



GBR-4001

4-WAN Gigabit Broadband VPN Router

User Manual

V1.0

Digital Data Communications Asia Co., Ltd.

<http://www.level1.com>

Table of Contents

Table of Contents	II
Introduction	1
0.1 Factory settings.....	1
0.2 Contact Us	1
Chapter 1. Product Overview	2
1.1 Key characteristics	2
1.2 Specifications	3
Chapter 2. Hardware Installation	4
2.1 Panel description.....	4
2.2 Precaution for installation	5
2.3 Preparing for installation	5
2.4 Hardware Installation	6
2.5 Hardware connection.....	7
Chapter 3. Login to the device	8
3.1 Configuring the correct network settings	8
3.2 Login to the device.....	9
Chapter 4. Configuration Wizard	12
4.1 WAN1 Port Configuration - Dynamic IP access	12
4.2 WAN1 port configuration - Static IP access	13
4.3 WAN1 configuration -- PPPoE access.....	13
Chapter 5. Start menu	15
5.1 Configuration Wizard	15
5.2 Interface status.....	15
5.3 Interface Traffic	16
5.4 Restart Device	17
Chapter 6. Network parameters	18
6.1 Configuration of WAN port.....	18
6.1.1 Network interface configuration	18
6.1.2 Internet Connection List.....	22
6.2 Line combination	24
6.2.1 Description of line combination function	25
6.2.2 Global Settings.....	26
6.2.3 Load Balancing List.....	28
6.2.4 Detection and Bandwidth	28
6.2.5 Identity Binding	29
6.3 Configuration of LAN port	30
6.4 DHCP server	31
6.4.1 DHCP server configuration	31
6.4.2 Static DHCP	33

6.4.3	DHCP auto binding	35
6.4.4	DHCP client list	35
6.4.5	Case of DHCP configuration	36
6.5	DDNS Settings	38
6.5.1	DDNS authentication.....	39
6.6	UPnP	40
Chapter 7.	Advanced Configuration	41
7.1	NAT and DMZ configuration	41
7.1.1	Description of NAT functions	41
7.1.2	Port Forwarding	42
7.1.3	NAT rules	45
7.1.4	DMZ.....	47
7.1.5	NAT and DMZ configuration instances	48
7.2	Static Route Settings	50
7.3	Policy routing	52
7.3.1	Enable policy routing.....	53
7.3.2	Policy routing configuration	53
7.4	Anti-NetSniper	55
7.5	Port mirroring.....	55
7.6	Port VLAN.....	56
7.7	SYSLOG configuration	58
Chapter 8.	User management.....	59
8.1	User status.....	59
8.2	IP/MAC binding	61
8.2.1	IP/MAC binding list	62
8.2.2	IP/MAC binding configuration	63
8.2.3	IP/MAC binding instances	64
8.3	PPPoE Server	67
8.3.1	PPPoE introduction	67
8.3.2	PPPoE global Settings	68
8.3.3	PPPoE account configuration	70
8.3.4	PPPoE user status	72
8.3.5	Export PPPoE Accounts	73
8.3.6	Import PPPOE Accounts	74
8.3.7	Instance of PPPoE server configuration	75
8.4	WEB authentication	77
8.4.1	WebAuth Global Settings	77
8.4.2	Web Authentication Account List.....	78
8.4.3	WEB Authentication Client Status	80
8.5	User Group Settings	81
Chapter 9.	App Control	82
9.1	Schedule Settings.....	82

9.2	Application Control.....	83
9.2.1	Application Management List.....	84
9.2.2	Internet Application Management Settings.....	84
9.2.3	Internet Application Management	86
9.3	QQ white list	88
9.4	TM Whitelist	90
9.5	Notification	91
9.5.1	Daily Routine Notification	92
9.5.2	Account expiration notification.....	93
9.6	Application Audit.....	94
9.7	Policy Database	95
Chapter 10.	QoS.....	97
10.1	Fixed Rate Limiting	97
10.2	Flexible bandwidth.....	98
10.3	Session Limiting	100
Chapter 11.	Firewall.....	102
11.1	Attack Prevention	102
11.2	Access control	103
11.2.1	Access Control Rule	104
11.2.2	Access control list	105
11.2.3	Access Control Settings	106
11.2.4	Access Control Settings instance	112
11.3	Domain filtering	115
11.3.1	Domain filtering Settings	115
11.3.2	Domain Block Notification	116
11.4	MAC Address Filtering	118
11.4.1	MAC Address Filtering	119
11.4.2	MAC Address Filtering Settings	120
Chapter 12.	VPN.....	122
12.1	PPTP	122
12.1.1	PPTP overview.....	122
12.1.2	PPTP list.....	123
12.1.3	PPTP server configuration.....	124
12.1.4	PPTP client Settings	126
12.1.5	PPTP configuration instance.....	128
12.2	IPSec	133
12.2.1	IPSec Overview	133
12.2.2	IPSec list	140
12.2.3	IPSec Settings	140
12.2.4	IPSec configuration instance	146
Chapter 13.	System	154
13.1	Administrator	154

13.2	Language	155
13.3	Time	155
13.4	Configuration	157
13.5	Firmware Upgrade	158
13.6	Remote Management.....	159
13.7	Scheduled task	160
Chapter 14.	System	162
14.1	Interface Status	162
14.2	System information	162
14.3	System log	163
14.3.1	System log information	163
14.3.2	Log Management Settings.....	165
Chapter 15.	Customer service	166
Appendix A	Configuration of LAN computers	167
Appendix A	FAQ	170
B-1.	How ADSL users go online?	170
B-2.	How the Fixed IP access users go online?.....	171
B-3.	How the Dynamic IP (Cable Modem) access users go online?.....	171
B-4.	How to restore the device to its factory settings?.....	172
Appendix B	Figure Index.....	174
Appendix C	LICENSE STATEMENT / GPL CODE STATEMENT	178

Introduction

⊕ **Tip:** In order to achieve the best results, it is proposed to upgrade Windows Internet Explorer browser to Version 6.0 or above.

0.1 Factory settings

1. The factory settings of interfaces are shown in Table 0-1.

Type of interfaces	IP address/subnet mask
LAN port	192.168.1.1/255.255.255.0
WAN port	Dynamic IP access

Table 0-1 Factory settings of interfaces

2. The factory user name of the system administrator is admin, and the factory password is admin (case-sensitive).

0.2 Contact Us

If you have any questions during installation or use, please contact us in the following manners.

- Customer service: 0800-011-110
- LEVELONE discussions: <http://www.level1.com>
- E-mail support: support@level1.com

Chapter 1. Product Overview

1.1 Key characteristics

- Support DSL, FTTX+LAN and Cable Modem and other access modes
- Support the configuration of dynamic WAN port
- Support traffic load balancing and line backup
- Support policy routing
- Support intelligent bandwidth management function
- Support fine speed limit
- Support the DHCP server function
- Support virtual server and DMZ
- Support the PPPoE server functions, and provide a fixed IP allocation, account billing and other functions
- Support routine business notification, due account notification functions
- Support WEB authentication function
- Support Internet behavior management for users, and provide a wealth of controlling policies
- Support SYSLOG configuration
- Support the Internet behavior audit function
- Support URL, MAC address, keyword filtering and other firewall policies
- Support QQ, MSN white list
- Support internal/external network attack and defense
- Support network vanguard
- Support port mirroring
- Support port VLAN
- Support user groups, time management
- Support multiprotocol VPN (PPTP, IPSec)

- Support UPnP
- Support dynamic domain names (3322. org, iplink. com. cn)
- Support HTTP remote management
- Support the WEB upgrading mode
- Support backup and import of WEB configuration files
- Support filtering of MAC addresses

1.2 Specifications

- Meets IEEE802.3 Ethernet and IEEE802.3u Fast Ethernet standards.
- Supports TCP/IP, DHCP, ICMP, NAT, PPPoE, static routes and other protocols.
- The physical ports support auto negotiation function, and support the MDI/MDI - X adapter function.
- Provide status indicators.
- Operating environment: Temperature: $0 \pm 40^{\circ}\text{C}$
Height: 0-4000m
Relative humidity: 10%-90%, no condensation

Chapter 2. Hardware Installation

2.1 Panel description



Figure 2_1 Front Panel - GBR-4001



Figure 2_2 Rear Panel - GBR-4001

1. LED description

LED lights	Description	Function
PWR	Power indicator	It is constantly on when the power supply is working properly.
SYS	System status indicator	Flashes in the frequency of 2 times per second, and the flashing frequency declines when the system burden is heavy; Defective often light or often.
Link/Act	Port status indicator	When a device is properly connected to a port, the status LED that corresponds to the port stays lit, and it will flash if there is flow.
100M	Port rate LED	When a device is connected to a port and after the success of 100M negotiation, the LED corresponding to the port stays lit.

Table 2_1 LED description

2. Description of interfaces

Interface	Meaning	Notes	Remarks
LAN	LAN interface	Integrated with multiple switched Ethernet ports. Some products are provided with only one LAN port.	LAN/WAN are all RJ-45 ports, and support the adapter function.

WAN	WAN interface	The number of WAN interfaces depends upon product model.	
Console	Serial port	Asynchronous communication serial ports that meet the RS232 standard	Some products support the Console port.

Table 2_2 Description of interfaces

3. Reset button

Reset button can be used to recover the device's factory settings when you forget the administrator password. Method: In the process of charged operation, hold down the Reset button for more than 5 seconds, and then release the button. The device will be returned to its factory settings after operation, and automatically restart.

⊕ **Note:** The above operations will delete all the original device configurations; please use it with care!

2.2 Precaution for installation

1. Make sure to install the workbench and ensure the stability of the rack.
2. Do not place any heavy objects on the device.
3. Make sure that the device is stored in a dry and ventilated area with proper heat dissipation, and do not put it in a dirty and damp place.
4. Avoid exposing the device directly to the sunlight and keep it far away from heating elements;
5. Please use the original power cord.

2.3 Preparing for installation

1. We have applied to local operators (ISP, such as China Telecom, China Unicom, etc.) for broadband services.
2. Preparation of related devices:
 - 1) Modem (This item is not required when connected directly to Ethernet).
 - 2) Hub or switch.

- 3) The PC with Ethernet card and Internet Protocol (TCP/IP) installed.
 - 4) Power socket.
3. Preparation of tools and cables: Phillips screwdriver, network cable.

2.4 Hardware Installation

Before installing the device, make sure the broadband service is normal. If you cannot access, please contact operators (ISP) to resolve the problem. After successfully accessing to the network, follow these steps to install the device. The power plug must be removed during installation.

1. Installed on the work bench

Place the device on a stable workbench, and the installation steps are as follows:

1. Place the device on a sufficiently large, stable and properly grounded workbench, with its bottom up;
2. Remove the adhesive protective paper from the foot pad, and stick the 4 pads in the 4 round slots at the bottom of the casing respectively.
3. Flip over the device, and place it on the workbench stably.

2. Install on the standard rack

Install the device on a 19-inch standard rack, and the installation steps are as follows:

1. Check the grounding and stability of the rack.
2. Install the two L-shaped brackets in the accessories on both sides of the device panel, and fix them with the screws in the accessories.

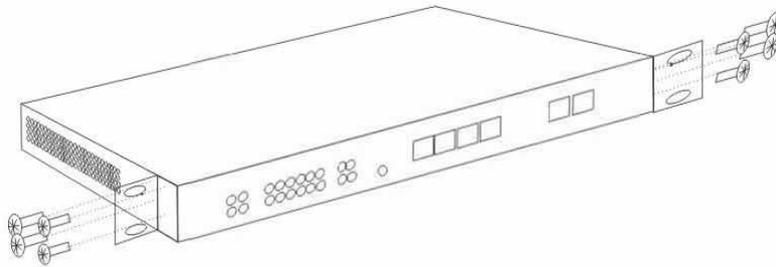


Figure 2_3 Product rack installation drawing I

3. Place the device in the appropriate location in the rack, and support it using a tray.
4. Secure the L-shaped brackets on the guide slots (as shown in the figure below) fixed at both ends of the rack.

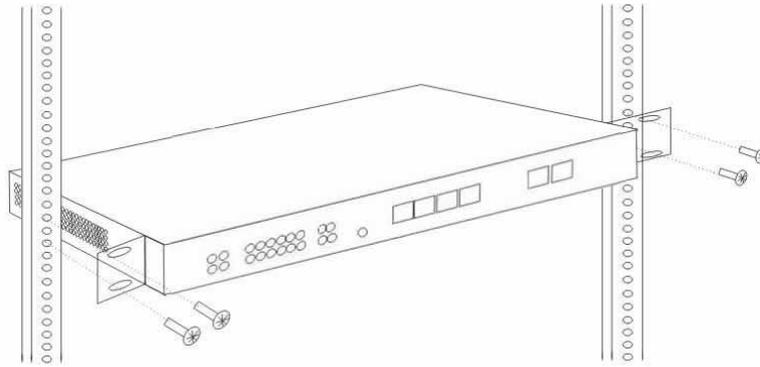


Figure 2_4 Product rack installation drawing II

2.5 Hardware connection

1. Establish a LAN connection

Connect the LAN port of the router or a PC or a hub or a switch in LAN with a network cable.

2. Establish a WAN connection

Connect the WAN port of the router to the Internet with a network cable, as shown in the figure below.

3. Connect the power supply

Before connecting the power supply, make sure that both power supply and grounding are correct.

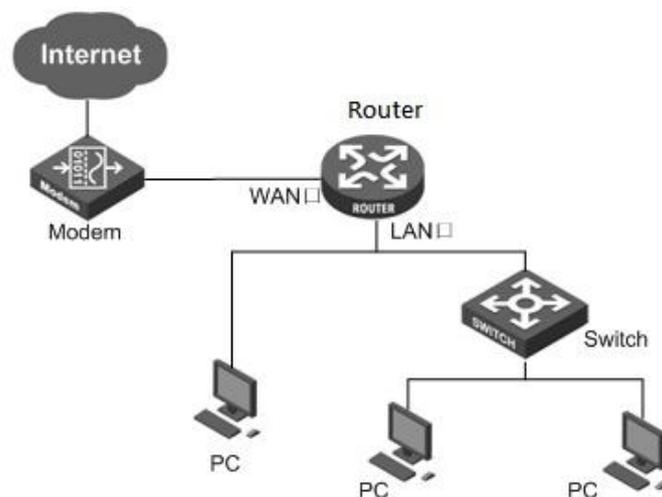


Figure 2_5 Establish a connection to LAN and WAN

⊕ **Tip:** The above network connection diagram is for reference only. Please configure the network architecture according to the actual situation and needs.

Chapter 3. Login to the device

This chapter describes how to configure the correct network settings for the network computers, how to log on to the appliances and how to use shortcut icons to quickly link to the GBR-4001 website for product information and services.

3.1 Configuring the correct network settings

Before logging to the device through the WEB interface, you must correctly configure the network computers in network settings.

First, connect your computer to the LAN port of the device, and then set the computer's IP address.

The first step is to set the computer's TCP/IP. If it has been set correctly, skip this step.

The second step is to set the computer's IP address. You can use either of the following methods:

1. Set the computer's IP address as one of the addresses from 192.168.1.2 - 192.168.1.254, the subnet mask is 255.255.255.0, and the default gateway is 192.168.1.1 (the LAN IP address of the device), and the DNS server is the address provided by the local operator.
2. Set the computer's TCP/IP as "Obtain an IP address automatically". After setting, the built-in DHCP server of the device will automatically assign IP addresses to computers.

The third step is to use the Ping command on your computer to check whether it is connected to the device. In **Start ->Operation**, type in **cmd**, and click <OK> to open the command window. Type in **ping 192.168.1.1**.

The following lists two kinds of results of executing the Ping command in the Windows XP environment:

If the screen is shown as follows, it indicates that the computer has been successfully and a connection is established on the device.

```
Pinging 192.168.1.1 with 32 bytes of data:
Reply from 192.168.1.1: bytes=32 time<1ms TTL=255
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
```

If the screen is shown as follows, it indicates that the connection between the computer and the device fails.

```
Pinging 192.168.1.1 with 32 bytes of data:
Request timed out.
Request timed out.
Request timed out.
Request timed out.
Ping statistics for 192.168.1.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),
```

When connection fails, please check the following items:

1. Hardware connections: The LEDs that correspond to the LAN port on the device panel and the PC network card LED must be on.
2. Configuring TCP/IP properties of the computer: If the LAN IP address of the device is 192.168.1.1, then the calculated IP address must be any one of the free addresses from 192.168.1.2 - 192.168.1.254.

3.2 Login to the device

When MS Windows, Macintosh, Unix or Linux operating systems are used on the PC, the device can be configured through browsers (such as Internet Explorer or Firefox).

