1	Primary W/ Backup W/ Mode:							
	Effective Ti Status:	ime:	Any	e				
[ОК	Cancel						

- Configuring the Policy Routing Rules
- 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

ID	Name	IP Address Type	IP Addre	ss Range	IP Address/M	lask	Description	Operation
 			-	-				
Name: IP Add	: Iress Type:	tp IP Addr	ess Range 🔿 IP	Address/Mask				
		192.168	.0.2	- 192.168.0.3	3			
Descri	ption:			(Optional)				
Ok	Cancel							

 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

	ID		Group Name		Address Name	Description	Operation
Ado	oup Name: dress Name: scription:		group1 tp	•	(Optional)		
	OK Ca	ncel					

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**.

ID	Name	Service Type	Source IP	Destination IP	WAN	Effective Time	Mode	Description	Status	Operation
Name:			olicy1							
Name:		P	oncyl							
Servic	e Type:	F	ITTP	•						
Source	e IP:	g	roup1	•						
Destin	ation IP:	I	PGROUP_ANY	-						
WAN:		v	VAN1	-						
Effecti	ve Time:	۵	ny	•						
Mode:		P	riority	•						
Descri	ption:			(Opt	ional)					
ID:				(Opt	ional)					
Status	:		Enable							
OK	C	ancel								

Figure 8-13 Configuring the Policy Routing Rule 1

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:		P	olicy2							
Servic	e Type:		LL	-						
Source	e IP:	g	roup1	-						
Destin	ation IP:	I	PGROUP_ANY	-						
WAN:		v	VAN2	-						
Effecti	ve Time:	А	ny	•						
Mode:		P	riority	•						
Descri	ption:			(Opt	ional)					
ID:				(Opt	ional)					
Status	:		Enable							
OK	C	ancel								

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 routers 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 router checks whether it matches any of the IP-MAC Binding entries. If not, the router will ignore the ARP packets. In this way, the router maintains the correct ARP table.

In addition, the router 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 router can identify and discard various attack packets which are sent to the CPU, and limit the packet receiving rate. In this way, the router can protect itself and the connected network against malicious attacks.

The router 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 router 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 router 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.



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 router sends the ARP request packets with the specific IP field to the hosts. Upon receiving the ARP reply packet, the router 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							
💌 Enabl	e ARP Spoof	ing Defense					
🗌 Permi	it the packet	s matching the IP-MAC Bind	ing entries only				
Send	GARP packet	ts when ARP attack is detect	ed				
Interval:		1000	ms				
Save							
IP-MAC E	Binding List						
						¢	🗗 Add 🛛 😑 Delete
	ID	IP Address	MAC Address	Interface	Description	Status	Operation

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

	ID	IP Ad	ldress	MAC Addres	s	Interface	Description	Status	Operatio
		-		-					
I	IP Address:								
	MAC Address	:							
I	Interface:		LAN	•					
0	Description:				(Option	al, 0-50 characters)			
	Export to DH Reservation:	CP Address	💌 Enable						
s	Status:		Enable						
	ОК	Cancel							

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.
Interface	Select the interface on which the entries will take effect.
Description	Enter a description for identification.
Export to DHCP Address Reservation	Whether to export the IP-MAC binding list to address reservation list.
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.



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 Etries via ARP Scanning

General				
Scanning IP Rang	je: 192.168	- 192.168.0.200		
Scan				
Scanning Result				
				e ∂ Bind
	ID	IP Address	MAC Address	Operation

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 *P* to export the corresponding entry to the IP-MAC Binding table, or select multiple entries and click *P* Bind to export the entries to the IP-MAC Binding table in batch.

Figure 2-5 ARP Scanning Result

Scanning Result

			a Bind
ID	IP Address	MAC Address	Operation
1	192.168.0.100	00-0A-EB-13-A2-3D	cP
2	192.168.0.200	00-19-66-35-E1-B0	cP
3	192.168.0.73	00-0A-EB-00-13-01	cP
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 P to export the corresponding entry to the IP-MAC Binding table, or select multiple entries and click *P* Bind to export the entries to the IP-MAC Binding table in batch.

Figure 2-6	ARP List				
ARP List					
					🧬 Bind 🛛 🖉 Refresh
	ID	IP Address	MAC Address	Interface	Operation
	1	192.168.0.100	00-0A-EB-13-A2-3D	LAN	
	2	192.168.0.200	00-19-66-35-E1-B0	LAN	e

2.1.2 Enable Anti ARP Spoofing

IP-MAC Binding List

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

Figure 2-7 IP-MA	C Binding-General Con	nfig			
General					
✓ Enable ARP Spoofing	Defense				
Permit the packets n	Permit the packets matching the IP-MAC Binding entries only				
Send GARP packets	when ARP attack is detected				
Interval:	1000	ms			
Save					

						🗗 Add 🗧 Delete
ID	IP Address	MAC Address	Interface	Description	Status	Operation

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 router 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 router 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.
I	THE IP-MAC DITIONING ENTITIES ONly	interface match any of the IP-MAC Binding entries. Only the

_ _ _

Send GARP packets when ARP attack is detected	With this option enabled, the router will send GARP packets to the hosts if it detects ARP spoofing packets on the network. The GAR 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 enabled, configure the time interval for sending GARP packets. Th valid values are from 1 to 10000 milliseconds.

3) Click Save.

Note:
Refore enabling "Permit the

_ _ _ _ _ _ _ _ _ _ _ _ _

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 router. If this happens, restore your router 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				
Multi-connections TCP SYN Flood	10000	Pkt/s		
Multi-connections UDP Flood	12000	Pkt/s		
Multi-connections ICMP Flood	1500	Pkt/s		
Stationary source TCP SYN Flood	4000	Pkt/s		
Stationary source UDP Flood	6000	Pkt/s		
Stationary source ICMP Flood	600	Pkt/s		
Packet Anomaly Defense				
✓ Block TCP Scan (Stealth FIN/Xmas/Nu	II)			
Block Ping of Death				
Block Large Ping				
✓ Block Ping from WAN				
Block WinNuke attack				
Block TCP packets with SYN and FIN Bi	ts set			
Block TCP packets with FIN Bit set but	no ACK Bit set	t		
 Block packets with specified IP options 				
 Security Option Loose Source 	Route Option			
✓ Strict Source Route Option	ecord Route Op	ption		
 Stream Option Timestamp 	Option			
No Operation Option				
Save				

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:

Multi-connections TCP SYN Flood	With this feature enabled, the router 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.
Multi-connections UDP Flood	With this feature enabled, the router 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.
Multi-connections ICMP Flood	With this feature enabled, the router 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.

Stationary source TCP SYN Flood	With this feature enabled, the router 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 router 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 router 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 router will filter the TCP scan packets of Stealth FIN, Xmas and Null.
Block Ping of Death	With this option enabled, the router 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 router 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 router will block the ICMP request from WAN.
Block WinNuke attack	With this option enabled, the router 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 router 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 router 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 router 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 router based on the MAC address of the devices. After the MAC filtering policy and MAC filtering

list are configured, the router 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

Enable MAC Filtering								
 Allow packets with the MAC addresses listed below and deny the rest 								
Deny packets with the MAC addresses listed below and allow the rest								
Direction: ALL								
Save								
IAC Filtering Lis	st							
-								
				🕒 Add 🛛 😑 Del				
		Name	MAC Address	Operation				
	ID							
	ID							

Follow the steps below to configure MAC Filtering.

1) In the **General** section, check the box to enable the MAC Filtering feature, configure the conresponding 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 router, 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 router.
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

MAC Filtering Lis	t			
				<table-cell-rows> Add 🛛 😑 Delete</table-cell-rows>
	ID	Name	MAC Address	Operation
Name:			(1-50 characters)	
MAC Add	dress:			
ок	Cancel			

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

Access (Control L	ist							
									🕂 Add 🛛 😑 Delet
	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

	ID	Name	Source	Destination	Policy	Service Type	Interface	Effective Time	Operatio	
	Name				(1-50 charac	tora				
Name: Policy:				(1-50 charac	ters)					
		Block	•							
	Service	Type:	ALL	•						
	Interfao	e:		•						
	Source:			•						
	Destinat	tion:		•						
	Effective	e 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 router 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 router to protect itself and the terminal hosts from the ARP attacks.





3.1.2 Configuration Scheme

The attacker can launch three types of ARP attacks: cheating router, 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 router.

The attacker pretends to be legal terminal hosts and sends fake ARP packets to the router, cheating the router 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 router from this kind of attack, you can configure Anti ARP Spoofing on the router.

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 router 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 router to send GARP packets to the hosts when the router 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 router and the hosts are configured with the relevant ARP defense features. Here we introduce how to configure Anti ARP Spoofing on the router. 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 router 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 router:

 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	General								
🗌 Enab	Enable ARP Spoofing Defense								
Permit the packets matching the IP-MAC Binding entries only									
Send	GARP packet	ts when ARP attack is detect	ed						
Interval:		1000	ms						
Save	Save								
IP-MAC E	Binding List								
Add Celete									
	ID	IP Address	MAC Address	Interface	Description	Status	Operation		

2) 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

							•	🕒 Add 🛛 🖨 🖸
ID IP Address MAC Address Interface Description	Status	Operatio						
	IP Address: 192.168.0.10 MAC Address: 00-19-56-8A-4C-71							
D	escription:		Host A	(Optiona	al, 0-50 characters)			

3) 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 Entires

IP-MAC Bi	nding List						
							🗜 Add 🛛 😑 Delet
	ID	IP Address	MAC Address	Interface	Description	Status	Operation
	1	192.168.0.10	00-19-56-8A-4C-71	LAN	Host A	Enabled 😢	2
	2	192.168.0.20	00-19-56-82-3B-70	LAN	Host B	Enabled 😢	2
	3	192.168.0.30	00-19-56-8D-22-75	LAN	Host C	Enabled 😣	e 🖸

4) 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.





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 router. 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 router 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:

 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.

IP	Addr	ess List								
									C	Add 🖨 Delete
		ID	Name	IP Address Type	IP Addres	s Range	IP Address/I	Mask	Description	Operation
					-					
	Name:			RD						
		IP Add	ress Type:	IP Addre		Address/Mask		1		
				192.168	.0.10	- 192.168.0.1	120			
	Description:					(Optional)				
		OK	Cancel							

Figure 3-2 Configure IP Address Range

 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

oup List							
							🔁 Add 🖨 Dele
	ID		Group Name		Address Name	Description	Operation
					1		
Gro	up Name:		RD_Dept				
Add	ress Name:		RD	•			
Description:					(Optional)		
	OK Ca	ncel					

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.

						🔁 Add 🕒 I
ID	Service Type Name	Protocol		Detail	Description	Operatio
Protocol: Source Port Range: Destination Port Range: Description:		0 – 443 –	0P () TCP/UD 65535 443	Optional)		

Figure 3-4 Configure HTTPS Service Type

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

ID Name Source Destination Policy Service Type Interface Effective Time Operation Name:									🔁 Add 🕒 🕻
Name: Allow_HTTP Policy: Allow Allow Service Type: HTTP Interface: LAN Source: RD_Dept Destination: IPGROUP_ANY	ID ID	Name	Source	Destination	Policy	Service Type	Interface	Effective Time	Operation
Policy:AllowService Type:HTTPInterface:LANSource:RD_DeptDestination:IPGROUP_ANY									
ID: (Optional)	Policy: Service Type: Interface: Source: Destination: Effective Time:		HTTP LAN RD_Dept IPGROUP_A	× × ANY ×	(Option 1)				

5) 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.

									🔁 Add
	ID	Name	Source	Destination	Policy	Service Type	Interface	Effective Time	Operatio
	Name:		Allow_HTT		(1-50 charac	ters)			
					(1-50 charac	cers)			
Policy:		Allow	•						
	Service	Туре:	HTTPS	•					
	Interfac	e:	LAN	•					
	Source:		RD_Dept	•					
	Destinat	tion:	IPGROUP_/	ANY 🔻					
	Effective	e Time:	Any	•					
	ID:				(Optional)				

Figure 3-6 Configure Allow Rule for HTTPS Service

6) 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.

4	Access (Control L	ist							
										🔁 Add 🖨 Delete
		ID	Name	Source	Destination	Policy	Service Type	Interface	Effective Time	Operation
		Name: Policy: Service Type: Interface: Source: Destination: Effective Time: ID:		Allow_DNS Allow DNS LAN RD_Dept IPGROUP_A Any	V V INY V	1-50 charact Optional)	ers)			
	[ОК	Cancel							

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.

								🕒 Add 🖨 D		
	ID	Name	Source	Destination	Policy	Service Type	Interface	Effective Time	Operatio	
	Name:		Discis all		1 E0 sharras	have)				
			Block_All		(1-50 charac	ters)				
	Policy:		Block	•						
	Service Type:		ALL	•						
	Interfac	e:	LAN	•						
	Source:		RD_Dept	•						
	Destinat	tion:	IPGROUP_4	ANY 🔻						
	Effective	e Time:	Any	•						
ID:				(Optional)						

8) Verify your configuration result. In the Access Control List, the rule with a smaller ID has a higher priority. Since the router 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 router 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.

ccess C	Control L	List							
									🔁 Add 🛛 😑 Del
	ID	Name	Source	Destination	Policy	Service Type	Interface	Effective Time	Operation
	1	Allow_HTTP	RD_Dept	IPGROUP_ANY	Allow	HTTP	LAN	Any	2
	2	Allow_HTTPS	RD_Dept	IPGROUP_ANY	Allow	HTTPS	LAN	Any	2
	3	Allow_DNS	RD_Dept	IPGROUP_ANY	Allow	DNS	LAN	Any	2
	4	Block_All	RD_Dept	IPGROUP_ANY	Block	ALL	LAN	Any	2

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 router 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

Figure 2-1 Web Group Page

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

Web Group Lis	t				
					🕂 Add 🛛 🖨 Delete
	ID	Name	Member	Description	Operation
Name	:		(1-28 characters)		
Memb	er:				
Cle	ar	(Use the Enter key, Space ke	y, "," or ";" to divide different webs	ites.)	
File Pa	th:		Browse (Optional. TXT file i	is required.)	
Imp	ort	Import web list file.			
Descri	ption:		(Optional)		
Oł	Cancel]			

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
i iguio z z	web oloup i illering i uge

General									
Enable Web Filtering									
Save									
/eb Filter	ing List								
								🔂 Add 🛛 😑 Del	
	ID	IP Group	Policy	Web Group	Effective Time	Status	Description	Operation	
	Group:			•					
Po	olicy:		 Whitelist 	 Blacklist 					
W	/eb Group	:		•					
Ef	ffective T	ime:	Any	•					
Description:					(Optional)				
ID:				(Optional)					
Status:									
_									
	OK	Cancel							

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 GroupSelect 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

G	General										
C	Enable URL Filtering										
	Save										
U	IRL Filt	ering List									
		-								•	Add 😑 Delete
		ID	IP Group		Policy	Mode	Filtering Content	Effective Time	Status	Description	Operation
		IP Group:				•					
		Policy:		0 A							
	Mode: Filtering Content:		Keywords O URL Path		○ URL Path	(Use the Enter key, Sp ";" to divide different fi	ace key, "," (Itering conte	or nts.)			
	Effective Time: Any 🔻										
	Status: 🕑 Enable										
	Description:				(Optional, 0-50 charact	ers)					
		ID: OK	Cancel				(Optional)				

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	Select the filtering mode.
	Keywords : If a website address contains any of the keywords, the policy will be applied to this website.
	URL Path : If a website address is the same as any of the entire URLs, the policy will be applied to this website.
Filtering Content	Add filtering contents. Use the Enter key, Space key, "," or ";" to divide different filtering contents.
	"." 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.
Effective Time	Select the effective time. The effective time referenced here can be created on the Preferences > Time Range page.
Status	Check the box to enable the rule.
Description	Enter a brief description for the group.
ID	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.

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

General										
🗌 Enable	Web Securit	ý								
Save										
Web Secur	ity List									
									🕀 Add	😑 Delete
	ID	IP Grou	p	File Suffix		Effective Time	Description	Status	Ope	ration
Blo	Group: ock HTTP Pos e Suffix:	t:	 Enab	▼	(Use divid	Enter key, Space ke e different file suffixe	y, "," or ";" to s.)			
De	Fective Time: escription : atus: OK		Any Enable	▼ ole	(Optio	onal)				

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 router. 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:

Figure 3-2 Configure IP Address Range

 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.

								🔂 Add 🕒 D
ID	Name	IP Address Type	IP Address Rang	e	IP Address/N	1ask	Description	Operation
Name: IP Addr	ress Type:	RD	ess Range 🔿 IP Address	/Mask		_		
		192.168	.0.10 - 1	92.168.0.1	20			
Descrip	otion:		(Optio	onal)				
OK	Cancel							

 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
	ID	Group Name	Address Name	Description	Operation
	up Name: Iress Name:	RD_Dept RD			
Des	cription:		(Optional)		
	OK Ca	ncel			

 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.

Web	Group Lis	st				
						🔂 Add 🖨 Delete
		ID	Name	Member	Description	Operation
	Name: Member: Clear		RD_Filtering www.tp-link.com (Use the Enter key, Space ke	(1-28 characters) y, "," or ";" to divide different webs	ites.)	
	File Path: Import		Import web list file.	Browse (Optional. TXT file	is required.)	
	Description : OK Cancel]	(Optional)		

Figure 3-4 Configure Web Group

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 Web Filtering List 🔁 Add 😑 Delete ID IP Group Policy Web Group Effective Time Status Description Operation IP Group: RD_Dept • Policy: RD_Filtering Web Group: • Effective Time: Any -Description: (Optional) ID: (Optional) Status: Enable Cancel ОК

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.

eb Filter	ring List							🔁 Add 🕒 D
	ID	IP Group	Policy	Web Group	Effective Time	Status	Description	Operation
IP Group: Policy: Web Group: Effective Time:		RD_Dept O Whitelist All Any	Blacklist					
Description : ID:				(Optional) (Optional)				
Status:			 Enable 					
	ОК	Cancel						

Figure 3-6 Configure Blacklist Rule

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 router matches the rules beginning with the highest priority, make sure the Whitelist rule has the smaller ID number. In this way, the router 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		
	ID	IP Group	Policy	Web Group	Effective Time	Status	Description	Operation		
	1	RD_Dept	Whitelist	RD_Filtering	Any	Enabled 😢		2		
	2	RD_Dept	Blacklist	All	Any	Enabled 😢		i		

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	
Save	

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 router. 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 router 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:

 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 filed, 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 Oelete
	ID	IP Gro	roup File Suffix			Effective Time	Description	Status	Operation
E	IP Group: Block HTTP Post: File Suffix:			ROUP_LAN 🔻	(Use divid	Enter key, Space ke e different file suffixe	y, "," or ";" to s.)		
Effective Time:			Any	•					
Description:					(Opti	onal)			
Status: 🕑 Enable				ble					
OK									

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.



1.2 Supported Features

The router 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 router plays in the negotiation process. You can specify the negotiation mode as responder mode or initiator mode.