Open the browser, and type in the IP address of the device's LAN port in the address bar, such as <http://192.168.1.1>. After the connection is established, you will see a login interface as shown in

Figure 3-1. In the first use, you should log in as a system administrator, that is, enter your administrator username and password (the factory values of username, password are Admin, case sensitive) on the login interface, and then click <OK>.



Figure 3_1 WEB login interface

If user name and password are correct, the browser will display the homepage of the WEB management interface, as shown in Figure 3-2. The top-right corner of the page displays device model, software version, hardware version and other information.

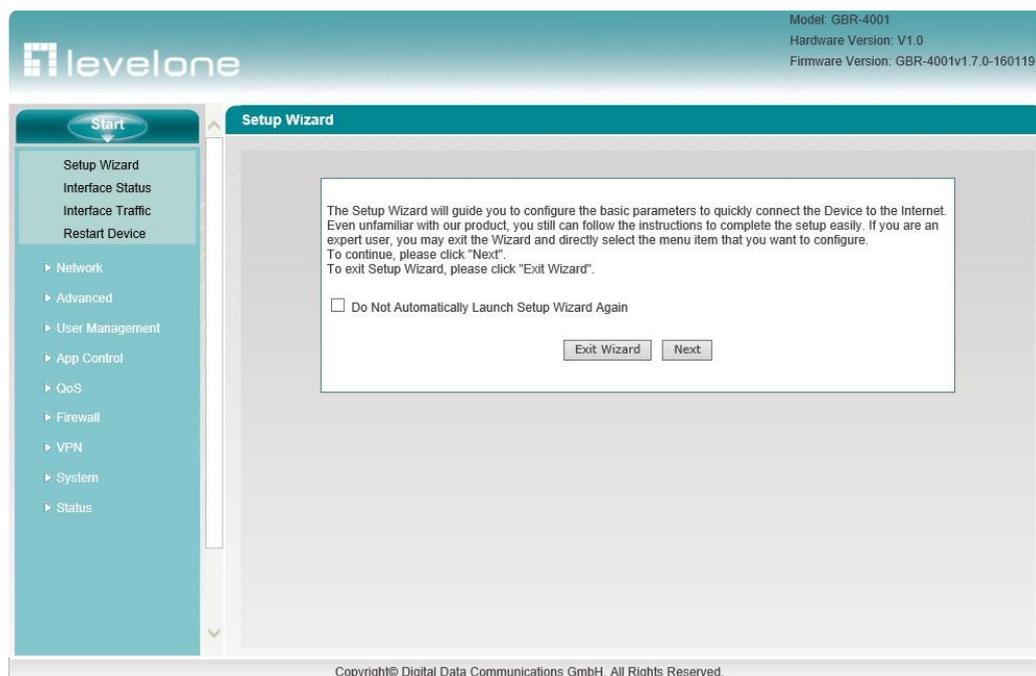


Figure 3_2 Homepage of the WEB interface

Homepage Description:

1. The top-right corner of the page displays device model, software version, hardware version and three fast link icons. These 3 shortcut icons have the following functions:
 - 1) **Product Discussion**– Link to the discussion forums of LEVELONE’s official website to participate in discussions about the product.
 - 2) **Knowledge Base**– Link to the knowledge base of LEVELONE’s official website for searching related technical information.
 - 3) **Booking Service**– Link to the booking service page of LEVELONE’s official website, for advance reservation of the customer service in a certain working period.
2. This page displays the main menu bar on the left.
3. The main operating page is located on the right of the page, in which you can configure various functions of the device, view the related configuration information and status information, etc.
4. If this is the first time for you to log in the device, the main operation page will be linked directly to the configuration wizard page. The next chapter describes how to configure the basic parameters required for the normal running of the device in the *Start -> Configuration wizard* page.

Chapter 4. Configuration Wizard

By reading this chapter, you can understand the basic network parameters required for the device to access to the Internet, and these parameters are configured to connect the device to the Internet. Before configuring "Internet Line" in the Configuration Wizard, you should properly configure the network settings of the network computer. For specific methods, see Chapter 3 Logging in the Device.

If this is the first time for you to log in the device, a configuration wizard homepage appears directly in the main operating page. As shown in Figure 4_1:



Figure 4_1 Home page of configuration wizard

- ◆ In logging next time, the wizard will no longer automatically pop up: When checking it, you can go directly to the *System Status* page in logging next time;
- ▶ Exit the wizard: Exits the Configuration Wizard and returns to the *System Status* page.
- ▶ Next step: Enter the *Selection of device access mode* page.

4.1 WAN1 Port Configuration - Dynamic IP access

Configure the second page of the wizard to configure the WAN1 port address of the device. The default WAN line access takes dynamic IP access, as shown in Figure 4-2. If your Internet access mode is dynamic IP access, please click <Finish>, to complete the configuration of the Internet line.

Here you can configure WAN1 connection as required.

Connection Type

Figure 4_2 Configuration Wizard - Dynamic IP access

4.2 WAN1 port configuration - Static IP access

If your Internet access mode is fixed IP access, please select " Static IP access" in the drop-down list box of Figure 4-3. The following describes the meaning of the parameters for configuration of fixed IP access.

Here you can configure WAN1 connection as required.

Connection Type

IP Address*

Subnet Mask*

Gateway IP*

Primary DNS Server*

Secondary DNS Server

Figure 4_3 Configuration Wizard - Static IP access

- ◆ IP address, subnet mask, gateway address, primary DNS server, secondary DNS server: Fill in the WAN IP address, subnet mask, gateway address and DNS server address that ISP (Such as China Telecom) offers you.

4.3 WAN1 configuration -- PPPoE access

If your Internet access mode is fixed IP access, please select "PPPoE access" in the drop-down list

box of Figure 4_4. The following describes the meaning of the parameters for PPPoE access.

The screenshot shows a configuration window titled "Here you can configure WAN1 connection as required." It contains a "Connection Type" dropdown menu set to "PPPoE". Below this are two text input fields: "User Name*" and "Password*", both with red asterisks indicating they are required. At the bottom of the window are four buttons: "Cancel", "Exit", "Finish", and "Help".

Figure 4_4 Configuration wizard - PPPoE access

- ◆ User name: Type in the user name the ISP provides you. If you have any questions, please ask your ISP.
- ◆ User name: Type in the password the ISP provides you. If you have any questions, please ask your ISP.

⊕ **Tip:**

1. After configuring the Internet line for the WAN1 port, please click < Finish >, this configuration will take effect.
2. For the multi-WAN device, if you need to configure more than one line for Internet access, go to *Network parameters->WAN port configuration* page to configure other Internet lines.

Chapter 5. Start menu

Start menu is located on the top of the Level 1 menu bar of the WEB interface, providing the interface for 4 common pages, including: configuration wizard, running status, Interface Traffic , device reboot. In the **Start** menu, you can quickly configure the basic parameters required by the device in working properly, view the information about the interfaces, and view the statistics data of the devices' real-time traffics.

5.1 Configuration Wizard

The **Start-> Configuration wizard** pages can help you to quickly configure the basic parameters required by some devices in working normally. For details, see Chapter 4 Configuration Wizard.

5.2 Interface status

This section describes the **Start-> Interface status** page, in which you can view the information about the device's interfaces. As shown in the interface in Figure 5_1, the connection type, connection status, IP address and other information about the interfaces can be viewed.

Interface	Connection Type	Status	IP Address	Subnet Mask	Gateway IP	MAC Address	Primary DN
LAN			192.168.1.1	255.255.255.0		00116bea6416	
WAN1	DHCP	Disconnected				00116bea6e27	
WAN2	DHCP	Connected	192.168.10.57	255.255.255.0	192.168.10.1	00116bea6e28	8.8.8
WAN3	DHCP	Disconnected				00116bea6e29	
WAN4	DHCP	Disconnected				00116bea6e2a	

Figure 5_1 Information about Interface status

5.3 Interface Traffic

This section describes the *Start-> Interface Traffic* page, as shown in Figure 5_2. You can view the average, maximum, sum and the current real-time rate for the relevant ports to receive and send data, and provide different units (kbit/s and KB/s) for them.

Tip:

If this page fails to display properly, please click the hyperlink "if it does not display properly, please install svgviewer" to have the svgviewer plug-in installed.



Figure 5_2 Interface Traffic

- ◆ WAN: WAN port of the device, click on the tab to view the dynamic figure of receiving, sending traffic.
- ◆ LAN: LAN port of the device, click on the tab to view the dynamic figure of receiving, sending traffic.
- ◆ Timeline: The x-coordinate in the flow chart. You can click on the timeline options (1x, 2x, 4x, 6x in the figure) in the figure to determine the display effect;
- ◆ Flowline: The y-ordinate in the flow chart. You can choose the display effects as needed (standardization, maximization as shown in the figure);
- ◆ Display: Provides two display effect options, solid effect and hollow effect;
- ◆ Color: It can be selected for display according to needs and preferences, such as red, blue,

black etc.

- ◆ Flip: Click the Flip bLeveloneon, and the colors can swap to receive and send data.

5.4 Restart Device

If you need to restart the device, just enter into the *Start-> Restart device* page to click <Restart>.



Figure 5_3 Restart device

- ⊕ **Tip:** Upon restarting, all users will be disconnected from the device.

Chapter 6. Network parameters

In the network parameter menu, you can configure the basic network parameters for the device, including WAN/LAN configuration, DHCP server, DDNS configuration, UPnP and WAN port number configuration.

6.1 Configuration of WAN port

This section focuses on the configuration interface and methods of *Network parameters* → *WAN configuration*. In this page, you can configure not only the line information, modify or delete the configured lines according to the actual needs, but also view the connection status of lines.

After completing the configuration of Internet line in *Configuration Wizard*, you can view the connection and configuration of the line in this page, or modify the configuration as needed.

6.1.1 Network interface configuration

This section describes how to configure Internet access lines. Internet connection types include: dynamic IP access, fixed IP access, PPPoE access.

Enter into the *Network parameters* → *WAN port configuration* pages, and the configuration interface is shown in Figure 6_1.

Internet Connection List 4/4

1/1 First Prev Next Last Goto Page Page Search

Interface	Connection Type	Status	IP Address	Subnet Mask	Gateway IP
WAN1	DHCP	Disconnected			
WAN2	DHCP	Connected 0Hours56Minute5Seconds	192.168.10.57	255.255.255.0	192.168.10.1
WAN3	DHCP	Disconnected			
WAN4	DHCP	Disconnected			

Delete Renew Release Refresh

Interface

Connection Type

ISP Policy

Advanced Options (MAC address, etc.)

Mode

MAC Address

Interface Mode

Save Cancel Help

Figure 6_1 Configuration of WAN port

1. Dynamic IP access

As shown in Figure 6_1, the following describes the meaning of the parameters for dynamic IP access.

- ◆ Interface: Selects the appropriate interface for the device.
- ◆ Access mode: Selects "Dynamic IP access" here.
- ◆ Operator policy: Selects the operator of the interface, with the options as follows: Operator policy, Telecom, China Unicom and China Mobile respectively.
- ◆ Working mode: options include NAT and routing mode.
 - NAT mode: Network address translation. The router working in this mode can convert the IP address of the Intranet (LAN side) to that of the external network (WAN side). The router works in this mode by default.
 - Routing mode: The router working in this mode will not NAT-convert the IP address for the Intranet (LAN side) to access to the external network (WAN side), and directly looks up the routing table for forwarding.

⊕ Tip:

Both NAT mode and routing mode can take effect to a single line.

- ◆ MAC address: The MAC address of the related interface, which usually requires no

modification.

- ◆ Interface mode: Sets the duplex mode and rate for interfaces. Options are: Auto (adaptive), 10M-FD (10M full duplex), 10M-HD (10M half duplex), 100M-FD (100M full duplex), 100M-HD (100M half duplex), 1000M-FD (1000M full duplex, supported by Gigabit devices). The default is Auto, which is usually not required to be modified, and if there is any compatibility issue, or the device used does not support auto negotiation function, then the type of Ethernet negotiation can be set up here.

⊕ **Tip:**

1. When configuring the line, users can select the appropriate operator through "Operator policy", and the system will generate a corresponding route based on the user's choice, you can easily achieve the goal that Telecom traffic flows on the Telecom routes while Unicom traffic flows on the Unicom routes.
2. Generally, it is not recommended to modify the MAC address of interfaces. However, in some cases, the operator binds the MAC of the device, which results in the failure of the new network device to dial up successfully, and at this time, the MAC address of the device needs to be modified as that of the original network device.

2. Static IP access

The screenshot shows a configuration window for Static IP access. The fields are as follows:

Interface	WAN1
Connection Type	Static IP
ISP Policy	ISP Policy
IP Address*	0.0.0.0
Subnet Mask*	0.0.0.0
Gateway IP*	0.0.0.0
Primary DNS Server*	0.0.0.0
Secondary DNS Server	0.0.0.0
Advanced Options (MAC address, etc.)	
Mode	NAT Mode
MAC Address	00116bea6e27
Interface Mode	Auto

Buttons: Save, Cancel, Help

Figure 6_2 Static IP access

The interface as shown in Figure 6_2 is the configuration interface for fixed IP access.

- ◆ IP address, subnet mask, gateway address: Static IP address, subnet mask and gateway address the operator provides to you.

- ◆ Primary DNS server, secondary DNS server: The DNS server address the operator provides to you.
- ◆ For the working mode in the advanced options, MAC address, interface mode, please refer to the configuration of dynamic access.

3. PPPoE access

The screenshot displays a configuration window for PPPoE access. The main configuration area includes the following fields:

- Interface: WAN1
- Connection Type: PPPoE
- ISP Policy: ISP Policy
- User Name*: (empty)
- Password*: (empty)
- PPP Authentication: EITHER
- Dial Type: Always On
- Dial Mode: Normal Mode
- Idle Timeout*: 0 Minutes
- MTU*: 1480 Byte (with a note: (MTU Range: 1-1492))

The 'Advanced Options' section (MAC address, etc.) contains:

- Mode: NAT Mode
- MAC Address: 00116bea6e27
- Interface Mode: Auto

At the bottom of the window are three buttons: Save, Cancel, and Help.

Figure 6_3 PPPoE access

The interface as shown in Figure 6_3 is the configuration interface for PPPoE access.

- ◆ Access mode: Here, PPPoE access, ADSL virtual dial-up (or PPPoE dial-up of Ethernet media) are selected, the device will obtain the IP address, subnet mask and gateway address information through dial-up.
- ◆ User name and password: The user name and password provided by the operator when it is conducting services.
- ◆ Password authentication mode: The way ISP uses to authenticate user names and passwords, which is EITHER by default. In most areas, PAP is used, and CHAP mode is also used in a few areas, NONE represents no username and password authentication is to be done, EITHER means to negotiate with the peer device automatically as to the specific authentication mode.
- ◆ Dial-up type:
 - Auto dial-up: Automatic dial-up connection after the device is powered on or the

previous dial-up disconnection occurs.

- Manual dial-up: Users may click related buttons below the "Line connection information list" of the *Network parameters* → *WAN configuration* to manually connect and hang up.
- On-demand dialing: The device will connect automatically when there is Internet traffic in the Intranet.
- ◆ Dial-up mode: Selects the PPPoE dial-up mode, which is normal mode by default. If the dial-up is not successful, try using other modes on the premise of using the correct user name and password.
- ◆ Idle time: The time length after there is no traffic of access and before automatic disconnection, 0 means no automatic disconnection (Unit: minutes).
- ◆ MTU: Maximum transmission unit, whose default value is 1480 bytes. The device will automatically negotiate with the peer device. Do not modify it unless in special applications.
- ◆ For the working mode in the advanced options, MAC address, interface mode, please refer to the configuration of dynamic access.

6.1.2 Internet Connection List

In the "Internet Connection List", you can view the configuration and status information for the lines, as shown in Figure 6_4, Figure 6_5.

Internet Connection List							4/4			
1/1	First	Prev	Next	Last	Goto	Page	<input type="text"/>	Page	Search	<input type="text"/>
Interface	Connection Type	Status		IP Address	Subnet Mask	Gateway IP	Ro			
WAN1	PPPoE	Connected 0Hours23Minute31Seconds		118.166.197.63	255.255.255.255	168.95.98.254				
WAN2	DHCP	Connected 17Hours19Minute0Seconds		192.168.10.57	255.255.255.0	192.168.10.1				
WAN3	Static IP	Connected		111.111.111.12	255.255.255.0	111.111.111.1				
WAN4	DHCP	Disconnected								

Figure 6_4 Internet Connection List

Internet Connection List								4/4
1/1	First	Prev	Next	Last	Goto	Page	Page	Search
Status	IP Address	Subnet Mask	Gateway IP	Rx Rate(KB/s)	Tx Rate(KB/s)	Edit		
Connected 0Hours23Minute31Seconds	118.166.197.63	255.255.255.255	168.95.98.254	1	2			
Connected 17Hours19Minute0Seconds	192.168.10.57	255.255.255.0	192.168.10.1	9	4			
Connected	111.111.111.12	255.255.255.0	111.111.111.1	0	0			
Disconnected				0	0			

Figure 6_5 Internet Connection List information (Continued Figure 6_4)

- ◆ Interface: This column displays the WAN port of the device.
- ◆ Connection type: The connection type of the current Internet access lines, including fixed access, dynamic access, PPPoE access.
- ◆ Connection status: The current connection status of the lines. It is displayed as "Off" when the connection is not successful or is not available, and displayed as "Connected" when the connection is successful; for dynamic IP access and PPPoE access, it also displays the time (Unit: hours: minutes: seconds) to maintain the connection when the connection is successful.
- ◆ IP address, subnet mask, gateway address: IP address, subnet mask, and gateway address for the WAN interface provided by ISP.
- ◆ Downstream rate, upstream rate: The downlink/uplink average rate of the current line in the time interval of two times of list refreshing. The unit is KB/s.