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

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

Exchange Mode

The exchange mode determines the way VPN routers 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 router uses the IP address for authentication.

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

Encapsulation Mode

The encapsulation mode determines how packets transfered 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 router 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.

	ID	Policy Name	Mode	Remote Gatew	vay	Local Subnet	Remote Subnet	Status	Operation		
	Policy Name:				(1-32 characters)						
	Mode:		LAN-to-LAN	•	•						
	Remote Gateway:				(IP Address/Domain Name)						
1	WAN:			•	•						
	Local Subnet:			/							
I	Remote Subnet:			/							
	Pre-shared	Key:			(1-1	28 characters)					
:	Status:		Enable								
(Advanced Settings										
[ОК	Cancel									

Figure 2-1 Configuring the Basic Parameters

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:	(IP Address/Domain Name)				
WAN:	*				
Local Subnet:					
Remote Subnet:					
Pre-shared Key:	(1-128 characters)				
Status:	✓ 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:	(IP Address/Domain Name)				
WAN:	v				
Local Subnet:					
Pre-shared Key:	(1-128 characters)				
Status:	✓ 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.

Phase-1 Settings		
IKE Protocol Version:	IKEv1 O IKEv2	
Proposal:	sha1-aes256-dh2 🔹	
Proposal:	•	
Proposal:		
Proposal:	🔻	
Exchange Mode:	Main Mode O Aggressive Mode	
Negotiation Mode:	● Initiator Mode 🛛 C Responder Mo	de
Local ID Type:	● IP Address ○ NAME	
Local ID:		(1-28 non-blank characters)
Remote ID Type:	IP Address O NAME	
Remote ID:		(1-28 non-blank characters)
SA Lifetime:	28800	seconds (60-604800)
DPD:	✓ Enable	
DPD Interval:	10	seconds (1-300)

Figure 2-2 Configuring the IKE Phase-1 Parameters

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	Specify the IKE Exchange Mode as Main Mode or Aggressive Mode. By default, it is Main Mode.
	Main Mode: Main mode provides identity protection and exchanges more information, which applies to scenarios with higher requirements for identity protection.
	Aggressive Mode: Aggressive Mode establishes a faster connection but with lower security, which applies to scenarios with lower requirements for identity protection.
Negotiation Mode	Specify the IKE Negotiation Mode as Initiator Mode or Responder Mode.
Mode	Initiator Mode: The local device initiates a connection to the peer.
	Initiator Mode: The local device initiates a connection to the peer.
Local ID Type	Specify the local ID type for IKE negotiation.
	IP Address: Use an IP address as the ID in IKE negotiation. It is the default type.
	NAME : Use a name as the ID in IKE negotiation. It refers to FQDN (Fully Qualified Domain Name).
Local ID	When the Local ID Type is configured as NAME, enter a name for the local device as the ID in IKE negotiation.
Remote ID	Specify the remote ID type for IKE negotiation.
Туре	IP Address: Use an IP address as the ID in IKE negotiation. It is the default type.
	NAME : Use a name as the ID in IKE negotiation. It refers to FQDN (Fully Qualified Domain Name).
Remote ID	When the Remote ID Type is configured as NAME, enter a name of the remote peer as the ID in IKE negotiation .
SA Lifetime	Specify ISAKMP SA (Security Association) Lifetime in IKE negotiation. If the SA lifetime expired, the related ISAKMP SA will be deleted.
DPD	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.
DPD Interval	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.

• 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

Phase-2 Settings			
Encapsulation Mode:	● Tunnel Mode 🛛 Transpo	ort Mode	
Proposal:	esp-sha1-aes256	-	
Proposal:		•	
Proposal:		-	
Proposal:		-	
PFS:	none	•	
SA Lifetime:	28800	seconds (120-6	604800
OK Cancel			

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 🛛 🖨 D
	ID	Group Name	Primary IPsec	Secondary IPsec	Status	Operation
Primary IPsec: Secondary IPsec: Automatic Failback: Gateway failover time-out: Status: OK Cancel		Enable Enable	seconds (10-	·3600)		

Follow these steps to configure the parameters, then click $\ensuremath{\textbf{OK}}$:

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 router 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.

IPSec	SA Li	st								
Entry	Coun	t: 2								🗭 Refresh
	ID	Name	SPI	Direction	Tunnel ID	Data Flow	Protocol	AH Authentication	ESP Authentication	ESP Encryption
	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
	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	

	ID	Name	Wan	Remote Gateway	IPsec Encryption	Local Subnets	Remote Subnets	Status	Operatio
	Name:								
				_					
	Wan:			•					
Remote Gateway: IPsec Encryption:									
			•						
	Pre-share	ed Key:		274	(1-128 characters)				
	Local Sub	bnets:		/					
	Remote S	Subnets:		1					
	Local GR	E IP:							
	Remote (GRE IP:							
	Status:		Enable						

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

4.1 Configuring the VPN IP Pool

Figure 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.

Pool Lis	t				🔂 Add 😄 Dele
	ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
St		Address:			
Er	OK	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

General		
L2TP Hello Interval:	60	seconds (60-1000)
PPP Hello Interval:	20	seconds (0-120, 0 means not send)
NetBIOS Passthrough:	Enable	
Save		

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.

						🔂 Add 🛛 🖨 De
	ID	WAN		IPSec Encryption	Status	Operation
WAN: IPSec Encryption: Pre-shared Key:			•	(1-128 characters)		
Status: Cancel OK Cancel						

Figure 4-3 Configuring the L2TP Server

L2TP Server Settings

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.

IPSecSpecify whether to enable the encryption for the tunnel. If enabled, the L2TPEncryptiontunnel 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.

ID	Tunnel	Account Name	WAN	Se	erver IP	IPSec Encryption	Remote Subnet	Working Mode	Status	Operation
Tunnel: Account Name: Password: WAN: Server IP:		Low N	liddle	High	(1-12 chara	acters)				
IPSec Encryption: Pre-shared Key:				•	(1-128 char	racters)				
Remote Subnet:										
Upstrea	m Bandwidth:	1000000			Kbps(100-1	.000000)				
Downst	ream Bandwidth:	1000000			Kbps(100-1000000)					
Working	Mode:	● NAT ○	Route							
Status:		Enable								
ОК	Cancel									

Figure 4-4 Configuring the L2TP Client

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.

TunnelSpecify the name of L2TP tunnel.

be configured identically on
nfigured identically on server
er.
el. If enabled, the L2TP tunnel
s range of LAN on the remote ress and subnet mask.
nel.
tunnel.
lows the router to translate n forwarding L2TP packets.
packets via routing protocol.

2) Click **OK**.

2)

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

	ID	Account Name	Protocol	Local IP Addre	IP Address Pool	Network Mode	Remote Subnet	Operation
	Account I							
ł	Password	1:	Low	Middle High				
I	Protocol:			•				
l	Local IP /	Address:						
1	IP Addres	ss Pool:						
I	DNS Add	ress:						
I	Network	Mode:		•				
I	Max Coni	nections:			(1-100)			
F	Remote S	Subnet:		/				
[OK	Cancel						

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.
Specify the prote	ocol 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

							🙆 Refresh
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 router 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 router acts as the PPTP server, you don't need to configure a PPTP client on the router.
- When the network mode is configured as LAN-to-LAN and the router acts as the PPTP client gateway, you don't need to configure PPTP users on the router.

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.

P Pool Lis	st				
					🕂 Add 🛛 😑 Delet
	ID	IP Pool Name	Starting IP Address	Ending IP Address	Operation
St	Pool Nar tarting IP nding IP / OK	Address:			

Figure 5-1 Configuring the VPN IP Pool

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.

General		
PPTP Hello Interval:	60	seconds (60-1000)
PPP Hello Interval:	20	seconds (0-120, 0 means not send)
NetBIOS Passthrough:	Enable	
Save		

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.

Server List					
					🕂 Add 🛛 🖨 Delete
	ID	WAN	MPPE Encryption	Status	Operation
WAN:		•			
MPPE I	Encryption:	•			
Status	:	✓ Enable			
ОК	Cancel				

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

Figure 5-4 Configuring the PPTP Client

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

|--|

ID	Tunnel	Account Name	Server IP	WAN	MPPE Encryption	Remote Subnet	Working Mode	Status	Operation
Tunnel:				(1-12 char	acters)				
Account Name:									
Password:									
		Low M	Iiddle High						
WAN:			•						
Server IP:									
MPPE Encryption:			•						
Remote Subnet:			/						
Upstream Bandwidth:		1000000		Kbps (100-	-1000000)				
Downstream Bandwidth:		1000000		Kbps (100-	-1000000)				
Working Mode:		● NAT 〇	Route						
Status:		 Enable 							
OK	Cancel								

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.

Status	Check the box to enable the PPTP tunnel.
	Route : Route mode allows the router to forward PPTP packets via routing protocol.
	NAT : NAT (Network Address Translation) mode allows the router to translate source IP address of PPTP packets to its WAN IP when forwarding PPTP packets.
Working Mode	Specify the Working Mode as NAT or Routing.
Downstream Bandwidth	Specify the downstream limited rate in Kbps for PPTP tunnel.
Upstream Bandwidth	Specify the uptream limited rate in Kbps for PPTP tunnel.
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.
MPPE Encryption	Specify whether to enable the encryption for the tunnel. If enabled, the PPTP tunnel will be encrypted by MPPE.

2) Click **OK**.