1. Dial-up and hang-up of PPPoE accesslines

If a line is PPPoE access, then click on the interface, the "Dial-up" and "Hang-up" buttons will appear below the "Line connection information list", as shown in Figure 6_6, the WAN3 interface is PPPoE access, click on "WAN3", the following four buttons are displayed on the lower right part of the line connection information list, and their functions are as follows:

- ▶ Delete: Delete this line.
- ▶ Dial-up: Establishes a connection with the PPPoE server. When the PPPoE connection dial-up type is set to "Manual dial-up", and the PPPoE dial-up is required here.
- ▶ Hang-up: Hangs up the current connection to the PPPoE server.
- ▶ Refresh: Click this button to display the up-to-date information of line connection information list.

Internet Connection List							4/4	
1/1	First	Prev	Next	Last	Goto	Page	Page	Search
Interface	Connection Type	Status		IP Address	Subnet Mask	Gateway IP	Rs	
WAN1	PPPoE	Connected 0Hours23Minute31Seconds		118.166.197.63	255.255.255.255	168.95.98.254		
WAN2	DHCP	Connected 17Hours19Minute0Seconds		192.168.10.57	255.255.255.0	192.168.10.1		
WAN3	Static IP	Connected		111.111.111.12	255.255.255.0	111.111.111.1		
WAN4	DHCP	Disconnected						

Figure 6_6 Internet Connection List - PPPoE access

2. Update and release of dynamic IP accesslines

If a line is a dynamic IP access line, then click on the interface, the "Update" and "Release" buttons are displayed below the "Line connection information list", as shown in Figure 6_7.

Internet Connection List							4/4	
1/1	First	Prev	Next	Last	Goto	Page	Page	Search
Interface	Connection Type	Status		IP Address	Subnet Mask	Gateway IP	Rs	
WAN1	PPPoE	Connected 0Hours23Minute31Seconds		118.166.197.63	255.255.255.255	168.95.98.254		
WAN2	DHCP	Connected 17Hours19Minute0Seconds		192.168.10.57	255.255.255.0	192.168.10.1		
WAN3	Static IP	Connected		111.111.111.12	255.255.255.0	111.111.111.1		
WAN4	DHCP	Disconnected						

Figure 6_7 Internet Connection List - Dynamic IP access

- ▶ Update: The system automatically complete the process of releasing the IP address, and then obtaining an IP address again.
- ▶ Release: Releases the currently obtained dynamic IP address.

6.2 Line combination

This section describes the *Network parameter -> Line combination* page.

In the line combination configuration, you can quickly configure line combination modes, and other related parameters, and specify the detection interval, detection number, detection target IP address and bandwidth of the lines.

6.2.1 Description of line combination function

1. Line detection mechanism

Regardless of line combination modes, make sure that the network is not interrupted when the line fails, which require that the device must be able to monitor line status in real time. To this end, we designed a flexible automatic detection mechanism, and provide a variety of line detection methods for users to choose, in order to meet the practical application needs.

To facilitate understanding, several related parameters are introduced first.

Detection interval: the time interval of sending inspection packets. One inspection packet is sent per time, and the default value is 0 seconds. In particular, when the value is 0, it means not to make line detection.

Detection times: The number of inspection packets sent within each detection cycle.

Destination IP address: The object of detection. The device will send inspection packets to the pre-designated target to detect if the line is normal.

The following is an introduction of the device's line detection mechanism in two cases: line normal and line failure.

When a line fails, the detection mechanism is described as follows: The device will send an inspection packet to the detection target of the line at the specified detection interval. If all the inspection packets sent have no response within a detection cycle, this line will be deemed to be failed, and it will be shielded immediately. For example, if the 3 inspection packets that are sent have no response within a detection cycle, the line is deemed to be failed by default.

When a line is normal, the detection mechanism is described as follows: Similarly, the device will send an inspection packet to the detection target of the line at the specified detection interval. If half of the inspection packets or above sent have response within a detection cycle, this line will be deemed to be normal, and it will be restored. For example, if the 3 inspection packets that are sent have response within a detection cycle, the line is deemed to be restored by default.

The device allows users to specify Internet lines for some hosts in the Intranet in advance, which is realized by setting the "Internal starting IP address" and "Internal end IP address" of the line, and the hosts whose IP addresses are within two address ranges will give priority to the use of the specified line. For the hosts with the specified Internet line, they can only access to the Internet through that line when the specified line is normal. However, when the specified line fails, they will use other normal lines for Internet access.

 **Tip:**Line detection is not enabled, then the "Detection interval" should be set to "0" second.

2. Line combination mode

The device provides 2 line groups: "Main line" group and "Backup line" group. For convenience's sake, the lines in the "main line" group are collectively known as main line, and the lines in the

"backup line" group are collectively known as backup line. All lines are main lines by default. Users can divide some lines into the "Backup line" group as needed.

The device provides two line combination modes, "All line load balancing" and "Partial line load balancing while the other backed up".

In the "All line load balancing" mode, all lines are used as main lines. Working principles are as follows:

1. When all lines are normal, the Intranet hosts can use all lines for Internet access simultaneously.
2. If a line fails, it should be shielded immediately, and the flow originally passing through the line will be allocated to the other lines.
3. Once the fault line is restored to normal, the device will enable this line automatically, and the flow is automatically redistributed.

In the "Partial line load balancing while the others backed up" mode, part of the lines are used as main lines, the other part of the lines is used as backup lines. Working principles are as follows:

1. As long as the main line is normal, the Intranet hosts use main lines for Internet access.
2. If the main line fails, it will automatically switch to using the backup line for Internet access.
3. Once the fault lines are restored to normal once, they will be immediately switched back to the main line.

 **Tip:**

When a line is interrupted for line switching, some user applications (such as part of network games) may be unexpectedly interrupted. This is determined by the TCP session property.

6.2.2 Global Settings

In these two line combination modes, "All line load balancing" and "Partial line load balancing while the others backed up", the interface of global setting is different; therefore, their universal setting parameters are described below respectively.

1. Full Load Balancing



Figure 6_8 Full Load Balancing

- ◆ Line load balancing mode: " Full Load Balancing " is selected here.
- ▶ Save: The line combination configuration parameters take effect.
- ▶ Refill: Restores to the configuration parameters before modification.
- ⊕ **Tip:** Line combination mode is " Full Load Balancing " by default.

2. Partial Load Balancing

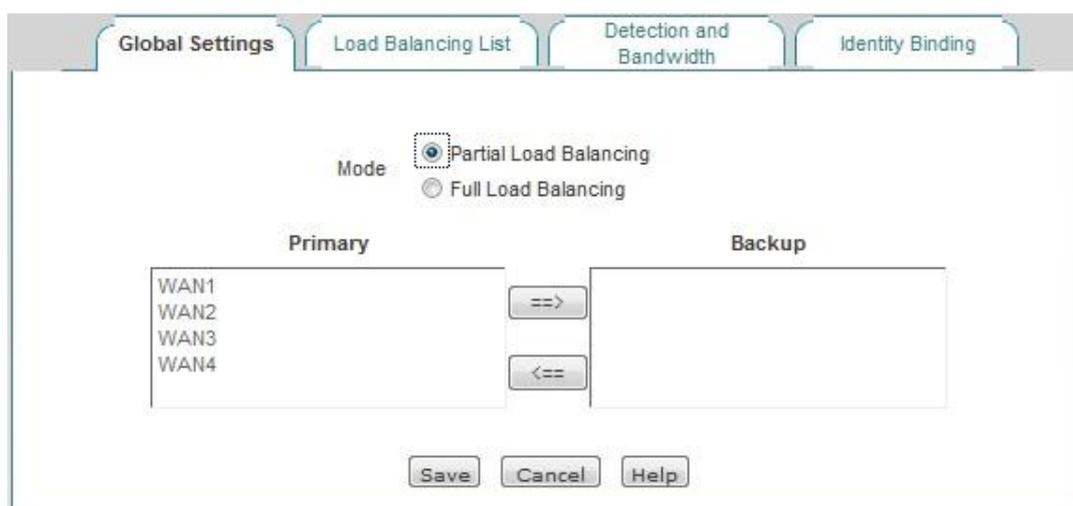


Figure 6_9 Partial Load Balancing

- ◆ Line combination mode: " Partial Load Balancing " is selected here.
- ◆ Main line: The list box represents the "main line" group, and all the lines in the list box are used as the main lines.
- ◆ Main line: The list box represents the "Backup line" group, and all the lines in the list box are used as the backup lines.
- ◆ ==> (Right arrow), <== (Left arrow): Select one (or more) line in the "Main line" list box first, and then click on "==>", and the selected lines are immediately moved to the "Backup line" list box. Similarly, select one (or more) line in the "Backup line" list box first, and then click on "<==", and the selected lines are immediately moved to the "Main line" list box.

- ▶ Save: The line combination configuration parameters take effect.
- ▶ Refill: Restores to the configuration parameters before modification.

6.2.3 Load Balancing List

In the *Network parameter* -> *Load Balancing* -> *Load Balancing List* page, you can view the information of configuration line.

Interface	Connection Type	Bandwidth	Status	IP Address	Detection Interval	Retry Times	Detection Target
WAN1	PPPoE	0k bit/s	Connected	118.166.197.63	0	10	Gateway IP Address
WAN2	DHCP	0k bit/s	Connected	192.168.10.57	0	10	Gateway IP Address
WAN3	Static IP	0k bit/s	Connected	111.111.111.12	0	10	Gateway IP Address
WAN4	DHCP	0k bit/s	Disconnected		0	10	Gateway IP Address

Figure 6_10 Load Balancing List

- ▶ Edit the line combination status information: Click on the interface of the line or the "Edit" hyperlink corresponding to the line, to skip to the relevant page for change,
- ▶ Refresh: Click <Refresh>, to get the latest status information of line combination.

6.2.4 Detection and Bandwidth

After configuring the line combination function, you also need to configure the detection mechanism of the lines, and the configuration methods are as follows.

Enter the *Network parameters* -> *Load Balancing* -> *Detection and Bandwidth* page, or enter the *Line combination status information list* line interface or edit the icon, enter the *Detection and bandwidth distribution* page.

Figure 6_11 Detection and Bandwidth

- ◆ Detection interval: The time interval for sending inspection packets, Unit: seconds, when you enable line detection, the value range is 1-60 (the value is 0, which means not to enable the line detection).
- ◆ Detection times: The number of inspection packets sent within the detection cycle (one detection packet is sent per time). The default value is 10.
- ◆ Detection Target IP address: The IP address of the target to be detected.
- ◆ Bandwidth: Sets the bandwidth ISP provides to the current line, and the Max custom value of the Gigabit device is set to 1000M.
- ◆ Internal starting and ending IP address: The address range of the hosts on the current line is to be used in priority in Intranet.
- ▶ Save: The above configuration parameters take effect.
- ▶ Refill: Restores to the configuration parameters before modification.
- ▶ Return: Returns to the line combination state information page.

6.2.5 Identity Binding

When the device has multiple WAN ports, you can enter the *Network parameters* -> *Load Balancing* -> *Identity Binding* page to enable the identity binding function.

In the case of multi-line session load balancing, NAT sessions in the same application may be distributed in different lines, which will cause such applications as online bank, QQ, etc. not to work properly due to change of identity, and the identity binding function can address this issue by binding the sessions in the same application from the same user on a line. For example, when a user in the Intranet logs in the online bank, if the first session is assigned to WAN2 port

connection line, all the online banking sessions of this user will go out from the WAN2 port until the user logs out.



Figure 6_12 Enabling identity binding

- ◆ Enable identity binding: Enables/disables the identity binding function. If multiple lines are configured, please enable the device's identity binding function to make normal use of such apps as QQ, online bank.

6.3 Configuration of LAN port

The device's LAN ports can be configured with 4 IP addresses, and the first default IP address of the LAN port is 192.168.1.1. If you need to change the LAN IP address in order to adapt to the existing network, enter the *Network parameters > LAN port configuration* page for configuration.

Figure 6_13 Configuration of LAN port

- ◆ IP address: Sets the LAN IP addresses, and the first IP address is 192.168.1.1 by default, while the other three IP addresses are 0.0.0.0 by default.
- ◆ Subnet mask: Sets the subnet mask of the corresponding IP address, which is 255.255.255.0 by default.
- ◆ MAC address: The MAC address of the LAN port. It is suggested not to modify the MAC address of the LAN port freely.
- ◆ Interface mode: Sets the duplex mode and rate for interfaces. Options are: Auto (adaptive), 10M-FD (10M full duplex), 10M-HD (10M half duplex), 100M-FD (100M full duplex), 100M-HD (100M half duplex), 1000M-FD (1000M full duplex, supported by Gigabit devices). The default is Auto, which is usually not required to be modified, and if there is any compatibility issue, or the device used does not support auto negotiation function, then the type of Ethernet negotiation can be set up here.

⊕ **Tip:**

After modifying the LAN IP address, you must use a new IP address to log into the device, and the IP for logging into the host must be on the same network segment!

6.4 DHCP server

This section mainly introduces the *Network parameters* -> *DHCP server* page, including DHCP server settings, static DHCP and DHCP automatic binding and DHCP client list.

6.4.1 DHCP server configuration

Below is a description of the parameters for configuring the DHCP server functions.

DHCP Server Settings | Static DHCP | DHCP Auto Binding | DHCP Client List

Enable DHCP Server

To make DHCP server settings take effect, select the check box to enable DHCP server.

Start IP Address * 192.168.1.100

End IP Address * 192.168.1.200

Subnet Mask * 255.255.255.0

Gateway IP * 192.168.1.1

Lease Time * 3600 Seconds

Primary DNS Server * 192.168.1.1

Secondary DNS Server 0.0.0.0

Enable DNS Proxy

To make DNS proxy settings take effect, select the check box to enable DNS proxy.

ISP DNS Server 1 0.0.0.0

ISP DNS Server 2 0.0.0.0

Save Cancel Help

Figure 6_14 Configuration of DHCP service

- ◆ Enable DHCP server: Used to disable or enable the device's DHCP server function. Selecting it means allow.
- ◆ Start and end IP address: The IP address fields the DHCP server assigns to the network computer automatically (which should be on the same network segment as the IP address of the device LAN port).
- ◆ Subnet mask: The subnet mask automatically assigned by the DHCP server to the network computer (which should be consistent with that of the LAN port of the device).
- ◆ Gateway address: The gateway IP address the DHCP server automatically assigns to the network computer (which should be consistent with the LAN IP address of the device).
- ◆ Leasing time: The leasing time for the network computers to obtain the IP address assigned by the device (Unit: Seconds).
- ◆ Primary DHCP server: The IP address of the primary DNS server automatically assigned by the DHCP server to the network computers.
- ◆ Secondary DNS server: The IP address of the secondary DNS server assigned by the DHCP server to the network computers automatically.
- ◆ Enable DNS proxy: Selecting it means enabled. The DNS proxy function of the device will not take effect unless enabled. After enabling this function, the gateway address is assigned to

a client as primary, secondary DNS servers.

◆ Operator DNS servers 1, 2: The IP address of operator DNS server.

⊕ **Tip:**

1. If the device's DHCP server function is to be used, network computer's TCP/IP protocol can be set to "obtain an IP address automatically".
2. If what's originally used by the user is a proxy server software (such as Wingate), and the PC's DNS server is set as the IP address of the proxy server, then the LAN IP address of the device only needs to be set to the same IP address, so that the user can switch to using the device's DNS proxy function without having to change the PC setting after the device enables the DNS proxy function.

6.4.2 Static DHCP

This section describes the static DHCP list and the way to configure a static DHCP.

Using the DHCP service to automatically configure TCP/IP properties for the network computers is very convenient, but it can cause a computer to be assigned with different IP address at different times. And some Intranet computers may need a fixed IP address, in this case, the static DHCP function is required, to bind the computer's MAC address with an IP address, as shown in Figure 6_15. When a computer having this MAC address requests the address from the DHCP server (device), the device will find a corresponding fixed IP address based on its MAC address and assign it to the computer.