5.5 (Optional) Configuring the PPTP Users

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

	ID	Account Name	Protocol	Local IP Addre	ss IP Address Pool	Network Mode	Remote Subnet	Operation
,	Account I	Name:						
I	Password	1:						
			Low	Middle High				
I	Protocol:			•				
I	Local IP Address:							
1	IP Addres	ss Pool:						
I	DNS Address:							
I	Network	Mode:		•				
I	Max Coni	nections:			(1-100)			
I	Remote S	Subnet:		/				
	OK	Cancel						

Figure 5-5 Configuring the PPTP User

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 router 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 router 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

OpenVPN Server List

									0	Add 🗢 Delet
	ID	Server Name	Protocol	Service Port	Local Ne	etwork	Primary DNS	Secondary DNS	Status	Operation
	Server Na	me:				(1-32 c	haracters)			
	AccountP\	VD:	🗌 Enable							
	Status:		Enable							
	Full Mode:		Enable							
	Protocol:		О ТСР .	UDP						
	Service Po	ort:	1194			(1-6553	35)			
	Local Netv	vork:			1					
	WAN:				•					
	IP Pool:				/					
	Primary DNS:									
Secondary DNS:						(Option	al)			
Authentication Type:			Local							
	OK	Cancel								

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 router.
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 router will act as an OpenVPN client to establish the VPN tunnel with the remote Server.

									🔁 Add 😑 🕻
	ID	Client Na	me	Service Port	Ren	note Server	Local Network	Status	Operatio
Client Name:					(1-32 characters	;)		
Mode:			CA	CA+PWD					
S	Service Port:		1194			(1-65535)			
R	Remote Server:								
L	.ocal Network:			/					
v	WAN:				•				
File Path:					Brows	e (OVPN file i	s required.)		
Import			Export th	e certificate file of the 0	OpenVPN	I Server.			
Status:			Enable	e					

Figure 6-2 Configuring the OpenVPN Client

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.

FIGULE 0-3 VIEWING LITE ODELLVEIN TUITIEL	Figure 6-3	Viewing the OpenVPN Tunnel
---	------------	----------------------------

OpenVPN Tunnel List

Entry Count: 0									
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.

Wireg	uard									
										🔂 Add 🛛 🗢 Delete
	ID Name MTU			TX Bytes RX Bytes TX Packets RX Pac		RX Packets	Listen Port	Status	Operation	
	Name:									
	MTU:			1420		(576-1440)				
	Listen	Port:		51820		(1-65535)				
	Private Key:					(Optional)				
	Public	Key:		2nKaZJITLWtm7loPU6CpU>						
	Local IP Address:									
	Status:		6	Enable						
	OK Cancel									
	ON	Cane								

Figure 7-1 Configuring the WireGuard VPN Server

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

Figure 7-2 Configuring the Peers

Choose the menu **VPN > WireGuard > Peers** and click **Add** to load the following page.

```
Peers
                                                                                                                              🔂 Add 🛛 😑 Delete
                            Endpoint
Port
                                                   TX Bytes RX Bytes TX Packets RX Packets Last
Handshake
                                        Allowed
       Interface Endpoint
                                                                                                               Status
                                                                                                                                 Operation
                                        Address
       Interface:
       Public Key:
       Endpoint:
                                                                (Optional)
                                                                (Optional, 1-65535)
       Endpoint Port:
       Allowed Address:
                                                               (Optional)
       Preshared Key:
       Persistent Keepalive:
                                    25
                                                                (0-65535)
       Comment:
                                   (0-128 characters)
                                  Enable
       Status:
                     Cancel
          ОК
```

You should configure an Endpoint and an Endpoint Port for at least one peer router.

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

	ID	Account Name	Protocol	Local IP Address	IP Address Pool	Network Mode	Remote Subnet	Operatio
	Account Password		Low	Middle High				
	Protocol:	:		•				
Local IP Address:								
	IP Addre	ss Pool:						
	DNS Add	Iress:						
	Network	Mode:		•				
	Max Con	nections:		(1-10	00)			
	Max Con							

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 router. 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 router.

Part 11 Configuring SSL VPN

CHAPTERS

- 1. Overview
- 2. Quick Setup
- 3. Status Configuration
- 4. SSL VPN Server Configuration
- 5. Resource Management
- 6. User Management
- 7. Authentication

1 Overview

SSL VPN provides remote users the access to the enterprise network from anywhere on the Internet. The remote access is enabled through a Secure Socket Layer (SSL) VPN gateway.

2 Quick Setup

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

Quick Setup					
General					
SSL VPN Server:	Enable				
Service Port:		•			
Virtual IP Pool:					
Primary DNS:					
Secondary DNS:		(Optional)			
Listen on Port:	1194	(1-65535)			
Export Certificate					
 The virtual IP pool sho Please configure a larg 	uld not overlap with th e IP Pool for SSL VPN	-	-		entication as
Back Next					

Follow the quick setup to configure the SSL VPN.

3 Status Configuration

This feature enables you to view the information of all the clients connected to the SSL VPN. You can also block or disconnect specific clients based on needs. Besides, you can view the currently locked out users, and add, delete or edit an entry.

Viewing the Status Information 3.1

Choose the menu **SSL VPN > Status > Connection** to load the following page.

Figure 3-7	1 Vie	ewing the Status Information						
Conne	ction	Locked Out User						
Online	Users							
	ID	Username	Login IP	Virtual IP	login Time	Upload	Download	Operation
	10	oschane	Login II	VICUUTI	login nine	opioda	Download	operation

In the Online Users section, you can view the information of all the clients connected to the SSL VPN. You can also block or disconnect specific clients based on needs.

Username	Displays the username a client used for login.
Login IP	Displays the IP address of a client.
Virtual IP	Displays the virtual IP address assigned to a client by the SSL VPN server.
Login Time	Displays the time when a client logged in.
Upload	Displays the total upload traffic of a client.
Download	Displays the total download traffic of a client.
Operation	Block or disconnect a client.
	Block: Disconnect a client and put the client into the list of Locked Out Users. A locked out user cannot log in again. To enable Username Lockout or IP Lockout, go to SSL VPN > SSL VPN Server > Advanced .
	Disconnect: Disconnect a client for once.

3.2 Viewing Locked Out User

Choose the menu **SSL VPN>Status > Locked Out User** to load the following page.

Figure 3-2 Viewing Locked Out User

Current	tly Locke	d Out Users			
				e A	dd 😑 Delete
	ID	Username	IP	Remaining Time	Operation

In the **Currently Locked Out Users** section, you can view the currently locked out users, and add user and set the **Locked Out Duration**, delete or edit an entry.

Туре	Displays locked out type.
Username	Displays the username of a locked out user.
IP	Displays the IP address of a locked out user.
Remaining Time	Displays the remaining effective time of a locked out entry.
virtua	re SSL VPN configuration, please go to Preferences > VPN IP Pool > VPN IP Pool to set a al IP pool for SSL VPN server. SSL VPN will take effect after the configuration is completed.

4 SSL VPN Server Configuration

In SSL VPN Server, you can enable the feature and configure the SSL VPN settings.

4.1 Configuring the SSL VPN Server

Choose the menu **SSL VPN > SSL VPN Server > SSL VPN Server** to load the following page.

Figure 4-1 Configuring the SSL VPN Server

SSL VPN Server			
General			
SSL VPN Server:	Enable		
Service Port:	SFP+ WAN1	•	
Virtual IP Pool:	admin	-	
Primary DNS:	211.127.160.5		
Secondary DNS:		(Optional)	
Export Certificate			
Advanced			
2 -1-1-1			
Save			

1. Please first go to Preferences > VPN IP Pool > VPN IP Pool to configure an IP pool for the virtual IP pool of the SSL VPN server.

- 2. The virtual IP pool should not overlap with the existing ones.
- 3. Please configure a large IP Pool for SSL VPN server.

4. The end-device cannot access the internet when SSL VPN is configured. If you want to access the internet, please select Local Authentication as Authentication Mode.

Check the box to enable the feature, then configure the corrresponding parameters

Service Port	Select the port for the SSL VPN server to listen on, and the VPN tunnel will take effect on the port.
Virtual IP Pool	Select a virtual IP Pool, and the SSL VPN server will assign an IP address to a connected client within the pool. To create an IP Pool, go to Preferences > VPN IP Pool > VPN IP Pool .
	The number of IP addresses in the IP pool should not be less than 4.
Primary DNS	Specify the IP address of the DNS server.
	Please assign the LAN IP to the SSLVPN DNS server.

.

_ _ __ _ _

Secondary DNS	Specify the IP address of the DNS server.				
DNS	Please assign the LAN IP to the SSLVPN DNS server.				
Listen on Port	Specify the port for the SSL VPN server to listen on. By default, it is 1194.				
Authentication Type	Select the authentication for the clients. For RADIUS Authentication, go to SSL VPN > Authentication to configure.				
Username Lockout	Block a client with the specific login username.				
LOCKOUL	Max. Login Attempts: Specify the maximum failed login attempts for a username. After the maximum attempt is reached, the username will be locked out.				
	Lock Duration: Specify how long the username will be locked out.				
IP Lockout	Block a client of the specific login IP.				
	Max. Login Attempts: Specify the maximum failed login attempts for a username. After the maximum attempt is reached, the username will be locked out.				
	Lock Duration: Specify how long the username will be locked out.				
Idle Timeout	Enable the feature and the VPN tunnel will close automatically if there is no traffic for the specified amount of time.				
Full Mode	Enable the feature and all traffic will go through the SSL VPN tunnel. When the feature is disabled, only the resource-related traffic will go through the tunnel.				
Note:					
	se first go to Preferences > VPN IP Pool > VPN IP Pool to configure an IP pool for the al IP pool of the SSL VPN server.				
• The v	rirtual IP pool should not overlap with the existing ones.				
Pleas	ase configure a large IP Pool for SSL VPN server.				