1. Static DHCP list

User Name	IP Address	MAC Address	Edit

Figure 6_15 Static DHCP list

2. Static DHCP configuration

Click <Add new entry> in the page as shown in Figure 6_15, to enter into the *Static DHCP configuration* page as shown in the figure below. Below is a description of the meaning of the parameters for configuring static DHCP.

User Name *

IP Address *

MAC Address *

Static DHCP, i.e., DHCP manual binding, allows you to manually bind an IP address to a PC's MAC address and thus that PC will always obtain the same IP address from the DHCP server.

Figure 6_16 Static DHCP configuration

- ◆ User name: Configures the user name of the computer bound by this DHCP (custom, no repeat is allowed).
- ◆ IP address: The reserved IP address, which must be the valid IP address within the address range specified by the DHCP server.
- ◆ MAC address: The MAC address of the computer to use this reserved IP address in a fixed way.

⊕ **Tip:**

1. After the setting is successful, the device will assign the preset IP address for the specified computer in a fixed way.
2. The assigned IP addresses must be within the range provided by the DHCP server.

6.4.3 DHCP auto binding

Below is the description of DHCP automatic binding function.



Figure 6_17 DHCP auto binding

- ◆ **Enable DHCP automatic binding:** When DHCP automatic binding is enabled, the device will scan the Intranet, and bind IP/MAC of intranet users who obtain an IP address dynamically, and the device will bind any one IP address it assigns subsequently with the MAC address of the client. Enabling this function can protect against network ARP spoofing. If it is not enabled, no automatic binding operation is to be done.
- ◆ **Enable DHCP automatic deletion:** When DHCP automatic deletion is enabled, it means that the device will automatically delete the IP/MAC previously bound automatically after the lease expires or the user releases the address actively; if it is not enabled, it means that no automatic deleting operation is to be done.

6.4.4 DHCP client list

For the IP address already assigned to the network computer, its information can be viewed in the DHCP client list. Information as shown in the figure below: The DHCP server assigns the IP address of 192.168.1.100 in the address pool to the network computers whose MAC address is 6C:62:6D:E9:6D:13, and the rest of the time for the computer to lease this IP address is 86333 seconds.

IP Address	Subnet Mask	MAC Address	Lease Remaining
192.168.1.101	255.255.255.0	50:3F:56:00:04:70	3070S
192.168.1.100	255.255.255.0	00:1B:24:A3:42:5C	2950S

Figure 6_18 DHCP client list

6.4.5 Case of DHCP configuration

Application requirements

In this example, the device must have the DHCP function enabled, and the starting address is 192.168.1.10, with a total number of 100 allocable addresses. The host with the MAC address of 00:21:85:9B:45:46 assigns the fixed IP address of 192.168.1.15, while the host with the MAC address of 00:1F:3C:0f:07:F4 assigns the fixed IP address of 192.168.1.10.

Configuration steps

The first step is to enter into the *Network parameters* -> *DHCP server* -> *DHCP service settings* page.

The third step is to enable the DHCP function, configure the related DHCP service parameters (as shown in Figure 6_19), and click <Save> after the end of configuration.

DHCP Server Settings

Static DHCP DHCP Auto Binding DHCP Client List

Enable DHCP Server

To make DHCP server settings take effect, select the check box to enable DHCP server.

Start IP Address * 192.168.1.100

End IP Address * 192.168.1.200

Subnet Mask * 255.255.255.0

Gateway IP * 192.168.1.1

Lease Time * 3600 Seconds

Primary DNS Server * 192.168.1.1

Secondary DNS Server 0.0.0.0

Enable DNS Proxy

To make DNS proxy settings take effect, select the check box to enable DNS proxy.

ISP DNS Server 1 0.0.0.0

ISP DNS Server 2 0.0.0.0

Save Cancel Help

Figure 6_19 DHCP service settings - Instance

The third step is to enter the *Network parameters -> DHCP server-> Static DHCP* page, and click <Add new entry>, to configure the two static DHCP instances in the request (such as Figure 6_20, Figure 6_21).

User Name * A

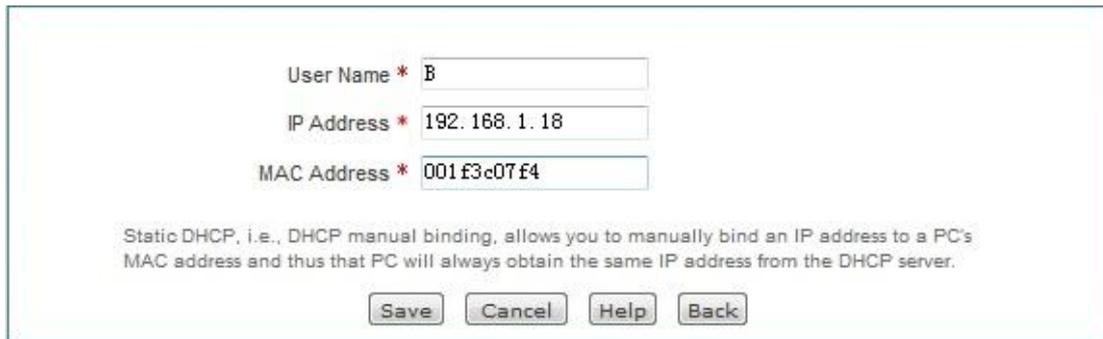
IP Address * 192.168.1.15

MAC Address * 6c826de145df

Static DHCP, i.e., DHCP manual binding, allows you to manually bind an IP address to a PC's MAC address and thus that PC will always obtain the same IP address from the DHCP server.

Save Cancel Help Back

Figure 6_20 Static DHCP configuration - Instance A



User Name * B

IP Address * 192.168.1.18

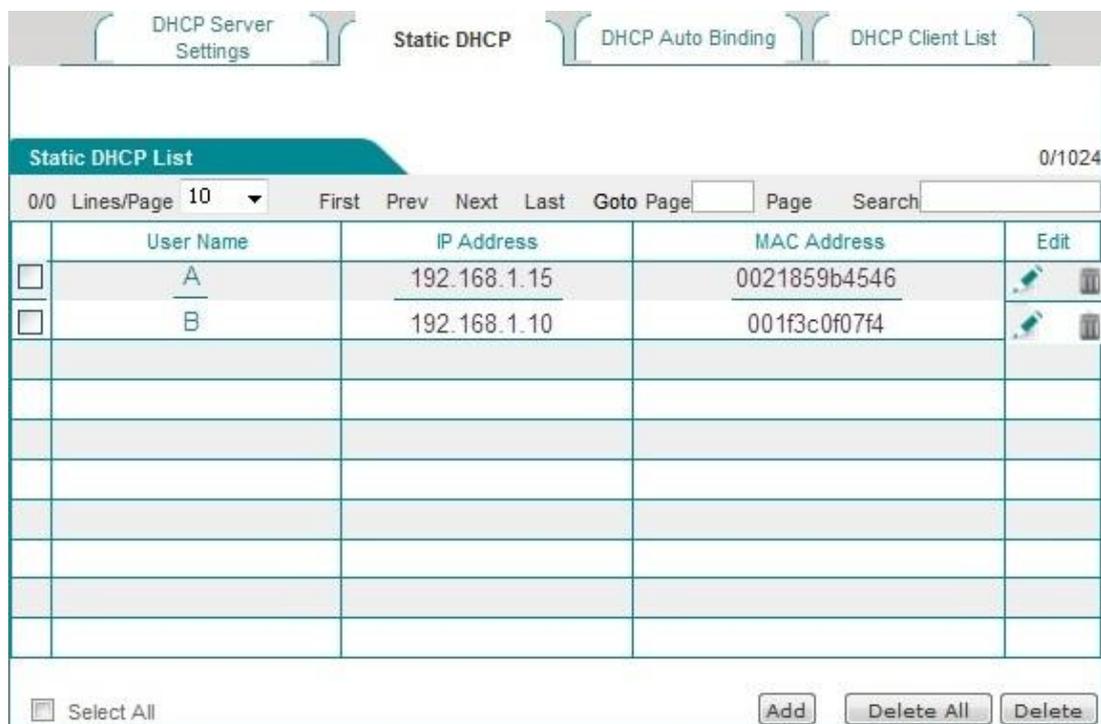
MAC Address * 001f3c07f4

Static DHCP, i.e., DHCP manual binding, allows you to manually bind an IP address to a PC's MAC address and thus that PC will always obtain the same IP address from the DHCP server.

Save Cancel Help Back

Figure 6_21 Static DHCP configuration - Instance B

At this point, the configuration is complete, and you can view the information about 2 static DHCP entries in the "Static DHCP information list", as shown in Figure 6_22. If configuration errors are found, you can click the corresponding item's  icon directly and enter into the *Static DHCP configuration* page for modification and saving.



Navigation: DHCP Server Settings | Static DHCP | DHCP Auto Binding | DHCP Client List

Static DHCP List 0/1024

0/0 Lines/Page 10 First Prev Next Last Goto Page Page Search

	User Name	IP Address	MAC Address	Edit
<input type="checkbox"/>	A	192.168.1.15	0021859b4546	 
<input type="checkbox"/>	B	192.168.1.10	001f3c0f07f4	 

Select All Add Delete All Delete

Figure 6_22 Static DHCP information list - Instance

6.5 DDNS Settings

This section describes the *Network parameters -> DDNS Settings* page and configuration methods. Includes: application for DDNS account, configuration of DDNS service, DDNS authentication.

Dynamic DNS (DDNS) is a service to resolve a fixed domain name to a dynamic IP address (such as ADSL dial-up Internet access) services. You need to apply to the DDNS service provider for this service, and the specific service of DDNS is provided by various service providers according to the actual situation. The DDNS service provider reserves the rights to change, interrupt or terminate part or all of the network services. At present, the DDNS service is free of charge, when the DDNS service provider may charge some fee for using DDNS services in providing network services. In this case, LEVELONE will give a notice as soon as possible. If you refuse to pay such expenses, you cannot use the related services. At the free stage, LEVELONE does not guarantee the DDNS service must be able to meet the requirements, nor guarantee the service will not be uninterrupted, nor guarantee the timeliness, safety, and accuracy of network services.

◆ Interface: Selects the interface binding of the DDNS service.

6.5.1 DDNS authentication

You can use the Ping command (for example: ping avery12345.3322.org) in the DOS status of intranet computers, to check if the DDNS update is successful. Upon seeing the correctly parsed-out IP address (for example: 58.246.187.126), it indicates that domain name resolution is correct. Note: Under normal circumstances, the device's IP address will not be pinged from the Internet after NAT is used on the device but only the IP address for that domain name can be parsed out.

```
Pinging avery12345.3322.org [58.246.187.126] with 32 bytes of data:
```

```
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63  
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63  
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63  
Reply from 58.246.187.126: bytes=32 time=1ms TTL=63
```

```
Ping statistics for 58.246.187.126:
```

```
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

```
Approximate round trip times in milli-seconds:
```

```
    Minimum = 1ms, Maximum = 1ms, Average = 1ms
```

1. Only when the IP address assigned by ISP (Such as China Telecom) to the WAN port connection line can the domain name be sure to be accessed by Internet users.
2. The DDNS function can help the Dynamic IP use VPN and server mapping.

6.6 UPnP

Universal Plug and Play (UPnP) is an architecture for common peer network connections used for PCs and intelligent devices (or instruments). Using UPnP means simpler, more choices and more innovative experiences. The network products supporting Universal Plug and Play needs only be physically connected to the network, to begin to work.

This section describes the *Network parameters ->UpnP* page and configuration. When configuring UPnP in this page, you need to simply enable or disable this feature.

Enable UPnP

UPnP Port Forwarding List
0/0

0/0 Lines/Page 10 ▼
First Prev Next Last Goto Page Page Search

ID	Internal IP	Internal Port	Protocol	Remote IP	External Port	Description

Figure 6_23 UPnP configuration

- ◆ Enable UPnP: Ticking the check box for enabling the UPnP feature.
 - ◆ Internal address: The host IP address when port translation is needed in the intranet.
 - ◆ Internal port: The port number provided by the host when port translation is required in the intranet.
 - ◆ Protocol: The protocol used by the UPnP port in translation (TCP/UDP).
 - ◆ Peer address: The IP address of the peer host.
 - ◆ External ports: The port number of the device used for port translation. This port is the service port the device provides to the Internet.
 - ◆ Description: The description information given when an application requests port translation to the device through UPnP.
- ⊕ **Tip:** It is recommended not to enable the UPnP feature when this feature is not in use.

Chapter 7. Advanced Configuration

The features described in this chapter include: NAT and DMZ, route configuration, network vanguard defense, port mirroring, port VLAN and SYSLOG configuration.

7.1 NAT and DMZ configuration

This section describes the features and configuration methods of the *Advanced Configuration->NAT and DMZ configuration* page.

7.1.1 Description of NAT functions

NAT (network address translation) is a technology to map an IP address field (such as Intranet) to another IP address field (such as the Internet). NAT was designed to solve the problem of increasing shortage of IP addresses, NAT allows a private network to use the IP address in any range internally, and for the public Internet, it is reflected as limited range of public network IP addresses. Since the internal network can be effectively isolated from the outside world, so NAT can also provide some assurance for network security.

LEVELONE routing products provide flexible NAT function. The following will detail its characteristics.

1. NAT address space

In order to correctly conduct the NAT operation, any NAT device must maintain two address spaces: one is the private IP addresses used internally by Intranet hosts, which is represented by "Internal IP address" in the device. Another is the public network IP address for external use, which is represented by "External IP address" in the device.

2. NAT Static mapping and virtual server (DMZ host)

After the NAT feature is enabled, the device blocks the access requests that originate outside. However, in certain application environments, a computer in the external network hopes to access to the Intranet server through the device, at this point, the static NAT mapping or virtual server

(DMZ host) needs to be set up on the device in order to achieve this objective.

With the static NAT mapping function, a one-to-one mapping relationship can be established between **<External IP address + External port>** and **<Internal IP address + Internal port>**, so that all the service requests for a specified port of the device will be forwarded to the matching intranet server, and the computer in the external network can access to the services provided by this server.

In some cases, a network computer needs to be fully exposed to the Internet, in order to achieve two-way communications, and at this time, you will need to set up this computer to a virtual server (DMZ host). When an external user accesses to the public network address that is mapped to the virtual server, the device will forward the packets directly to the virtual server.

 **Tip:** The computer that is set to a virtual server will lose the firewall protection of the device.

The priority of NAT static mappings is higher than the virtual server. When the device receives a request from an external network, it will first check to see if there is a matching NAT static mapping based on the IP address and port number of the external access requests, and send the request messages matching the static NAT mapping to the Intranet computers if any. If there are no matching static mappings, it will check to see if there is a matching virtual server.

3. Two types of NAT rules

The device provides two NAT types: "Easy IP" and "One2One".

Easy IP: The translation of network port addresses. Multiple internal IP addresses are mapped to the same external IP address. It can dynamically assign a port associated with a single external address for each internal connection, and maintain the mapping of these internal connections to an external port, thus enabling multiple users to use a public network address to communicate with the external Internet.

One2One: The translation of static addresses. The internal IP and the external IP address are subject to one-to-one mapping. In this mode, the port number will not change. It is typically used to configure the extranet-access-to-intranet server: The network servers still use private addresses, and provide the public IP address assigned to it to the external network users.

We refer to each specific NAT configuration as "NAT rules". The exit IP address and lines must be specified when configuring the NAT rules. When there are multiple valid public network addresses, each type of NAT rules can be configured with more than one. In practical application, a mixture of different types of NAT rules often needs to be used.

7.1.2 Port Forwarding

This section describes the static NAT mapping functions of the device. Below is the description of the meaning of the parameters for the static NAT mapping list and the static NAT mapping configuration.

Figure 7_2 Port Forwarding Settings

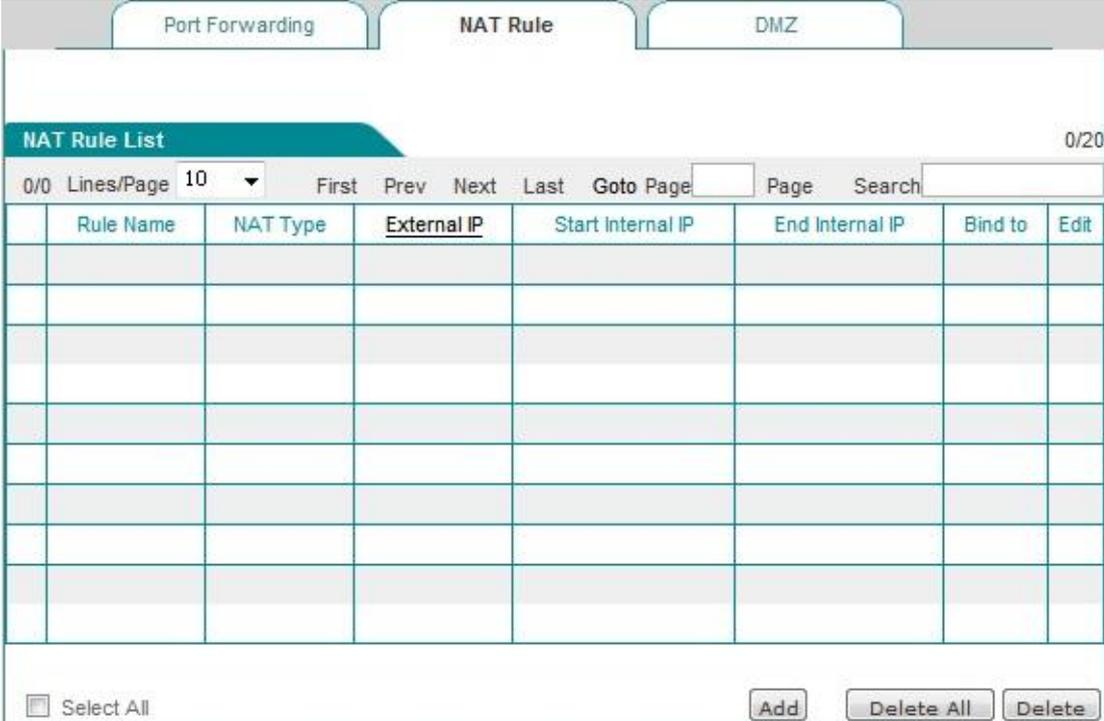
- ◆ Static mapping name: The name of static NAT mapping, which is custom and cannot be repeated.
- ◆ Enable this configuration: Selecting it indicates that the static NAT mapping takes effect, and not selecting it means that the static NAT mapping does not take effect, but retains its configuration.
- ◆ Protocol: The protocol type of packets, the available options are: TCP, UDP and TCP/UDP. When you are unable to confirm that the protocol used by the application is TCP or UDP, select TCP/UDP.
- ◆ External starting port: The starting service port the device provides to the Internet.
- ◆ IP address: The IP address of the computer as a server in the Intranet.
- ◆ Common port: The port number that corresponds to the common protocol type for users' choice. When you are unable to confirm the protocol, select TCP/UDP.
- ◆ Internal starting port: The starting port of the services enabled by the network server.
- ◆ Number of ports: A segment of ports starting from the internal starting port, whose maximum value is set to 500.
- ◆ NAT binding: Selects the interface bound by the static NAT mapping.

7.1.3 NAT rules

The NAT rules features of the device are described below, including: NAT rule info lists, meaning of Easy IP NAT rules configuration parameters, meaning of One2One NAT rules configuration parameters.

1. List of NAT rules information

In NAT rules information list, you can see the configured NAT rules. As shown in Figure 7_3, it has two NAT rules instances configured. The NAT type of an instance: EasyIP converts the address with the intranet IP address of 192.168.1.20-192.168.1.25 to 200.200.202.20, and binds to the WAN1 port to achieve Internet access. The NAT type of an instance: One2One converts the address with the intranet IP address of 192.168.1.50-192.168.1.52 to 200.200.202.50, 200.200.202.51, 200.200.202.52, and binds to the WAN1 port to achieve Internet access.



NAT Rule List							
Rule Name	NAT Type	External IP	Start Internal IP	End Internal IP	Bind to	Edit	

Figure 7_3 List of NAT rules information

Tip: Multiple NAT rules are configured for the same object, and the rules configured last will take effect first.

2. Easy IP

Click <Add new entry> in Figure 7_3 to enter the NAT rules configuration page. The following describes the meaning of the parameters for configuring the NAT rules with the type of EasyIP.

Rule Name *

NAT Type EasyIP

Multiple internal IP addresses are mapped to a single external IP address.

External IP *

Start Internal IP *

End Internal IP *

Bind to WAN1

Save Cancel Help Back

Figure 7_4 Easy IP

- ◆ Rule name: Customizes the name of the NAT rule.
- ◆ NAT type: Selects EasyIP here, which means the internal IP address are mapped to the same external IP address.
- ◆ External IP address: In the NAT rule, the external IP address mapped to the internal IP address.
- ◆ Internal starting IP address, internal ending IP address: The IP address range for the computers in the intranet that have the priority to use the NAT rules for Internet access.
- ◆ Binding: Selects the interface bound by the static NAT mapping.

3. One2One

Select the NAT type as One2One in Figure 7_5. The meaning of the parameters for configuring the NAT rules as One2One type is described here, and those parameters same as EasyIP are repeated no longer here.

Rule Name *

NAT Type One2One

One internal IP address is mapped to one external IP address.

Start External IP *

Start Internal IP *

End Internal IP *

Bind to WAN1

Save Cancel Help Back

Figure 7_5 One2One

- ◆ NAT type: Here, One2One is selected. The internal IP address and the external IP address are

subject to one-to-one mapping.

◆ External starting IP address: In the NAT rule, the external starting IP address mapped to the internal starting IP address.

⊕ **Tip:**

1. Each One2One rule can only bind 20 external addresses at maximum.
2. "External starting IP address" must be set, and the actually mapped external IP address is gradually increased from the set value. For example, if "Internal starting IP address" is set to 192.168.1.50; "Internal ending IP address" is set to 192.168.1.52; "external starting address" is set to 200.200.202.50, then 192.168.1.50, 192.168.1.51, 192.168.1.52 are in turn mapped to 200.200.202.50, 200.200.202.51, 200.200.202.52.

7.1.4 DMZ

The DMZ functions of the device are described below.

Figure 7_6 DMZ configuration

- ◆ Enable DMZ function: Enables or disable the DMZ function.
- ◆ DMZ host IP address: The IP address of the network computer used as a virtual server (DMZ host).

⊕ **Tip:**

The computer that is set to a DMZ host will lose the firewall protection of the device, which takes effect to all WAN ports.

7.1.5 NAT and DMZ configuration instances

This section describes the specific instances of NAT and DMZ configuration. Includes: Static NAT mapping instances, instances with the type of NAT rules as EasyIP, One2One.

I. Instances of Static NAT mapping configuration

Intranet computer 192.168.1.99 starts the TCP80 port services, and wants to access this service through WAN1 port 80. It's configuration is as shown in Figure 7_7.

The screenshot shows a web-based configuration interface for port forwarding. The fields are as follows:

- Name: * (empty text box)
- Enable: (checked)
- Protocol: TCP (dropdown menu)
- Start External Port: * 1 (text box)
- IP Address: * (empty text box)
- Used Port: 80 (web) (dropdown menu)
- Start Internal Port: * 80 (text box)
- Port Count: * 1 (text box)
- Bind to: WAN1 (dropdown menu)

Below the form are four buttons: Save, Cancel, Help, and Back.

Figure 7_7 Port Forwarding Settings

II. EasyIP configuration instances

An Internet café uses a single line for Internet access, and the ISP has assigned 8 addresses for this line: 218.1.21.0/29 -218.1.21.7/29, where 218.1.21.1/29 is the gateway address of the line, and 218.1.21.2/29 is the IP address of WAN1 port of the device. Note that 218.1.21.0/29 and 218.1.21.7/29 are respectively the related subnet number and broadcast address, which cannot be used.

Now, Game B Zone (IP address range: 192.168.1.10/24-192.168.1.100/24) wishes to use 218.1.21.3/29 as a NAT mapping address for accessing to the Internet through the WAN port.

Configuration steps are follows:

The first step is to enter the *Advanced configuration -> NAT and DMZ configurations -> NAT rules* page, and click <Add new entry>.

The second step is to enter the *NAT rules configuration* page, and fill in "Game Zone" in the

"Rule name".

The third step is to select "NAT type" as "EasyIP".

The fourth step is to fill in 218.1.21.3 in the "External IP address". Fill in 192.168.1.10 and 192.168.1.100 in "Internal starting IP address" and "Internal ending IP address" respectively.

The fifth step is to select the rule-bound interface as WAN1 port.

The sixth step is to click <Save>, and the NAT rule is configured successfully.

The screenshot shows a configuration window for a NAT rule. The fields are as follows:

- Rule Name *: Game
- NAT Type: EasyIP (dropdown menu)
- External IP *: 218.1.21.3
- Start Internal IP *: 192.168.1.10
- End Internal IP *: 192.168.1.100
- Bind to: WAN1 (dropdown menu)

Below the fields, there is a note: "Multiple internal IP addresses are mapped to a single external IP address." At the bottom of the window, there are four buttons: Save, Cancel, Help, and Back.

Figure 7_8 NAT rules Settings——EasyIP

⊕ **Tip:**

When configuring Easy IP, if the "External IP address" is not on the same network segment as the IP address of the bound interface, a route must be configured on the upper router to the network segment on which the "External IP address" resides or a 32-bit host route to the "external IP address", and the next hop is set to the IP address of the bound interface.

III. One2One configuration instance

Demands

An enterprise applies for a line of Telecom, which adopts the fixed IP access method, and the bandwidth is 6M. Telecom assigned 8 addresses to it: 202.1.1.128/29-202.1.1.135/29. Here, 202.1.1.129/29 is the gateway address of the line, and 202.1.1.130/29 is the IP address of the device's WAN1. Note: 218.1.21.0/29 and 218.1.21.7/29 are respectively the related subnet number and broadcast address, which cannot be used.

The company wants its people to access to the Internet via NAT by using 202.1.1.130/29 sharing. Additionally, there are four servers that are in one-to-one NAT (One2One) and use 202.1.1.131/29-202.1.1.134/29 for providing services externally. The internal network address is 192.168.1.0/24, and the address for 4 servers is 192.168.1.200/24-192.168.1.203/24.

Analysis

Since the fixed IP access mode is used for Internet access on this line, it is necessary to configure

the fixed IP access to the default Internet line in *Network parameters* —> *WAN port configuration* page, or directly enter the *Start--> Configuration wizard > Network parameter* spage to configure the line. After the default Internet access line is configured correctly, the system-reserved NAT rules corresponding to the default line will be automatically generated, and the NAT function is automatically enabled.

And this enterprise provides four internal servers for external access, so it is also necessary to set an NAT rule with the type of "One2One".

Configuration steps are follows:

The first step is to enter the *Advanced configuration -> NAT and DMZ configurations -> NAT rules* page, and click <Add new entry>.

The second step is to enter the NAT rules configuration page, and fill in "Server" in the "Rule name".

The third step is to select "NAT type" as "One2One".

The fourth step is to fill in 202.1.1.131 in the "External starting IP address". Fill in 192.168.1.200 and 192.168.1.203 in "Internal starting IP address" and "Internal ending IP address" respectively.

The fifth step is to select the rule-bound interface as WAN1 port.

The sixth step is to click <Save>, and the NAT rule is configured successfully.

The screenshot displays a web-based configuration form for a NAT rule. The form includes the following fields and controls:

- Rule Name ***: A text input field containing "Server".
- NAT Type**: A dropdown menu set to "One2One". Below it, a descriptive text reads: "One internal IP address is mapped to one external IP address."
- Start External IP ***: A text input field containing "202.1.1.131".
- Start Internal IP ***: A text input field containing "192.168.1.200".
- End Internal IP ***: A text input field containing "192.168.1.203".
- Bind to**: A dropdown menu set to "WAN1".

At the bottom of the form, there are four buttons: "Save", "Cancel", "Help", and "Back".

Figure 7_9 NAT rule Settings —One2One

7.2 Static Route Settings

This section describes the *Advanced Configuration-> Routing configuration* page and configuration methods.

Static route is manually configured by a network administrator, making the transmission of packets to the specified destination network be realized according to the predetermined path. Static routing does not change with changes in the structure of the network, therefore, when network structure changes or there is a network failure, you need to manually modify the static routing information in the routing table. Setting and using static routes correctly can improve network performance and meet special requirements, such as implementing traffic control, guaranteeing bandwidth for important applications and so on.

The following describes the list of routing configuration information and the meaning of the parameters in the routing configuration.

Route Name	Status	Destination IP	Subnet Mask	Gateway IP	Priority	Interface	Edit

Figure 7_10 Static Route List

Click <Add new entry> in the above figure, and enter the *Route configuration* page.

Route Name *

Enable Select the check box to make the static route take effect.

Destination IP *

Subnet Mask *

Gateway IP *

Priority * The smaller the number, the higher the priority.

Interface

Figure 7_11 Static Route Settings

- ◆ Routing name: The name of static routes (custom, no repetition).
- ◆ Enable this configuration: Enables this static route. Selecting it means enabled, while deselecting it means the route is disabled.
- ◆ Destination network: The destination network number for this static route.
- ◆ Subnet mask: The mask of the destination network for this static route.
- ◆ Gateway address: The IP address of the next-hop router ingress. The device defines a line for hopping to the next router through interface and gateway. Typically, the interface address and the gateway must be on the same network segment.