The end-device cannot access the internet when SSL VPN is configured. If you want to access

the internet, please select Local Authentication as Authentication Mode.

User Guide
207

5 Resource Management

This feature enables you to configure the resources the clients can access through the VPN tunnel, including IP range and domain name, or add the multiple tunnel resources to a group for better management.

5.1 Configuring the Resources

Choose the menu **SSL VPN > Resource Management > Tunnel Resources** and click **Add** to load the following page.

Figure 5-1 Configuring the Resources

unnel	Resourc	es					
						c	Add Oelete
	ID	Name	Domain Name/IP Address	Resource Group	Protocol	Port	Operation
	Name:			1-20 characters, digits	s, or underscores		
Resource Type:		ce Type:	IP Address	,			
IP Address/Subnet Mask:		ress/Subnet Mask:	/				
Protocol:		ol:		•			

Specify the name for the entry and configure other parameters, and click OK.

 Resource Type
 Select the type for the resources.

 IP Address: Specify IP range the clients can access, and the protocols the clients can use to access.

 Domain Name: Specify domain name the clients can access.
5.2 Grouping Tunnel Resources

Choose the menu **SSL VPN > Resource Management > Tunnel Resources** and click **Add** to load the following page.

Figure 5-2 Grouping Tunnel Resources

Tunnel	Resourc	es Resource Gr	oup			
Group	List					
					Ar	dd 🗢 Delete
	ID		Resource Group		Resources	Operation
	Decour	ce Group:		20 char	acters, digits, or underscores	
				L-20 Chan	acters, digits, of underscores	
	Resour	ces:				
	OK	Cancel				
	1		GROUP_LAN			2
	2		GROUP_ALL			1 T

Specify the name for the resource group, select the resources for the group, and click **OK**.



- GROUP_LAN refers to the resources of the LAN segment.
- GROUP_ALL refers to the resources of all network segments.

_ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _ _

6 User Management

This feature enables you to view and configure all user settings of the SSL VPN, or add multiple users to a group for better management.

6.1 Adding the User List

Choose the menu **SSL VPN > User Management > User** and click **Add** to load the following page.

Fig	ure 6	6-1 A	Adding the User	List					
	User	Use	er Group						
	User Li	ist							
								🔁 Add	🕒 🕒 Delete
		ID	Username		Us	er Group	Expiration Date	Status	Operation
		Userna	ime:			1-20 characters, dig			
		Passwo	ord:			1-64 characters, dig symbols	its, or haif-width		
		User G	roup:						
	Expiration Date:			MM/DD/YY					
	Max. Concurrent Users:				1-100				
		Status	:	💌 Enable					
		OK	Cancel						

Configure relevaant parameters and click **OK**.

Username	Specify the username a client used for login.
Password	Specify the password a client used for login.
User Group	Select which group the user belongs to. A user can only be added to one user group.
Expiration Date	Specify when the user will expire.
Max. Concurrent Users	Specify the maximum number of clients using the username for login concurrently. After the maximum number is reached, new login attempts will be rejected.
Status	Displays the status of the user entry.

6.2 Grouping Users

Choose the menu **SSL VPN > User Management > User Group** and click **Add** to load the following page.

-igure 6	6-2 0	Grouping Users				
User	Use	r Group				
User (Group List	t				
					🔁 Ad	dd 😑 Delete
	ID	Name		Group Member	Resource Group	Operation
	Name: Group Member:		1-20 characters, digits, or und	lerscores		
	Resource Group:		•			
	OK	Cancel				

Specify the name for the user group, select the resources for the group, and click **OK**.

Name	Specify a name for the user group.
Group Member	Select the users you want to add into the group. All users in the group share the same resources.
Resource Group	Select the resource group for the user group.

7 Authentication

This feature enables you to view and add authentication servers, or view and configure RADIUS server settings.

7.1 Adding the Authentication Server List

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

0							
Authe	ntication	Server Ra	dius Server				
Auther	ntication	Server List					
Column for Searching: Name 💌							
Server	Server Type:						
Search	Scope:		Search in All Entries				
Res	et Se	earch					
						🔂 Ade	d 😑 Delete
	ID Name Server Type Description Operati				Operation		
	Name:				1-20 characters, digits, or unde	erscores	
	Server	Type:	Radius				
		/ Server:					
	Second	ary Server:		•	(Optional)		
	Recove	r Time:			Minutes (30-1440)		
	Descrip	otion:			(Optional, 1-50 characters)		
	OK	Cancel	1				
	UK	Cancer					

Figure 7-1 Adding the Authentication Server List

Specify a name for the authentication server, configure relevant parameters and click **OK**.

Server Type	Select the type for the authentication server. Currently, only RADIUS server is supported.
Primary Server	Specify the primary server for authentication.
Secondary Server	Specify the secondary server for authentication. When the primary server is down, the secondary server will be used.
Recover Time	Specify the interval to connect the primary server again when the primary server is down.
Description	Enter a description for the server. User Guide = 212

Status

Displays the status of the user entry.

7.2 Configuring the Radius Server

Choose the menu **SSL VPN > Authentication > Radius Server** and click **Add** to load the following page.

	Server L	ist						
Columr	n for Sea	rching:	Name	•				
	Type:	-						
Search	Scope:		Search i	n the Results 🔹				
Rese	et Se	arch						
							Ad 🔁	d 🗢 Del
	ID	Nam	e	Authentication Address	Authentication Port	Accounting Port	Authentication Type	Operatio
	Name:				1-20 characters, digits			
	Name:	tication Server	IP:		1-20 characters, digits			
	Name: Authen	tication Server		 PAP	 1-20 characters, digits			
	Name: Authen Authen			PAP 🔻	 1-20 characters, digits (1-65535)			
	Name: Authen Authen Authen	tication Mode:		PAP V				
	Name: Authen Authen Authen Accoun	tication Mode: tication Port: ting Port:		РДР 🗸	(1-65535) (1-65535)			
	Name: Authen Authen Authen Accoun Pre-Sha	tication Mode: tication Port: ting Port: ared Key:		 PAP	(1-65535) (1-65535) (1-120 characters)			
	Name: Authen Authen Authen Accoun Pre-Sha	tication Mode: tication Port: ting Port:		PAP	(1-65535) (1-65535)			
	Name: Authen Authen Authen Accoun Pre-Sha Max. Ro	tication Mode: tication Port: ting Port: ared Key:		 PAP •	(1-65535) (1-65535) (1-120 characters)			

Figure 7-2 Configuring the Radius Server

Specify the name for the RADIUS server, configure relevant parameters and click OK.

Authentication Server IP	Specify the IP address of the RADIUS server.
Authentication Mode	Select the authentication protocol for the RADIUS server. Two authentication protocols are available: PAP and CHAP.
Authentication Port	Specify the UDP destination port on the authentication server for authentication requests. The recommended port is 1812.

Accounting Port	Specify the UDP destination port on the RADIUS server for accounting requests. The recommended port is 1813.
Pre-Shared Key	Specify the password that will be used to validate the communication between the router and the RADIUS authentication server.
Max. Request	Specify the maximum number of requests sent when no response is received.
Request Timeout	Specify the maximum interval for request timeout. After timeout, the request will be sent again.
NAS IP	Specify the IP address for the router to communicate with the RADIUS server.

Part 12

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 guestaccess 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 router. 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:





- 1) The client is connected to the router but not authenticated, and starts to visit the internet through HTTP;
- 2) The router 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 router forwards the username and password to the authentication server;
- 7) The authentication server returns the authentication result to the router;
- 8) The router 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 router 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 router.

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 router 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 router 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.

Settings		
Status:	Enable	
SSID&Interface:		•
Idle Timeout:	30	minutes (0 or 5-1440, 0 means always online)
Portal Authentication Port:	8080	(8080, 1024-65535)
Authentication Parameters		
Authentication Page:	Custom Page 🔹	
Background Picture:	Upload	(The image size cannot exceed 200KB.)
Welcome Information:		(1-50 characters)
Copyright:		(1-50 characters)
Page Preview:	Login Page Preview	
Authentication Type:	Local Authentication	
Expiration Reminder:	✓ Enable	
Time to Remind:	3	days (1-10)
Remind Type:	Remind Periodically	
Remind Interval:		minutes (1-120)
Remind Content:		(1-50 characters)
Page Preview:	Remind Page Preview	
Save		

Figure 2-1 Configuring the Authentication Page

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.
SSID&Interface	Specify the valid wireless interface and the effective interface, and you can specify more than one.
	The selected LAN Network contains all clients of the SSIDs that belong to this LAN Network.
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	Choose the authentication page type.
- uge	Custom : You can use the built-in web server to customize the authentication page by specifying the background picture, welcome information and copyright information.
	External Links : You can specify a external web server to provide the authentication page by entering the URL of the external web server.
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 ex	piration 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 router 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 router uses the built-in authentication server to authenticate users. You need to configure the authentication accounts for the local users.

The router 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.