- ◆ Priority: Sets the priority of a static route. When the destination network, subnet mask are the same, select the high priority routing for forwarding data, and the smaller the value is, the higher the priority is.
- ◆ Interface: The forwarding interface for the specified packets. The packets matching the static route will be forwarded from the specified interface.

⊕ **Tip:**

When the destination network and priority of multiple routes are the same, the device will match them in the principle of first matching for last establishment.

7.3 Policy routing

This section mainly describes *Advanced Configuration*—>*Policy routing* page and configuration methods. In this page, you can define policy routing, and the packet are routed according to the source IP addresses, protocols, destination addresses and destination ports.

7.3.1 Enable policy routing

Enable policy routing

Policy Routing List 0/20

0/0 Lines/Page First Prev Next Last Goto Page Page Search

Policy routing name	Allow	Interface	Source IP	Destination address	Pr

Select All

Figure 7_12 Policy routing list

- ▶ Enable policy routing: This is a global switch of policy routing. Only after it is enabled can the configured policy routing can take effect.
- ▶ Move to: Users can appropriately sort the policies using this bLeveloneon.

7.3.2 Policy routing configuration

Click <Add new entry> in the above figure, and enter the *Policy routing configuration* page.

Enable

Select the check box to make the rule take effect.

Policy routing name*

Interface* WAN1 ▼

Source IP IP Range To

A group of LAN hosts to which the rule applies.

User Group ▼

Destination address IP Range To

Policy controlled WAN IP addresses.

User Group ▼

Protocol ▼

Common Service ▼

Dest Port Start* Dest Port End *

Schedule Settings

Days Every Day

Mon Tue Wed Thu Fri Sat Sun

Time All Day

From : To :

Figure 7_13 Policy routing configuration

- ◆ Interface: Sets the physical interface bound by the policy routing, and the packets that meet the conditions of policy routing will be forwarded from the bound interface.
- ◆ Policy route name: Customizes the name of the policy.
- ◆ Source address: The source IP address of the packets following this policy route, which can be configured in two ways.
 - Network segment: The starting IP address and the ending IP address following this policy route.
 - User group: The user group following this policy route, click on "User group" to refer to the source address for policy reference for the user group. Enter User management -> User group configuration-> Add new entry to set up the source address field for the policy routing to take effect.
- ◆ Destination address: The destination address in the packet following this policy route, which is configured in the same way as the source address.
- ◆ Services: The services in the packets following this policy route, which can be configured in the following manner.
 - Ports: Range 1-65535, the corresponding protocols are TCP and UDP; when the selected

protocol is ICMP, the port range needs not be configured.

- ◆ Effective time setting: Selects the time period for the policy routing takes effect, and the default date is "Every day". The time is "All day". You can go to Advanced settings —> Configure policy route page to edit the time for the policy route to take effect.

⊕ **Tip:**

1. When all the packets match the defined source IP address, protocol and destination port, they will be forwarded to the specified interface, but the packets that cannot find a matching policy routes will go the normal route.
2. The execution order of policy routing: Static route to the LAN port > Policy routing > Static route to the WAN port.

7.4 Anti-NetSniper

This section describes the *Advanced Configuration* -> *Anti-NetSniper* page and configuration methods. Network vanguard defense is used to crack the shared detection set by the network operator. Verify that the intranet is experiencing a sharing problem, or don't enable that function.



Figure 7_14 Anti-NetSniper

7.5 Port mirroring

This section describes the port mirroring function of the *Advanced configuration* -> *Port mirroring* page. With the port mirroring function, you can copy the flow of the monitoring port to the monitoring port, to provide the detailed information on the transmitting status of the monitored ports, allowing network managers to make traffic monitoring, performance analysis and troubleshooting.

Except HiPER™ 840G, the devices of HiPER series that support the port mirroring function have the default LAN1 port of monitoring port, and other LAN ports are monitored ports. The

configuration interface is shown in the figure below.



Figure 7_15 Port mirroring

- ◆ Enable mirroring: Checking it to enable this feature.

When the HiPER™ 840G device supports two or more LAN ports, the port mirroring function can work.

- ◆ Monitoring port: The port for monitoring the traffic of the monitored ports, which can be only one.
- ◆ Monitored port: Only one monitored port can be selected.

⊕ **Tip:** The monitored port cannot be the same port as the monitoring port.

7.6 Port VLAN

This section describes the port VLAN function of the *Advanced configuration -> Port VLAN* page.

VLAN (virtual LAN) can split the network into several different broadcast domains logically. A logical constitutes a logical broadcast domain. The members of the same VLAN share broadcast and can communicate with each other. To achieve physical isolation between different VLANs, the unicast, broadcast and multicast packets within a VLAN will not be forwarded to any other VLAN, thereby helping to control traffic, simplify network management and enhance network security.

3. Port VLAN list

2. A VLAN can contain more than one port, and one port can belong to more than one VLAN.

5. Instances of Port VLAN

Requirements: The host under the LAN1 port can communicate with the hosts under the LAN2, LAN3 ports, but those under the LAN2 and LAN3 ports cannot access to each other.

Configuration steps:

1. Modify VLAN 1, whose member ports only include: 1, 2.
2. Create VLAN 2, whose member ports are: 1, 3.

Analysis: Both LAN1 port and LAN2 port belong to VLAN1, both LAN1 and LAN3 belong to VLAN2; the hosts under the fixed LAN1 port can communicate with the hosts under LAN2, LAN3 ports. Additionally, both LAN2 port and LAN3 port are not in the same VLAN, and the hosts under LAN2 and LAN3 cannot access to each other.

7.7 SYSLOG configuration

This section describes the *Advanced Configuration -> SYSLOG configuration* page.

The screenshot shows a configuration form for Syslog. It contains the following elements:

- Enable Syslog:** A checkbox that is currently unchecked.
- Syslog Server IP Address (Domain Name):** A text input field that is empty.
- Syslog Server Port:** A text input field containing the value "514".
- Syslog Message Facility:** A dropdown menu with "Local0" selected.
- Buttons:** Three buttons labeled "Save", "Cancel", and "Help" are located at the bottom of the form.

Figure 7_18 SYSLOG configuration

- ◆ **Enable Syslog service:** After the syslog service feature is enabled, this feature will send a large amount of information of device operation to a syslog server, which makes it easy for administrators to analyze system conditions, and monitoring system activity.
- ◆ **Address of syslog server (domain name):** Sets the address of the syslog server, which can be an IP address or a domain name.
- ◆ **Port of Syslog server:** Sets the service ports that are opened by the syslog server, whose default value is 514.
- ◆ **Syslog message type:** Sets the type of syslog message to be sent, whose default value is Local0.

Chapter 8. User management

This chapter describes the secondary menu under the primary menu of user management, including: User state, IP/MAC binding, PPPoE server, WEB authentication, user group configuration.

8.1 User status

This section describes the *User management-> User status* page. Administrators can understand all intranet users' net behaviors, the traffic occupied by the net behaviors and the status of each user, and so on by viewing, analyzing the pie charts and lists in this page.



Figure 8_1 User Status

- ◆ Analysis of the current network traffic usage: analyzes the current percentage of network traffic used by Intranet applications.
- ◆ Analysis of current net behaviors: Analyzes the net behavior of all currently online users.
- ▶ Clear data: The system counts the traffic and net behaviors from 00:00 every day. Clicking this button will clear the historical data of the day and immediately begin to recount.
- ▶ Disable identification statistics: Click this button to disable the identification function for net behavior management. After doing this, the net behavior management function will be

- ◆ Total uplink, downlink traffic: Displays the total uplink and downlink traffic of Intranet users.
- ◆ Online time: Displays the user's online time.
- ◆ Group: Displays the group to which the user belongs.
- ◆ Net behavior: Displays the user's net behaviors.
- ◆ Settings: Click the icon. If you want to clear the user's net behavior statistics, please click "Clear data".
- ◆ Note: Click on the icon to modify the description information of PPPoE dial-up user, WEB authenticated user.
- ◆ Automatic refreshing interval: This list supports automatic refreshing, with the interval of 1-5 seconds.
- ▶ Stop automatic refreshing: Click this button and the list will stop automatic refreshing. If you need to view the information of the entire list or modify the notes, etc., it is proposed to stop automatic refreshing.
- ▶ Start automatic refreshing: Click this button and the list will refresh the list at the automatic refreshing interval.

8.2 IP/MAC binding

This section describes the *User management->IP/MAC binding* page and configuration method.

To implement network security management, you must first solve the identity problems of users before you can carry out the necessary service authorization work. In *Firewall -> Access control policy*, we will introduce how to implement the control of Intranet users' net behaviors. In this section, we will describe how to solve the problem of user identification.

In the device, user's identification can be completed through the IP/MAC binding function. The use of the bound IP/MAC address pair as the user's unique identity ID can protect the device and network against IP spoofing attacks. IP spoofing attack means that a host attempts to use another trusted host's IP address to connect to the device or pass through the device. This host's IP address can be easily changed as a trusted IP address, but the MAC address is added by the manufacturer to the Ethernet card, so it cannot be easily changed.

8.2.1 IP/MAC binding list

IP/MAC Binding List IP/MAC Binding Settings

Allow Undefined LAN PCs

IP/MAC Binding List 0/1024

0/0 Lines/Page 10 Goto Page Page Search

User Name	IP Address	MAC Address	Allow	Edit

Select All

Figure 8_3 IP/MAC binding global configuration

- ◆ Allow non-IP/MAC bound user to connect to the device: Allows or disallows the non-IP/MAC bound users to connect to the device, and access to other networks through the device.
- ◆ Allow: Ticking this check box means to allow the bound user to connect to the device, but unchecking it means to disallow the bound user to connect to the device.
- ◆ Modify the IP/MAC binding entries, click the Edit icon, to enter the *IP/MAC binding configuration* page as shown in the figure below, and after change, click <Save>.
- ▶ Export: This button is used to export the IP address, MAC address, user name in the list of IP/MAC binding information.

用户名 *

IP地址 *

MAC地址 *

Figure 8_4 Modification of IP/MAC instances

⊕ **Tip:**

Before deciding to cancel the "Allow non-IP/MAC bound user to connect to the device" function, you must make sure that the management computer has been added to the "IP/MAC binding information list", otherwise it will cause the management computer to be unable to connect to the device.

8.2.2 IP/MAC binding configuration



Figure 8_5 IP/MAC binding configuration

- ◆ Network segment: The management IP address/subnet mask of the device by default.
- ◆ Text box: Displays the scanned IP/MAC information, or the configured IP/MAC binding information, whose input format is "IP+MAC+ username".
 - IP address, MAC address: The user's IP address, MAC address (which can be obtained using the ipconfig /all command under DOS environment on Windows platforms).
 - User name: It can be ignored, because the system will automatically assign a name for it.
- ▶ Scan: Click <Scan> to display the ARP information dynamically learned by the device.

- ▶ **Binding:** Binds all the IP/MAC entries in the text box.

⊕ **Tip:**

1. In the above input format, there may be one or more spaces between the IP and MAC, MAC and username.
2. For the invalid entries, the system will skip the invalid configuration entries in binding.

8.2.3 IP/MAC binding instances

Flexibly using the IP/MAC binding feature can configure "white list" and "black list" for Internet access for Intranet users.

By configuring the "white list" for Internet access, only the users in "white list" are allowed to access the Internet through the device, while prohibiting all other users from doing it. Therefore, if only a few users in the intranet are allowed for accessing the Internet, a "white list" is to be configured to achieve this goal.

By configuring the "black list" for Internet access, only the users in "black list" are prohibited from accessing the Internet through the device, while allowing all other users to do it. Therefore, if only a few users in the intranet are prohibited from accessing the Internet, a "black list" is to be configured to achieve this goal.

In the device, the users in the "white list" are legal users - their IP and MAC address exactly matches an entry in the "IP/MAC binding information list", and the entry selects "Allow".

The users in the "black list" are illegal users - their IP and MAC address exactly matches an entry in the "IP/MAC binding information list", and the entry does not select "Allow". Or, there is only one entry in their IP and MAC address matches the corresponding information of a bound entry.

1. Configure "white list" of Internet access for Intranet users, following these steps:

First, Specify legal users by configuring the IP/MAC binding entries, and use the IP address and MAC address of the host with the permission to access the Internet as the IP/MAC address binding pair, and add it to the "IP/MAC-binding information list", and "Allow" needs also be selected, that is, allow the users exactly matching the IP/MAC address to access the Internet.

Next, deselect the "Allow non-IP/MAC binding user to connect to the device", so that all other hosts not included in the "IP/MAC binding information list" will not be able to access the Internet.

For example, if you want to allow a host with the IP address of 192.168.1.2, and the MAC address of 0021859b4544 to connect to and pass the device, you can add an IP/MAC address binding entry, enter the host's IP address and MAC address, and select "Allow", as shown in Figure 8_6.

IP/MAC Binding List

IP/MAC Binding Settings

Allow Undefined LAN PCs Save Help

IP/MAC Binding List 0/1024

0/0 Lines/Page 10 First Prev Next Last Goto Page Page Search

	User Name	IP Address	MAC Address	Allow	Edit
<input type="checkbox"/>	test	192.168.1.2	00:21:85:9b:45:44	<input checked="" type="checkbox"/>	

Select All Export Add Delete All Delete

Figure 8_6 IP/MAC binding information list – Instance I

2. Configure "Black list" of Internet access for intranet users, following these steps:

First, specify the illegal user by configuring the IP/MAC binding entries, and there are two methods:

1. Use the IP address of the host that is prohibited from Internet access and the MAC address of any of the non-intranet adapter as the IP/MAC address binding pair, and add it into the "IP/MAC-binding information list".
2. You can use the IP and MAC addresses of the host that is prohibited from Internet access as the IP/MAC address binding pair, and deselect "Allow" (no "√" in the box), namely, to prohibit the users that exactly match the IP/MAC address from accessing to the Internet.

Next, select the "Allow non-IP/MAC binding user to connect to the device", so that all other hosts whose IP addresses and MAC addresses are not included in the "IP/MAC binding information list" will be able to access the Internet.

For example, if you want to prohibit a host with the IP address (for example, 192.168.1.3) from accessing and connecting to the device, you can add a IP/MAC address binding pair, enter the IP address, and the MAC address is set to the MAC address of any non- intranet adapter, as shown in the table below.

IP/MAC Binding List

IP/MAC Binding Settings

Allow Undefined LAN PCs

IP/MAC Binding List 0/1024

0/0 Lines/Page 10 Goto Page Page Search

	User Name	IP Address	MAC Address	Allow	Edit
<input type="checkbox"/>	test	192.168.1.2	00:21:85:9b:45:44	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Select All

Figure 8_7 IP/MAC binding information list – Instance II

For example, if you want to prohibit a host with the IP address of 192.168.1.30 and the MAC address of 0021859b2564 from connecting and passing the device, you can add an IP/MAC address binding pair, enter the host's IP address and MAC address, and deselect "Allow" (no "✓" in the box), as shown in Figure 8_8.

IP/MAC Binding List

IP/MAC Binding Settings

Allow Undefined LAN PCs

IP/MAC Binding List 0/1024

0/0 Lines/Page 10 Goto Page Page Search

	User Name	IP Address	MAC Address	Allow	Edit
<input type="checkbox"/>	test	192.168.1.2	00:21:85:9b:45:44	<input type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Select All

Figure 8_8 IP/MAC binding information list – Instance III

8.3 PPPoE Server

This section describes the device's PPPoE function, including: PPPoE introduction, PPPoE global configuration of device, configuration of PPPoE accounts and viewing of PPPoE connection status.

8.3.1 PPPoE introduction

PPPoE (Point-to-Point Protocol over Ethernet). It allows a host on the Ethernet to connect to the Internet through a simple access device. PPPoE protocol uses Client/Server, which encapsulates PPP packets in an Ethernet frame, and provides the point-to-point connection over Ethernet. PPPoE dial-up connections include two stages, Discovery (discovery) and Session (PPP session). The following will introduce these two stages.

1. Discovery stage

This stage is used to establish a connection. When a user host wants to start a PPPoE session, it must first implement the discovery stage to identify the Ethernet MAC address of PPPoE Server, and establish a PPPoE session ID (Session ID).

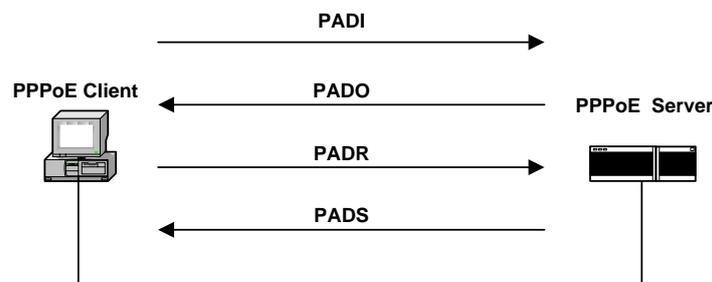


Figure 8_9 Basic workflow of Discovery stage

As shown in the figure above, Discovery stage consists of four steps. The following describes the basic workflow.

- PADI: If you want to set up a PPPoE connection, PPPoE client should first send a PADI (PPPoE Active Discovery Initiation) packet as a broadcast. The PADI packet includes the services the client requests.