ID	User Type	Useri	name	Authentication Timeout	I	MAC Address	Description	Status	Operation
 		-							
User Ty			Form	al User	_				
			FOIIII	ii Usei	•				
Userna	me:					(1-100 Charac	ters)		
Passwo	ord:					(1-100 Charac	ters)		
Expirat	ion Date:		2017-	12-31		(YYYY-MM-DD)			
Auther	tication Peroi	d:	00:00	-24:00		(нн:мм-нн:м	M)		
MAC Bi	nding Type:		Static	Binding	•				
MAC A	ddress :					(XX-XX-XX-XX-XX)			
Maxim	um Users:		1			(1-1024)			
Upstre	am Bandwidth	:	0			Kbps (0 or 10-1,000,000. 0 means no limit)			
Downs	tream Bandwi	dth:	0			Kbps (0 or 10-1,000,000. 0 means no limit)			
Name:						(1-50 characte	ers, optional)		
Telepho	one:					(1-50 characters, optional)			
Descrip	ition :		(1-50 characte	ers, optional)					
Status: 🕑 Enable									
OK Cancel									

Figure 2-2 Configuring the Formal User Account

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 Peroid	Specify the period during which the client is allowed to be authenticated.
MAC Binding Type	Specify the MAC Binding type. There are three types of MAC Binding: No binding, Static Binding and Dynamic Binding.
	No Binding: The client's MAC address will not be bound.
	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.
	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.
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

ID	User Type	User	name Authentication Timeout		١	1AC Address	Description	Status	Operation	
User Ty	pe:		Free U	Jser	•					
Userna	me:					(1-100 Charact	ters)			
Passwo	rd:					(1-100 Charact	ters)			
Authen (minut	tication Time es):	out	30	(1-14		(1-1440)	(1-1440)			
Authen	tication Peroi	d: 00:00		0-24:00 (HH:MM-HH:MM)		1)				
Maxim	imum Users: 1		1			(1-1024)				
Upstrea	am Bandwidth	:	0	0		Kbps (0 or 10-1,000,000. 0 means no limit)				
Downst	tream Bandwi	dth:	0			Kbps (0 or 10-1,000,000. 0 means no limit)				
Descrip	tion:					(1-50 characte	rs, optional)			
Status: 🕑 Enable										
OK	Canc	el								

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

Backup	
Backup	
Restore	
File: Restore	Browse

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 router 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:

. . _ _ . _ _ . _ _ . _ _ . _ .

- 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.



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.

User Guide 224

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.

Settings		
Status:	Enable	
SSID&Interface:		•
Idle Timeout:	30	minutes (0 or 5-1440, 0 means always online)
Portal Authentication Port:	8080	(8080, 1024-65535)
Authentication Parameters		
Authentication Page:	Custom Page 🔹	
Background Picture:	Upload	(The image size cannot exceed 200KB.)
Welcome Information:		(1-50 characters)
Copyright:		(1-50 characters)
Page Preview:	Login Page Preview	
Authentication Type:	Radius Authentication 🔹	
Primary Radius Server:		(Required)
Secondary Radius Server:		(Optional)
Authentication Port:	1812	(1024-65535)
Authorized Share Key:		(1-48 characters)
Retry Times:	3	(1-10)
Timeout Interval:	3	(1-60 seconds)
Authentication Method:	PAP 🔻	
Save		

Figure 3-1 Configuring the Radius Authentication

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.
SSID&Interface	Specify the valid wireless interface and the effective interface, and you can specify more than one.
	The selected LAN Network contains all clients of the SSIDs that belong to this LAN Network.
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	Choose the authentication page type.	
T dge	Custom : You can use the built-in web server to customize the authentication page by specifying the background picture, welcome information and copyright information.	
	External Links : You can use external pages by specifying the external links as the authentication page.	
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	Copyright Specify the copyright information to be displayed on the custom authenticatio 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 router 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
------------	-------------	---------	----------------

Settings		
Status:	Enable	
SSID&Interface:		*
Idle Timeout:	30	minutes (0 or 5-1440, 0 means always online)
Portal Authentication Port:	8080	(8080, 1024-65535)
Authentication Parameters		
Authentication Page:	Custom Page 🔹	
Background Picture:	Upload	(The image size cannot exceed 200KB.)
Welcome Information:		(1-50 characters)
Copyright:		(1-50 characters)
Page Preview:	Login Page Preview	
Authentication Type:	Onekey Online 🔹	
Free Authentication Timeout:	60	minutes (1-1440)
Save		

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.
SSID&Interface	Specify the valid wireless interface and the effective interface, and you can specify more than one.
	The selected LAN Network contains all clients of the SSIDs that belong to this LAN Network.

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.

Settings			
Status:	Enable		
SSID&Interface:			▼
Idle Timeout:	30		minutes (0 or 5-1440, 0 means always online)
Portal Authentication Port:	8080		(8080, 1024-65535)
Authentication Parameters			
Authentication Page:	Custom Page	•	
Background Picture:	Upload		(The image size cannot exceed 200KB.)
Welcome Information:			(1-50 characters)
Copyright:			(1-50 characters)
Page Preview:	Login Page Preview		
Authentication Type:	LDAP	•	
LDAP Profile:			
Save			

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.
SSID&Interface	Specify the valid wireless interface and the effective interface, and you can specify more than one.
	The selected LAN Network contains all clients of the SSIDs that belong to this LAN Network.

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.

	ID	Name	Туре	Source IP	Range	Destination IP Range	Source Port	Destination Port	Status	Operation
Na	ame:				(1-5	0 characters)				
Ту	pe:		Five Tuple Type	•						
So	ource IP Ra	nge:		/	(Opt	ional)				
Destination IP Range:			/	(Optional)						
Source MAC Address:				(XX-XX-XX-XX-XX, optional)						
So	ource Port F	Range:	-		(1-6	5535, optional)				
De	estination F	ort Range:	-		(1-6	5535, optional)				
Pro	Protocol: TCP 🔻									
De	escription :				(1-5	0 characters)				
St	atus:	(Enable 							
	ОК	Cancel								

Figure 6-1 Configuring the Five Tuple Type

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.
Туре	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 router 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

	ID	Name	Туре	Source IP Ran	ge Destination IP Range	Source Port	Destination Port	Status	Operation	
					· · · · · · · · · · · ·					
Na	Name:		(1	(1-50 characters)						
Ту	pe:		URL Type	•						
UR	URL Address:			(1	128 characters)					
So	urce IP Ra	nge:		/ (0	(Optional)					
So	Source MAC Address:			(X	(XX-XX-XX-XX-XX, optional)					
So	Source Port Range:		-	(1	(1-65535, optional)					
De	Description:			(1	(1-50 characters)					
Sta	atus:	[Enable 							
	ОК	Cancel								

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.
Туре	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:	
paramet	st Resource entry, if some parameter is left empty, it means the router will not restrict that er. For example, if the source IP range is left empty, it means all the clients can visit the 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.

LDAP	DAP Profiles									
								🕀 Add	Delete	
	ID	Name	Status	Bind Type	Server Address	Destination Port	Common Name Identifer	Base Distinguished Name	Operation	
	Sta Bir Se De Us Re	me: atus: nd Type: rver Address: estination Port: e SSL: gular DN: gular Password:	 Ena Ena 		(1-50 charact (1-64 charact (1-65535)					
	Co	mmon Name Identi			(1-100 chara	cters)				
	Ba	se Distinguished Na	me:		(1-200 characters)					
	Additional Filter:				(0-100 characters, optional)					
	Group Distinguished Name:			(0-200 chara optional)	cters, Q					
		OK Cancel								

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.

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

Authenticate	Authenticated User List							
Entry Count: 1								
	ID	Туре	Starting Time	IP Address	MAC Address	Operation		
	1	Local Authentication	2017-1-1 1:10:54	192.168.0.197	74-D4-35-9F-DB-1C	Ĩ		

Here you can view the clients that pass the portal authentication.

Туре	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.



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:	Enable	
Idle Timeout:	30	minutes (0 or 5-1440, 0 means always online)
Portal Authentication Port:	8080	(8080, 1024-65535)

 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 Parameter	5	
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**.

5 5	51 1	
Authentication Type:	Local Authentication 🔹	
Expiration Reminder:	✓ Enable	
Time to Remind:	3	days (1-10)
Remind Type:	Remind Once 🔹	
Remind Content:	Your account is about to ex	(1-50 characters)
Page Preview:	Remind Page Preview	
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.

ID	User Type	User	name	Authentication Timeout	MAC Address	Description	Status	Operation			
User Ty	pe:		Forma	al User	•						
Userna	me:		Room	101	(1-100 Charac	ters)					
Passwo	rd:		1234	56	(1-100 Charac	ters)					
Expirat	ion Date:		2017	-12-31	(YYYY-MM-DD)	(YYYY-MM-DD)					
Authentication Peroid:		d:	00:00-24:00		(HH:MM-HH:M	(нн:мм-нн:мм)					
MAC Bi	nding Type:		No Bir	nding	•						
Maximu	ım Users:		3		(1-1024)						
Upstrea	am Bandwidth		0		Kbps (0 or 10-	1,000,000. 0 means no limit)					
Downst	ream Bandwi	dth:	0		Kbps (0 or 10-	1,000,000. 0 means no limit)					
Name:					(1-50 characte	rs, optional)					
Telephone:		(1-50 characte	(1-50 characters, optional)								
Description:				(1-50 characte	rs, optional)						
Status:			🕑 Enab	le							
ОК	Canc	el									

After all the configuration finished, the guest can use the account to authenticate and access the internet after the authentication succeeded.

Part 13 Managing Services

CHAPTERS

- 1. Services
- 2. Dynamic DNS Configurations
- 3. UPnP Configuration
- 4. Configuration Example for Dynamic DNS
- 5. mDNS Configuration Configuration
- 6. Reboot ScheduleReboot Schedule
- 7. DNS ProxyDNS 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
- Custom DDNS

2.1 Configure and View Peanuthull DDNS

Choose the menu **Services** > **Dynamic DNS** > **Peanuthull** and click **Add** to load the following page.