- PADO: When the PPPoE server receives a PADI packet, it will determine if it is able to provide services, and if so, it will send to the client a PADO (PPPoE Active Discovery Offer) packet to respond. PADO packets include the PPPoE server name and the service name

same as that in the PADI packet. If the PPPoE server cannot provide services to PADI, it is not allowed to use the PADO packet to respond.

- **PADR:** Since PADI is sent as a broadcast, the PPPoE client may receive more than one PADO packet, and it will review all the PADO packets received and choose a PPPoE server based on the server name in it or the services provided, and then send a PADR (PPPoE Active Discovery Request) packet to the selected server. PADR packet includes the services requested by the client.
- **PADS:** When PPPoE server receives the PADR packet sent by the client, it is ready to start a PPPoE session, and creates a unique PPPoE session ID for PPPoE session, and sends to the client a PADS (PPPoE Active Discovery Session-confirmation) package as a response.

When the discovery stage ends normally, both ends of the communication obtain the session ID and their MAC addresses, and they define a PPPoE session together uniquely.

2. PPP session stage

When PPPoE enters the PPP session stage, the client and the server will conduct a standard PPP negotiation, and after this, the data is sent over PPP encapsulation. The PPP packets are encapsulated as the payload of PPPoE frame in an Ethernet frame, and sent to the peer end of the PPPoE link. Session ID must be the ID determined in the Discovery stage, and remains unchanged during the session. The MAC address must be that of the peer end.

At any time during the session stage, both PPPoE server and client can send PADT (PPPoE Active Discovery Terminate) to each other, notifying the other side of ending the session. When receiving PADT, it is not allowed to use the session to send the PPP traffic. After sending or receiving a PADT packet, even the conventional PPP end packet is not allowed to be sent. Normally, both parties of PPP communication end the PPPoE session using the PPP itself, but can end the session using PADT if PPP cannot be used.

8.3.2 PPPoE global Settings

Enter *User management->PPPoE server* page to configure the PPPoE server function. The configuration parameters are described as follows.

Figure 8_10 PPPoE Global Settings

- ◆ Enable PPPoE server: Enables/disables the PPPoE server function of the device. Select it to enable.
- ◆ Forcing PPPoE authentication: Enabling it means to only allow the users who pass the intranet PPPoE authentication to access the Internet.
- ◆ Exception address group: After the device enables the forcing PPPoE authentication, the users of the address group can communicate with external network without dial-up authentication, and the address group needs to be configured in the *User management -> User group configuration* page.
- ◆ Starting IP address: The starting IP address the PPPoE server automatically assigns to the network computers.
- ◆ Primary DNS server: The IP address of the primary DNS server automatically assigned by the PPPoE server to the network computers.
- ◆ Secondary DNS server: The IP address of the secondary DNS server automatically assigned by the PPPoE server to the network computers.
- ◆ Allow users to modify the dial-up password: Checking it means to allow intranet PPPoE dial-up users to modify dial-up password on their own.
- ◆ Password authentication mode: The way PPPoE authenticates username and password. The device provides three authentication modes, PAP, CHAP and AUTO, and the default value is AUTO, which means that the system automatically selects one of PAP and CHAP to authenticate the dial-in users, and generally does not need to be set.
- ◆ Maximum number of sessions: The maximum number of PPPoE sessions supported by the

- ◆ User name: The user name of PPPoE dial-up users.
- ◆ Enable: If the user is allowed to access the Internet. Checking it means allow.
- ◆ Fixed IP address: Displays the IP address bound to that user name.
- ◆ Charging mode: When the charging feature is enabled, the "by date" will be displayed (which currently supports charged by date).
- ◆ User status: The using status of the user will be displayed after the charging feature is enabled, including: normal, to be expired, expired.
 - To be expired: This parameter is controlled through "Account Days Remaining" in the account expiration notification feature (Here, the account expiration notification feature, please go to **Behavior management** -> **Electronic notification** page for configuration).
 - Expired: Means that the account is not in the effective date of account.
- ◆ Date of account opening, date of account disabling: When the charging feature is enabled, the effective date of the account will be displayed.
- ◆ Upload rate limit, download rate limit: The maximum upload and download rates of PPPOE (0 means unlimited rate).
- ◆ Maximum number of sessions for account: Displays the number of users who can simultaneously use the account for PPPoE connection.
- ◆ MAC address: Displays the MAC address bound by the account.
- ◆ Upload rate limit, download rate limit: Sets rate limit in batch for the accounts checked in the PPPoE account info list (0 means unlimited rate).
- ◆ Rate limit: Click on this bLeveloneon, to bring the upload speed, download rate limit in force.

User Name *	<input type="text"/>
Password *	<input type="password"/>
MAC Binding	None ▼
Max Sessions *	1
Static IP Address	<input type="text"/>
Select Account Group	None ▼
Accounting Mode	<input type="checkbox"/>
Account Effective Date	yyyy-mm-dd
Account Expiration Date	yyyy-mm-dd
Max. Tx Rate	0 kbit/s <== No Limit ▼
Max. Rx Rate	0 kbit/s <== No Limit ▼
Remarks	<input type="text"/>

Figure 8_12 PPPoE account settings

- ◆ User name: The account (custom, not repeatable) used by users in initiating PPPoE connections for the PPPoE server to authenticate, the value range is: 1-31 characters.
- ◆ Password: The password used by users in initiating PPPoE connections for the PPPoE server to authenticate.
- ◆ MAC binding: Chooses to bind the user name with the corresponding MAC address. If binding, only the hosts with the corresponding MAC address can use the account for accessing to the Internet.
 - No binding: Means no user name/MAC binding is to be done.
 - Automatic binding: After the user dials up successfully for the first time, the device will automatically bind the user name with the dial-up user's MAC address.
 - Manual binding: Manually enters the MAC address in the MAC address bar for user name/MAC binding.
- ◆ Maximum number of sessions for account: Sets the number of users who can simultaneously use the account for PPPoE connection.
- ◆ Fixed IP address: The fixed IP address assigned for the PPPoE dial-up user, which must be within the scope of address pool.
- ◆ Added to the account groups: the user name will be added to the appropriate account group, which must be configured in the *User management -> User group configuration* page.
- ◆ Charging mode: Checking it means that the PPPoE charging feature is enabled. Here, the account expiration notification feature is configured in the *Behavior management -> Electronic notification* page.
- ◆ Date of account opening, date of account disabling: Sets the effective date for the dial-up user using the account.
- ◆ Upload rate limit, download rate limit: The maximum upload and download rates of the PPPOE account (0 means unlimited rate).
- ◆ Note: Fill in the information to be noted. When Note Information is long, the page displays only 5 characters, and when you position the mouse pointer over the content of the note, the page will automatically display all the contents of the note.
- ⊕ **Tip:**

If the PPPoE account is configured with the upload and download rate, then the account will no longer match the fine rate limit.

8.3.4 PPPoE user status

Enter the *User management -> PPPoE server -> PPPoE user connection status* page, on which

Figure 8_14 Export PPPoE Accounts

- ▶ Export account: Click this button to export all PPPoE accounts in the list, including the user name, password for the account, in the .txt format.

8.3.6 Import PPPOE Accounts



test1 123456

Save

1. PPPoE account input format is: User Name Password, e.g., test 123456. One account per line.
2. Please note that there must be one or more spaces between the account and the password.

Figure 8_15 Import PPPOE Accounts

Tip:

1. When configuring PPPOE accounts to be imported and bound in batch, its input format is "Account + password", for example, test 123456, each row can have only one configuration item entered.
2. In the above input format, there may be one or more spaces between the account and the password.

8.3.7 Instance of PPPoE server configuration

1. **Demand:** Only the users authenticated by the Intranet can access the Internet.

Now, 3 accounts are configured for intranet users, and their user names are test1, test2, and test3 respectively. Initial passwords are: password1, password2, password3, in which test1, test2 are separately bound with 10.0.0.1, 10.0.0.2 and the charging feature is enabled (the using period of the account is from October 1, 2012 to December 31, 2013) and a notification is issued 15 days prior to account expiration; the maximum number of sessions of test3 is set to 5.

2. Configuration steps:

- 1) Configure the PPPoE server. Log on to the device, enter the *User management -> PPPoE server* page, configure the content as shown in the figure below, and enable the forced PPPoE authentication and allow users to modify the dial-up password (The password change message can be given to users by configuring the routine business notification feature).

Figure 8_16 Instance - PPPoE Global Settings

- 2) Configuration of PPPoE account. Enter the *PPPoE account Settings*. Click on the <Add new entry>, configure a PPPoE account, bind the account with the IP address, and enable the charging feature. The configured content with the user name of test1 is as shown in the figure below:

8.4 WEB authentication

8.4.1 WebAuth Global Settings

Enter the *User management->WEB certification* page to configure the WEB authentication feature of the device. WEB Authentication is used to authenticate Intranet users as to having permission to access the Internet, that is, after enabling this feature, the intranet users cannot access to the Internet unless passing the WEB authentication.

Figure 8_19 WebAuth Global Settings

- ◆ Enable WEB authentication: Checking it means that the intranet users cannot access the Internet unless passing the WEB authentication.
- ◆ Enable background image: Check it to enable this feature.
- ◆ Allow users to modify authentication password: Checking it means to allow the WEB authentication users to modify the authentication password on their own.
- ◆ Exception address group: After the device enables the forced PPPoE authentication, the users of the address group can communicate with external network without WEB authentication, and the address group needs to be configured in the *User management -> User group Settings* page.

- ◆ User name: Displays/configures the user name of the WEB authentication user.
- ◆ Concurrent number: Displays the number of users using the same WEB authentication.
- ◆ User status: Displays the connection status of the WEB authentication users, including: not used, in use.
- ◆ Charging mode: Displaying/checking it means to enable the charging mode.
- ◆ Account opening/expiry date: Displays/configures the time period for the WEB authenticated user to use the account.
- ◆ Total time: Restricts the total time for the WEB authenticated user to use the account. 0 means no limit.
- ◆ Used time: Displays the time the currently authenticated account used accumulatively.
- ◆ Description: Displays/configures that described content.
- ◆ Password: Configures the password of the WEB authentication user.
- ◆ Maximum number of sessions for the account: Configures the maximum number of sessions for the account.
- ▶ Hang up: Clicks this button to hang up the connection to the user.
- ▶ Add new entry: Click this button to enter the Figure 8_21 page to configure the information WEB authentication account.
- ▶ Delete all entries: Click this button to delete all information configured on the page.

⊕ **Tip:**

1. Steps that the WEB authenticated users modify the authentication password:

- 1) Users open the browser for authentication using the user name, password.
- 2) After a successful authentication, click to change the password in the dialog box for successful authentication that opens.
- 3) On the password change page, enter the user name, old password, new password and confirming password.
- 4) Click "Submit" to display "Operation is successful", and the password is successfully changed.
- 5) Users can modify their password 5 times a day on their own.
- 6) The administrator can use the **Behavior management** -> **Electronic notification** page to configure the Routine business notification for informing users of how to modify the PPPoE dial-up password.

8.5 User Group Settings

In the *User management -> User Group Settings* page, and click <Add new entry> in the "User group configuration list", to enter the page as shown in Figure 8_24.

组名	类型	成员	编辑
<input type="checkbox"/> zu1	地址组	P(192.168.2.1-192.168.2.10)	
<input type="checkbox"/> zu2	地址组	P(192.168.2.100-192.168.2.150)	

全选 / 全不选
 添加新条目
删除所有条目
删除

Figure 8_23 User group list

Group Name:
 Group Type: Address Group ▾
 New Address: ▾

Start IP:
 End IP:

==>
 <==
 Delete

Address Members List:

Save Cancel Help Back

Figure 8_24 User group Settings

- ◆ Group name: Customizes the group name of the user group.
- ◆ Group type: It consists of address group and account group. Here, account group refers to the PPPoE authentication accounts, WEB authentication accounts.

⊕ **Tip:**

The depth of the user group cannot be greater than 2, for instance: Address A contains Address Group B, and now it is configured with Address Group C, it is not allowed to make it contain Address Group A.

Schedule Name	<input type="text"/>
Effective Date Range	<input checked="" type="radio"/> Forever <input type="radio"/> <input type="text" value="yyyy-mm-dd"/> To <input type="text" value="yyyy-mm-dd"/>
Time Period 1	<input type="checkbox"/>
Days	<input checked="" type="checkbox"/> Every Day <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun
Time	<input checked="" type="radio"/> All Day <input type="radio"/> From <input type="text" value="00"/> : <input type="text" value="00"/> To <input type="text" value="00"/> : <input type="text" value="00"/>
Time Period 2	<input type="checkbox"/>
Days	<input checked="" type="checkbox"/> Every Day <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun
Time	<input checked="" type="radio"/> All Day <input type="radio"/> From <input type="text" value="00"/> : <input type="text" value="00"/> To <input type="text" value="00"/> : <input type="text" value="00"/>
Time Period 3	<input type="checkbox"/>
Days	<input checked="" type="checkbox"/> Every Day <input type="checkbox"/> Mon <input type="checkbox"/> Tue <input type="checkbox"/> Wed <input type="checkbox"/> Thu <input type="checkbox"/> Fri <input type="checkbox"/> Sat <input type="checkbox"/> Sun
Time	<input checked="" type="radio"/> All Day <input type="radio"/> From <input type="text" value="00"/> : <input type="text" value="00"/> To <input type="text" value="00"/> : <input type="text" value="00"/>
<input type="button" value="Save"/> <input type="button" value="Help"/> <input type="button" value="Back"/>	

Figure 9_2 Schedule Settings

9.2 Application Control

This section describes the net behavior management list and net behavior management configuration in the *App Control* -> *Application Control* page.

9.2.1 Application Management List

Enter the *Behavior management-> Net behavior management* page, to enable the net behavior management feature in this page, and view the net behavior management information configured in the list of net behavior management information.

Enable Internet Application Management Save

Application Management List 0/20

0/0 Lines/Page 10 First Prev Next Last Goto Page Page Search

Group Name	Network Objects	Blocked Applications

Select All Add Delete All Delete

Figure 9_3 Application Management List

- ◆ Enable net behavior management: Checking it means to enable the net behavior management feature.

9.2.2 Internet Application Management Settings

Click <Add new entry> on the above image to enter the *Net behavior management configuration* page, to manage intranet users' net behavior.

- ◆ Group name: Customizes the group name for the instances of the net behavior management, which must be unique.
- ◆ Select net behavior management object: Fills out the address field or user group on which the behavior management instance takes effect.
- ◆ The net behavior management supported by the device: Chat software, P2P software, stock software, web video, online game, shopping web sites, social networking sites, web games,

messages, forums, etc.

- ◆ Effective time setting: Sets the time when the net behavior management instance takes effect.

⊕ **Tip:**

When a net behavior management feature does not take effect, make sure that this policy library is up-to-date. In the *Behavior management* → *Policy library* page, click <Update> hyperlink to update the corresponding policy library.

Group Settings :

Group Name *

Network Object IP Range To

User Group

Select All

IM Software : Select All

P2P Software : Select All

Stock Software : Select All

Network Video : Select All

Online Game : Select All

Shopping Site :	Select All	<input type="checkbox"/>	<input type="button" value="+"/>

Social Networking Site :	Select All	<input type="checkbox"/>	<input type="button" value="+"/>

Web Game :	Select All	<input type="checkbox"/>	<input type="button" value="+"/>

Email :	Select All	<input type="checkbox"/>	<input type="button" value="+"/>

Forum :	Select All	<input type="checkbox"/>	<input type="button" value="+"/>

Others :	Select All	<input type="checkbox"/>	<input type="button" value="+"/>

Schedule Settings:

Days Every Day
 Mon Tue Wed Thu Fri Sat Sun

Time All Day
 From : To :

Figure 9_4 Internet Application Management Settings

9.2.3 Internet Application Management

1. Demands

In order to control its employees' net behavior, a company prescribes according to their actual needs, to prohibit QQ, MSN and other chat software, stocks and game software, checking stocks and game site information, and access to the shopping website during the working time. In the rest of the time, all operations are opened up.

Here, the users at the management level (address: 192.168.1.5 and 192.168.1.9) are not subject to any restrictions in net behavior.

Sales and customer service staff, whose addresses are 192.168.1.70-192.168.1.99 and 192.168.1.50 - 192.168.1.69 respectively, must use chat software to communicate with customers as required by their work.

The R & D Department (address: 192.168.1.100-192.168.1.129) prohibits the use of chat software.