ID	Interface	Account Name		Update Interval	Status	Service Status	Domain Name	Service Type	Operation
Interface: Account Name: Password: Update Interval: Status: OK Cancel			 I En	able	G	<u>o to register</u>			

Figure 2-1 Configure Peanuthull DDNS

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.												
	Stat	tus		Check	the box	to enable the	DDNS service.						
---	---	------	---	--------------------	--------------------	----------------	----------------	-------------------	---------------------------	-------------	--	--	--
3)	View the DDNS status.												
Figure 2-2 View the Status of Peanuthull DDNS													
	Peanuthull												
									🔂 Ac	dd 😑 Delete			
	ID ID		Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Service Type	Operation			
		1	WAN1	user1	6 hours	Enabled 😣	Offline			C 🔋			
	Ser	vice	ce 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 nor	mally.						
	Incorrect account name or password: The account name or password is incorrect.									word is			
	Domain Name Displays the Domain Names obtained from the DDNS server.												
	Ser	vice	Туре	Display service		DDNS service	type, includin	g Professional se	ervice and S [.]	tandard			

2.2 Configure and View Comexe DDNS

Choose the menu **Services** > **Dynamic DNS** > **Comexe** and click **Add** to load the following page.

Figure 2-3 Configure Comexe DDNS

	ID	Interface	Accoun	t Name	me Update Sta		atus	Service Status	Domain Name	Operation
			-							
	Interfa	ace:				•				
	Account Name:					Go to registe	<u>er</u>			
	Passw	ord:								
	Update Interval: Status:					•				
			💌 Enable	e						
	OK Cancel									

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

						0	Add 😑 Delete
ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Operation
1	WAN1	user1	6 hours	Enabled 😣	Connecting		2

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 **Services** > **Dynamic DNS** > **DynDNS** and click **Add** to load the following page.

ID	Interface	Account Name		Update Interval	Status		Service Status	Domain Name	Operation
 		-							
Passw Domai	nt Name: ord: in Name: e Interval:				•	<u>Go to regist</u>	<u>er</u>		
Oł		ncel							

Figure 2-5 Configure DynDNS

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

				Update			0	Add 😑 Del
	ID	Interface	Account Name	Interval	Status	Service Status	Domain Name	Operation
	1	WAN1	user1	6 hours	Enabled 😢	Connecting	domainname1.com	0 🕯
Stat	tus		Displays v	vhether	the correspond	ling DDNS service is	enabled.	

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.					
	Incorrect domain name: The domain name is incorrect.					
Domain Name	Displays the Domain Names obtained from the DDNS server.					

2.4 Configure and View NO-IP DDNS

Choose the menu **Services** > **Dynamic DNS** > **NO-IP** and click **Add** to load the following page.

	ID	Interface	Accoun	nt Name Update Interval		St	atus	Service Status	Domain Name	Operation
			-							
	Interface: Account Name: Password:					•	<u>Go to regist</u>	<u>er</u>		
Domain Name: Update Interval:					•					
Status:			💌 Enable	e						
	Oł	Ca	ncel							

Figure 2-7 View NO-IP DDNS

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.

3)

Update Interval Specify the Update Interval that the device dynamically updates IP addresse registered domain names.											
Status Check the box to enable the DDNS service.											
View the DDNS status.											
F	Figure 2-8 View the Status of NO-IP DDNS										
	NO-IP										
								0	Add 😑 Delete		
		ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Operation		
		1	WAN1	user1	6 hours	Enabled 🙁	Connecting	domainname1.com	2		
	Stat	us		Displays v	vhether	the correspond	ding DDNS service is	enabled.			
	Ser	vice S	Status	Displays t	he curre	ent status of DE	ONS service.				
				Offline: D	DNS se	rvice is offline.					
				Connecti	ng: DDN	NS client is conr	necting to the server				
				Online: DI	DNS is v	working normall	у.				
	Incorrect account name or password: The account name or password is incorrect.										
				Incorrect	domaiı	n name: The do	main name is incorre	ect.			
	Domain Name Displays the Domain Names obtained from the DDNS server.										

2.5 Custom DDNS

The router lists common DDNS service providers. If the service provider you registered at is not listed, you can add a custom DDNS entry.

- 1) Register at a service provider, and get your username, password, and domain name.
- 2) Choose the menu **Service** > **Dynamic DNS** > **Custom DDNS** and click **Add** to load the following page.

Figure	2-9	Custom	DDNS						
Gener	al								
Updat	e URL:								
Sav	/e								
Custor	m DDNS								
								c	Add 😑 Delete
	ID	Interface	Account	Name	Update Interval	Status	Service Status	Domain Name	Operation
	Passw Doma	nt Name: ord: in Name: e Interval: s:	ncel	 Y Enable	2	▼ ≫*			

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

Update URL	Enter the URL provided by your DDNS service provider in format of http://[USERNAME]:[PASSWORD]@api.cp.easydns.com/dyn/tomato.php?hostname=[DOMAIN]&myip=[IP]. The router will automatically update user information to the service provider.
Interface	Select the WAN port which the DDNS entry applies to.
Account Name	Enter your account name for the service provider.
Password	Enter your password for the service provider.
Domain Name	Enter the domain name provided by your service provider. Remote users can use the domain name to access your local network through WAN port.
Update Interval	Specify the update interval to report the change of the WAN IP address for DDNS service.
Status	Click the checkbox to enable the entry.

3 UPnP Configuration

UPnP (Universal Plug and Play) is the networking protocol that allows devices to discover each other and then establish connections for communication. With the help of UPnP, It is convenient to realize seamless connections between the devices, especially from WAN to LAN.

Choose the menu **Services** > **UPnP** to load the following page.

Figure 3-1 Configure	UPnP		
General			
Enable UPnP			
LAN Interface:	LAN		
Interface:			
Save			
UPnP Portmap List			

						🗢 Delete 🗧	Delete All	🖉 Refresh
ID	Description	Protocol	Interface	IP Address	External Port	Internal Port	Status	Operation

Follow these steps to configure UPnP.

- 1) Check the box to enable the **UPnP** function.
- 2) Specify the effective interfaces. Then click Save
- 3) (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 router.
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 router's web management interface using another host on the internet.



4.2 Configuration Scheme

For security management, the internet hosts attempting to manage the router must be permitted by the router. 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 router may be changed each time the dial-up connection is established. When the public IP address of the router 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 router 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 router, we take Peanuthull DNS as an example here.

 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

							O A	dd 🕒 Dele
ID	Interface	Account Na	me Update Interval	Status	Service Status	Domain Name	Service Type	Operation
Pass	unt Name: word: ate Interval:			<u>Got</u>	<u>to register</u>			

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

eant	ithull							O A	dd 😑 Dele
	ID	Interface	Account Name	Update Interval	Status	Service Status	Domain Name	Service Type	Operation
	Acco Pass Upda Stati		6	hours	▼ Gott	<u>o register</u>			

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.

mDNS							
	d Rules:	Repeater: Enab	le	•			
mDNS	(Bonjour) Rules				Ad	d 🕒 Delete
	ID	Description		Service Network	Client Network	Services	Operation
		Network: Network:		• • •			
	1	lt		All	All		

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.

ervic	es				
				🕒 Ado	Del
	ID	Name	Domain	Туре	Operatio
	Name: Domain OK	1: Cancel			
	1	any	any	Default	
	2	AirPlay	_airplaytcp,_raoptcp,_appletv-v2tcp	Default	
	3	AFP	_afpovertcptcp	Default	
	4	BitTorrent	_bittorrenttcp	Default	
	5	FTP	_ftptcp,_sftp-sshtcp	Default	
	6	iChat	_presencetcp,_ichattcp	Default	
	7	iTunes	_daaptcp,_home-sharingtcp,_apple- mobdevtcp,_dacptcp	Default	
	8	Printers	_ipptcp,_pdl- datastreamtcp,_printertcp,_httptcp, _http_alttcp,_ipp-tlstcp,_fax- ipptcp,_riousbprint_tcp,_ica- networking2tcp,_ica- networking2tcp,_ptptcp,_canon- bjnp1tcp,_ippstcp	Default	
	9	Samba	_smbtcp,_smbdirecttcp	Default	
	10	Scanners	_ipptcp,_pdl- datastreamtcp,_scannertcp,_httptcp ,_http_alttcp,_ipp-tlstcp,_fax- ipptcp,_riousbprinttcp,_ica- networking2tcp,_icp,_ica- networking2tcp,_ptptcp,_canon- bjnp1tcp,_ippstcp	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.

				🔂 Add 🛛 😑 Dele
ID	Name	Status	Next Execution	Operation
us: irrence: DK Cance	Enable Every on at	00 🔹 : 00	▼ in Pacific Time.	

Figure 6-1 Configure Reboot Schedule

 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.

DNSSEC				
DNSSEC:	Enable			
DNS Server:	8.8.8.8	🔁 Add		
	8.8.4.4	🖨 Minus		
Action for Bog	us Replies: 🔿 Pass 💿 Di	rop		
Save				
Diagnose				
Domain:				
Туре:	⊖ IPv4 ⊖ IP	Pv6		
DNS Server:				
D ¹				
Diagnose				
Result				🗑 Clear
ID	Domain Name	Туре	IP Address	Verify Result

Figure 7-1 Configure DNSSEC

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.	
Туре	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.	

In **Diagnose** section, configure the following parameters.

7.2 DOH

Choose the menu **Services** > **DNS Proxy** > **DOH** to load the following page.

Figure 7-2	Configure DOH

OH S	erver: 🗌 Enable			
Sav	e			
	Provider	DNS Server	● Ad Status	d Operation
	Name: DNS Server: https:// Status: Enable			
	Google	https://dns.google/dns-query	Disabled 🥑	
	Cloudflare	https://cloudflare-dns.com/dns-query	Disabled 🥑	
	Quad9_1	https://dns.quad9.net/dns-query	Disabled 🥑	
	Quad9_2	https://dns9.quad9.net/dns-query	Disabled 🕑	

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

OT Se	erver			
DT Se	erver: 🗌 Enable			
Sav	e		➡ Add	d 🗢 Dele
	Provider	DNS Server	Status	Operatio
		-		
	DNS Server: Enable	Add		
	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 🥑	

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 14 System Tools

CHAPTERS

- 1. System Tools
- 2. Admin Setup
- 3. Controller Settings
- 4. Management
- 5. SNMP
- 6. Diagnostics
- 7. LED Control
- 8. Time Settings
- 9. System Log

1 System Tools

1.1 Overview

The System Tools module provides several system management tools for users to manage the router.

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 router. With this function, you can reset the router, backup and restore the configuration file, reboot the router 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 router 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 router 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 router. You can also configure the router 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

Admin Setup 2.1

Choose the menu **System Tools > Admin Setup > Admin Setup** to load the following page.

Account		

Figure 2-1 Modifying the Admin Account

Account	
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)
Low Middle High	
Confirm New Password:	(6-15 letters, digits or special characters)
Save	

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 Manage	ment			🔂 Add 🛛 😑 Delet
	ID	Subnet/Mask	Status	Operation
Subnet/Mask: Status:		/ /		
ОК	Cancel			

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.

Settings		
HTTP Server Port:	80	(80, 1024-65535)
	Redirect HTTP to HTTPS	
HTTPS Server Port:	443	(443, 1024-65535)
HTTPS Server Status:	🕑 Enable	
Web Idle Timeout:	60	minutes (5-60)
Save		

Figure 2-3 Configuring System Settings

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 router, make sure the router can be discovered by the controller. Controller Settings enable your router to be discovered in either of the following scenarios.

- If you are using Omada Cloud-Based Controller, Enable Cloud-Based Controller Management.
- If your router and controller are located in the same network, LAN and VLAN, the controller can discover and adopt the router without any controller settings. Otherwise, you need to inform the router 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 Cl	loud-Based Controller	Management
---------------	-----------------------	------------

Cloud-Based Controller M	anagement
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 router of the controller's URL/IP address, and click **Save**. Then the router makes contact with the controller so that the controller can discover the router.

Figure 3-2 Cloud-Based Controller Management

Controller Inform URL	
Inform URL/IP Address:	
Save	

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 Reseting the Device

Factory Defaults	
Revert all the configuration to factory default.	
Factory Restore	

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

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
Restore
Restore saved settings from a file.
File: Browse Restore Image: Comparison of the second seco

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 router.

4.3 Reboot

Choose the menu **System Tools > Management > Reboot** to load the following page.

Figure 4-3	Rebooting the Device
Reboot	
Reboot	

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
```

Firmware Upgrade	
Firmware Version:	1.0.0 Build 20200422 Rel.65131
Hardware Version:	ER605 v1.0
New Firmware File:	Browse
Upgrade	

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.

SNMP		
SNMP:	 Enable 	
Contact:	www.tp-link.com	
Device Name:	ER605	
Location:	TP-Link	
Get Community:	public	
Get Trusted Host:	0.0.0.0	
Set Community:	private	
Set Trusted Host:	0.0.0.0	
Save		

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 routers along the route path.

6.1.1 Configuring Ping

Choose the menu **System Tools > Diagnostics > Diagnostics** to load the following page.

Diagnostics	
Diagnostic Tool:	Ping
Destination IP/Domain Name:	
Interface:	*
Start	
 Advanced 	
The Router is ready.	

Figure 6-1 Configuring Diagnostics

Follow these steps to configure Diagnostics:

1) In **Diagnostics** section, select **Ping** and configure the following parameters.

Diagnostic Tool Select **Ping** to test the connectivity between the router and the desired device.

Destination IP/ Enter the IP address or the domain name that you want to ping or tracert. Domain Name

- 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

۲			
Ping Count:		4	(1-50)
Ping Packet Size:		64	(4-1472 Bytes)
Ping Count	Specify the	e count of the test packets	to be sent during the ping process.
Ping Packet Size	Specify the	e 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:	•
Start	
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 router and the desired device.
Destination IP/ Domain Name	Enter the IP address or the domain name that you want to ping or tracert.
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

 Image: Comparison of the content of th

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.



Remote Assistance		
It is recommended not to enable Remote Assistance. Enable this function with the help of technicians if needed. Remote Assistance: Enable		
Save		
Diagnostic Information		
You can export diagnostic information and send it to technicans for assistance.		

- In the Remote Assistance section, check the box and click Save to enable the remote assistance function and then the technicians can access your router 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 LED Control

You can manually turn on or off the LED via a web browser.

Choose the menu System Tools > LED Control, check the box to turn on or off the LED.

Figure 7-1 Getting Automatically from the Internet

LED ON/OFF	
LED:	✓ Enable
Save	

8 Time Settings

In Time Settings module, you can configure the following features:

- System Time
- Daylight Saving Time

8.1 Setting the System Time

Choose one method to set the system time.

8.1.1 Getting time from the Internet Automatically

Choose the menu **System Tools** > **Time Settings** > **Time Settings** to load the following page.

Figure 8-1 Getting Automatically from the Internet

Time Settings		
Current Time :	01/01/2017 03:31:00	
Time Config:	• Get automatically from the Interne	et 🔿 Manually
Time Zone:	(GMT-08:00) Pacific Time	•
Primary NTP Server:	0.0.0.0	
Secondary NTP Server:	0.0.0.0	(X.X.X.X, optional)
Save		

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.

8.1.2 Setting the System Time Manually

Choose the menu **System Tools** > **Time Settings** > **Time Settings** to load the following page.

Time Settings	
Current Time :	01/01/2017 03:44:07
Time Config:	 Get automatically from the Internet Manually
Date:	01/01/2017 (MM/DD/YYYY)
Time:	03 ▼ : 26 ▼ : 44 ▼ (HH/MM/SS)
Synchronize with PC's Clo	ock
Save	

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 router with PC's clock.

8.2 Setting the Daylight Saving Time

Choose one method to set the daylight saving time.

8.2.1 Predefined Mode

Choose the menu **System Tools** > **Time Settings** > **Time Settings** to load the following page.

Daylight Saving Time			
DST Status:	Enable		
Mode:	Predefined Mode	O Recurring Mode	O Date Mode
Predefined Country:	Europe 🔹		
Save			

Figure 8-3 Predefined Mode Page

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.

8.2.2 Recurring Mode

Choose the menu **System Tools** > **Time Settings** > **Time Settings** to load the following page.

Figure 8-4 Recurring Mode Page

Daylight Saving Time													
DST Status:	💌 Enable												
Mode:	O Predefined Mode Recurring Mode Date Mode												
Time Offset:	60		minutes (1	-18	D)								
Starting Time:	Last	•	Sun	•	in	Mar	•	at	01	•	:	00	•
Ending Time:	Last	•	Sun	•	in	Oct	•	at	01	•	:	00	•

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.

8.2.3 Date Mode

Choose the menu **System Tools** > **Time Settings** > **Time Settings** to load the following page.

Figure 8-5 Date Mode Page

Daylight Saving Time													
DST Status:	Enable												
Mode:	O Predefined Mode O Recurring Mode O Date Mode												
Time Offset:	60		minutes (1-180)										
Starting Time:	2014 🔻	-	Mar	•	-	01	•	at	01	•	:	00	•
Ending Time:	2014 💌	-	Oct	•	-	01	•	at	01	•	:	00	•
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 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.

9 System Log

Choose the menu **System Tools** > **System Log** > **System Log** to load the following page.

igure	9-1 System Log	g Page			
Log S	ettings				
✓ Enable Auto-refresh✓ Severity					
		All Level	•		
Send Log					
Serve	r IP:	0.0.0.0			
Sa	ve				
Log Li	ist				
				💋 Refresh	😑 Delete Al
ID	Time	Module	Level	Content	
1	2017-01-01 16:48:45	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!	
2	2017-01-01 16:47:37	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!	
3	2017-01-01 15:37:23	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!	
4	2017-01-01 15:27:04	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!	
5	2017-01-01 01:47:17	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!	
6	2017-01-01 00:10:12	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!	
7	2017-01-01 00:07:12	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!	
9	2017-01-01 00:01:39	WEB	NOTICE	192.168.0.200 Has logged in to web managment system successfully!	
10	2017-01-01 00:01:38	WEB	NOTICE	192.168.0.200 Has logged in to web managment 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	e Log				

Follow these steps to view the system log:

1) In the **Log Settings** section, configure the following parameters and click **Save**.

Enable Auto-
refreshCheck the box to enable this function and the page will refresh automatically
every 10 seconds.

Severity	Enable Severity and specify the importance of the logs you want to view in the log list.
	ALL Level: Logs of all levels.
	EMERGENCY : Errors that render the router unusable, such as hardware errors.
	ALERT: Errors that must be resolved immediately, such as flash write errors.
	CRITICAL : Errors that put the system at risk, such as a failure to release memory.
	ERROR: Generic errors.
	WARNING: Warning messages, such as WinNuke attack warnings.
	NOTICE: Important notifications, such as IKE policy mismatches.
	INFO: Informational messages.
	DEBUG : Debug-level notifications, such as when the router receives a DNS packet.
Send Log	Enable the Send Log function and then the newly generated logs will be sent to the specified server.
Server IP	Specify the IP address of the server that the logs will be sent to.

2) (Optional) Click **Save Log** to save the current logs to the host.