The company's working hours are: Monday-Friday, 9 o'clock -18 o'clock.

2. Analysis

From above, 2 net behavior management policies are configured based on the requirements of the company's net behavior management.

- 1) Configure the net behavior management policies for sales and customer service staff to enable the chat software feature. However, other features are disabled.
- 2) Configure the net behavior management policies for R&D staff by only prohibiting the use of chat software.

3. Configuration steps

- 1) Enter the *Behavior management-> Net behavior management* page, to enter the *Net behavior management configuration* page.

- 2) Configure behavior management policies for sales department, customer service department:

Group name: IM

Starting IP address, ending IP address: 192.168.1.50, 192.168.1.99.

Behavior management: Checks the "Select All" box of stock software, online video, online games, shopping sites, social networking sites, Web games, mails, forums and others.

Effective time period: Monday to Friday, from 9:00-18:00. Click <Save>.

- 3) Configure the behavior management policies for the R&D Department:

Group name: yanfa

Starting IP address, ending IP address: 192.168.1.100, 192.168.1.129.

Behavior management: Just checks the "Select All" box of the chat software.

Effective time period: Monday to Friday, from 9:00-18:00. Click <Save>.

4. View the configuration list

Enable Internet Application Management

Application Management List 0/20

0/0 Lines/Page 10 Goto Page Page Search

	Group Name	Network Objects	Blocked Applications
<input type="checkbox"/>	IM	192.168.1.50--192.168.1.99	BitTorrent;Thunder;QLive;PPStream
<input type="checkbox"/>	yanfa	192.168.1.100--192.168.1.129	WLMessenger;AliiM;WebQQ;Fetion;

Select All

Figure 9_5 Internet Application Management

Enable Internet Application Management

Application Management List 0/20

0/0 Lines/Page 10 Goto Page Page Search

ects	Blocked Applications	Schedule	Enable	Edit
	BitTorrent;Thunder;QLive;PPStream;...	09:00-18:00	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>
	WLMessenger;AliiM;WebQQ;Fetion;QQ;	09:00-18:00	<input checked="" type="checkbox"/>	<input type="button" value="Edit"/> <input type="button" value="Delete"/>

Select All

Figure 9_6 Internet Application Management (Continued Figure 9_5)

9.3 QQ white list

QQ white list refers to the QQ users who are defined to be allowed to log on after QQ is

prohibited in the *Net behavior management* page.

Enter the *App Control-> QQ white list* page, after the QQ white list feature is enabled, click "Add new entry" to add QQ white list users in the QQ white list configuration page.

Allow 400/800 Enterprise QQ
 Enable QQ Whitelist

QQ Whitelist 0/1024

0/0 Lines/Page 10 Goto Page Page Search

QQ Number	Description	Edit

Select All

Figure 9_7 QQ white list

- ◆ Allow 400/800 Business QQ: Checks to allow 400/800 Business QQ.
- ◆ Enable QQ white list: Checks to enable the QQ white list feature.
- ▶ Export account: Click this button to export the QQ accounts in the QQ white list entry.
- ▶ Import account: Click this button to import QQ to the QQ white list entries.



1. Enter one entry per line, in the format: QQ Number Description, e.g., 1440398074 Jimmy.

2. There must be at least one space between QQ Number and Description.

Figure 9_8 Import QQ Accounts



Tip:

The maximum number of QQ numbers supported by this version is 4294967295

9.4 TM Whitelist

Aliwangwang White List refers to the Aliwangwang users allowed to log in after Aliwangwang is prohibited in the **Net behavior management**

Enter the *App Control* -> *TM Whitelist* page, and after the Aliwangwang white list feature is enabled, click "Add new entry" to enter into the Aliwangwang white list configuration page to add Aliwangwang white list users.

9.5.1 Daily Routine Notification

Enable

IP Address Range To

Notification Title

Redirection Time Sec(Leave it blank to disable redirection)

Redirect to URL **http://**

Notification Content

Effective Date Range To

Recurring Time Range

Days Every Day
 Mon Tue Wed Thu Fri Sat Sun

Time All Day
 From : To :

Figure 9_10 Daily Routine Notification

- ◆ Enable: Checks to enable the Routine business notification feature.
- ◆ Notification network segment: Sets the address range of routine business notification, which can only contain 65535 addresses at maximum.
- ◆ Notification title, content: Sets the title and content of the routine business notification.
- ◆ Redirecting time: Redirects to the specified page according to the specified time.
- ◆ Redirecting URL: Automatically redirects to the specified URL address.
- ◆ Setting of effective date: Sets the date when the routine business notification takes effect.

- ◆ Effective frequency: Sets the frequency of routine business notification.
- ▶ Preview page: Click this bLeveloneon to preview the configured notification contents.
- ▶ Save: After click <Save>, the specified users in the Intranet will receive a routine business notification sent by the device when it accesses to the web page for the first time with the effective time period.

⊕ **Tip:**

When the routine business notification only involves the change of "Notification title", "Notification content", click <Save> and the notification will not take effect.

9.5.2 Account expiration notification

The screenshot shows a web-based configuration interface for account expiration notifications. It features two tabs at the top: 'Daily Routine Notification' and 'Account Expiration Notification'. The 'Account Expiration Notification' tab is active. Below the tabs, there are four configuration fields:

- Enable:** A checkbox that is currently unchecked.
- Notify:** A text input field containing the number '0', followed by the text 'Days before Expiration Date'.
- Notification Title:** A text input field that is currently empty.
- Notification Content:** A large, empty text area with a vertical scrollbar on the right side.

 At the bottom right of the form, there are three buttons: 'Preview', 'Save', and 'Help'.

Figure 9_11 Account expiration notification

- ◆ Enable: Checks to enable the account expiration notification feature.
- ◆ Days for sending expiration notices in advance: Sets the effective number of days for sending expiration notification. When this parameter is set to 10, the user will receive the expiration

notification sent by the device when it dials up successfully and accesses to the website for the first time starting from 10 days before the expiration of the account.

- ◆ Notification title, content: Sets the title and content of the account expiration notification.
- ◆ Preview page: Click this button to preview the configured notification contents.

⊕ **Tip:**

When the account of the network dial-up user expires, dial-up can be made successfully, and the user can access to the device, but cannot access the Internet. Meanwhile, it will receive an expiration notification sent by the device in accessing the website.

9.6 Application Audit

The section describes the net behavior audit feature. Enter the *App Control* -> *Application Audit* -> *Log Management* page, as shown in the figure below.

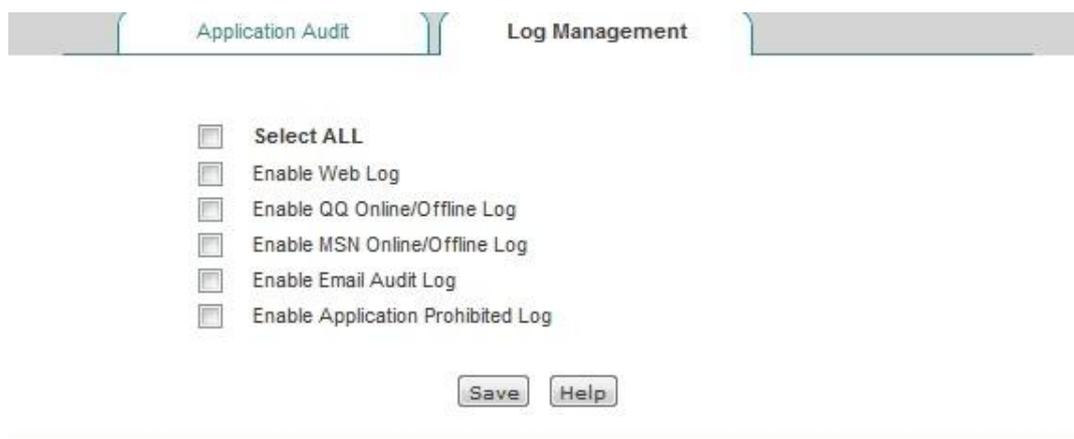


Figure 9_12 Log management

- ◆ Enable web logs: Enables the web log to view the records of Intranet users' access to webpages in the *Behavior audit* page. Such as “2012-12-03 15:07:47 srcip=10.0.0.10; url=www.Levelone.com.cn”, which means that the users whose Intranet IP address is 10.0.0.10 at 15:07 on December 3, 2012 visited www.Levelone.com.cn.
- ◆ Enable QQ online/offline logs: Enable the QQ online/offline logs to view the online/offline logs of the Intranet user QQ in the *Behavior audit*.
- ◆ Enable MSN online/offline logs: Enable the MSN online/offline logs to view the online/offline logs of the Intranet user MSN in the *Behavior audit*.
- ◆ Enable mail audit logs: Enable the mail audit logs to view the records of Intranet user mails in the *Behavior audit* page.

- ◆ Enable behavior-blocking log: Enable the behavior-blocking log to view the user records filtered by the behavior management PDB.

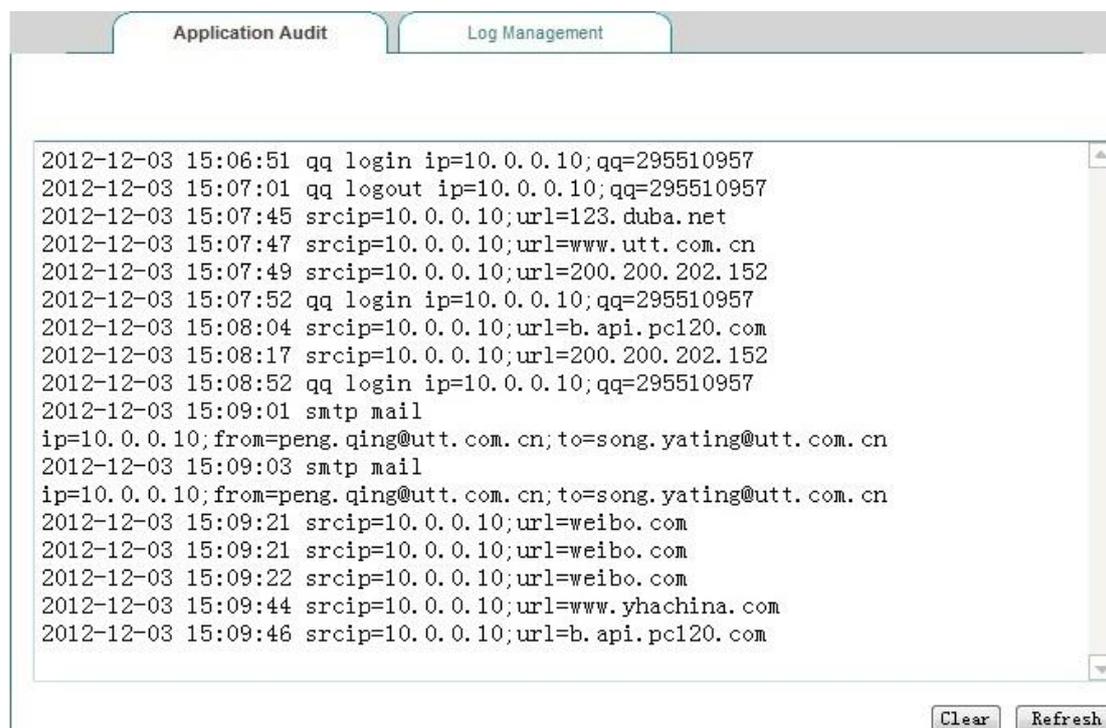


Figure 9_13 Internet Audit

- ⊕ **Note:** Net behavior audit can record the latest 400 log information.

9.7 Policy Database

This section describes the *App Control - Policy Database* page and operating procedures. The system provides 11 different types of policies at present, including: emails, IM, P2P, STOCK, online video, online games, shopping websites, social networking sites, web games, forums, etc. Users can bring the behavior management referencing these policies into force by updating one policy or all policies.

Policy Database List				167/167				
1/17 Lines/Page 10		First	Prev	Next	Last	Goto Page	Page	Search
Name	Type	Description				Update Policy		
MailQQ	Email	Block QQ Mail				Update		
WLMessenger	IM	Block MSN				Update		
AliIM	IM	Block Ali Wangwang				Update		
WebQQ	IM	Block Web QQ				Update		
Fetion	IM	Block Fetion				Update		
BitTorrent	P2P	Block BitComet, BitSpirit				Update		
Thunder	P2P	Block Thunder Search				Update		
QQLive	P2P	Block QQLive				Update		
PPStream	P2P	Block PPS				Update		
KuGou	P2P	Block KuGou Search				Update		

Figure 9_14 Policy Database list

The following describes the meaning of the parameters in the policy library info list.

- ◆ Name: The name of a policy.
- ◆ Type: The type of a policy, for example, QQ is of the IM type as shown in the above figure.
- ◆ Notes: A detailed description of a policy.
- ◆ Update policy: Click < Update > to update a policy online through the Internet.

2. Fixed Rate Limiting Rule Settings

Click <Add new entry> in the above figure to enter the **Fixed Rate Limiting Rule Settings** page. The following describes the meaning of the parameters for configuring fine rate limit.

The screenshot shows a configuration window for Fixed Rate Limiting Rule Settings. It contains the following elements:

- Group Name ***: A text input field.
- Network Object**: Two radio buttons. The first is **IP Range** with input fields for **0.0.0.0** and **To 0.0.0.0**. The second is **User Group** with a dropdown menu showing **All Users**.
- Rate Limiting Mode**: A dropdown menu set to **Each (Assign Bandwidth for Each IP Address)**.
- Max. Tx Rate**: A text input field with **0**, followed by **kbit/s** and a dropdown menu set to **No Limit**. A note in parentheses says **(0 means no limit)**.
- Max. Rx Rate**: A text input field with **0**, followed by **kbit/s** and a dropdown menu set to **No Limit**. A note in parentheses says **(0 means no limit)**.
- Schedule Settings**:
 - Days**: A checked checkbox for **Every Day** and unchecked checkboxes for **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, and **Sun**.
 - Time**: A radio button for **All Day** and a radio button for **From** with dropdowns for **00**, **:00**, **To**, **00**, **:00**.
- At the bottom are four buttons: **Save**, **Cancel**, **Help**, and **Back**.

Figure 10_2 Fixed Rate Limiting Rule Settings

- ◆ **Group name:** Customizes the group name of the instance of the fine rate limit, which cannot be the same as another instance name.
- ◆ **Select the object of rate limit:** Fills in the starting IP address and ending IP address of the address field for the fine rate limit to take effect.
- ◆ **Rate limit policy:** The available options are exclusive and shared; Exclusive means each IP addresses in this range can use this bandwidth. Shared means the IP addresses in this range share this bandwidth.
- ◆ **Uploading rate limit and downloading rate limit:** Sets the maximum uploading, downloading rates of the IP addresses in this range here. 0 means no limitation.
- ◆ **Effective time setting:** Sets the time for the fine rate limit to take effect in the IP address range.

10.2 Flexible bandwidth

This section describes the *QoS* **Flexible bandwidth** page and the meaning of the configuration parameters. When the network is busy, the flexible bandwidth feature guarantees that each intranet user can have a normal Internet access.

⊕ **Tip:** It is not recommended to enable the flexible bandwidth feature and fine rate limit feature.

The screenshot displays a configuration window for flexible bandwidth and game optimization. At the top, there is a checkbox for 'Enable Flexible Bandwidth' which is currently unchecked. Below this, four sections are provided for WAN ports (WAN1Port, WAN2Port, WAN3Port, and WAN4Port). Each section contains two input fields: 'Uplink Bandwidth' and 'Downlink Bandwidth', both set to '0' kbit/s. To the right of each input field is a dropdown menu set to '<== No Limit' with a note '(0 means no limit)'. At the bottom, there is a section for 'Enable Game Optimization' with a checked checkbox and a list of games: 'Select All', 'LOL', 'WOW', 'DNF', 'Fantasy', 'Westward Journey', and 'CF', all of which are checked. At the very bottom are three buttons: 'Save', 'Cancel', and 'Help'.

Figure 10_3 Flexible Bandwidth

- ◆ Enable flexible bandwidth: Checks to enable the flexible bandwidth feature.
- ◆ Uplink and downlink bandwidth of WAN1: Sets the uplink and downlink bandwidth of WAN1 applied for from ISP, and the custom maximum value of Gigabit devices can be set to 1000M.
- ◆ Uplink and downlink bandwidth of WAN2: Sets the uplink and downlink bandwidth of WAN1 applied for from ISP, and the custom maximum value of Gigabit devices can be set to 1000M.
- ◆ Enable game acceleration: Checks to enable the acceleration of games.

10.3 Session Limiting

This section describes the *QoS-> Session Limiting* page. You can define the maximum total number of connections, the maximum number of TCP connections, the maximum number of UDP connections, and the maximum number of ICMP connections established by each host in the Intranet allowed by the device by setting the numbers of connections.

The screenshot shows a configuration interface for session limiting. It includes a checkbox for 'Enable Session Limit' which is checked. Below it are four text input fields: 'Max. Sessions' with the value 1500, 'Max. TCP Sessions' with 1000, 'Max. UDP Sessions' with 800, and 'Max. ICMP Sessions' with 100. A note below the fields states 'Note: 0 means no limit.' At the bottom of the form are three buttons: 'Save', 'Cancel', and 'Help'.

Figure 10_4 Session Limiting

- ◆ Enable connections limit: Checks to enable the connections limit.
- ◆ Total connections: The maximum total number of connections established per host in the Intranet, whose default is 1500.
- ◆ Total connections: The maximum number of TCP connections established per host in the Intranet, whose default is 1000.
- ◆ Total connections: The maximum number of UDP connections established per host in the Intranet, whose default is 800.
- ◆ Total connections: The maximum number of ICMP connections established per host in the Intranet, whose default is 100.

⊕ **Tip:**

1. When the number of connections is set at 0, the number of connections per Intranet host is not to be limited.
2. When the connection of Intranet applications (such as network game) becomes slow, you can increase the "Total number of connections" and "Number of UDP connections" (or "Number of TCP connection") appropriately. Note: The number of the above connections is set too high, which may cause the device's capability to lower or lose its capability against the DDoS attacks.

3. Under normal circumstances, the maximum number of sessions cannot be set too low, so it is recommended that: "The number of TCP connections" is not less than 100, "the number of UDP connections" is not less than 50, "the number of ICMP connections" is not less than 10. If their value is too small, it will cause the LAN users to be unable to access the Internet or access the Internet normally.

Chapter 11. Firewall

This chapter describes how to configure the device's firewall feature, including security configuration, access control policy, and domain name filtering.

11.1 Attack Prevention

This section describes the *Firewall -> Attack Prevention* interface and its configuration.

1. Internal Attack Prevention

Figure 11_1 Attack Prevention - Internal Attack Prevention

- ◆ Enable DDoS attack defense: When enabled, the device will effectively defend against the common Intranet DDOS attacks.
- ◆ Enable IP spoofing defense: When enabled, the device can effectively defend against Intranet IP spoofing.
- ◆ Enable UDP FLOOD defense: When enabled, the device can effectively defend against Intranet UDP FLOOD attacks.
- ◆ Enable ICMP FLOOD defense: When enabled, the device can effectively defend against Intranet ICMP FLOOD attacks.

- ◆ Enable SYN FLOOD defense: When enabled, the device can effectively defend against Intranet SYN FLOOD attacks.
- ◆ Enable ARP proofing defense: When enabled, the device's LAN port can send ARP broadcast packets at a certain time interval (the default is 100 milliseconds), which can effectively defend against ARP spoofing.
- ◆ Enable device access control: When enabled, only the hosts within the address field range to log on the device via the LAN port.
- ◆ Enable port scan defense: When enabled, the device can effectively defend against Intranet port scanning.

2. External Attack Prevention



Figure 11_2 Attack Prevention - External Attack Prevention

- ◆ Reject external Ping: When enabled, the WAN port of the device does not respond to the ping requests from the external network.

11.2 Access control

This section describes the functions and configuration methods of the *Firewall -> Access control policy*.

Flexibility in the use of the access control feature not only can set Internet access for different users, but also can control the Internet access of users at different times. In practical applications, the device can be configured with related access control policies according to the management regulations of individual agencies. For example, for school users, access control policies can be configured to prohibit students from visiting the games websites. For family users, it can be configured to only allow children to access the Internet during the specified time. For enterprise users, it can be configured to prevent the machines of the finance department from being accessed by the Internet.

11.2.1 Access Control Rule

Configuring access control policies on the device can monitor each packet flowing through the device. By default, the device is not configured with access control policies, and it will forward all the legitimate packets received. If the access control policy is configured, when the device receives a packet, it will extract the source MAC address, source address, destination address, upper-layer protocol, port number or the packet content for analysis, and assign them according to the order of the policy table from top to bottom, view any matching policy, and implement the action defined by the first policy: forwarding or discarding. And it will no longer compare the rest of the policies.

You can specify the filter type for access control policy by setting the "Filter type". The device offers four filter types: IP filtering, URL filtering, keyword filtering and DNS filtering.

1. IP filtering

IP filtering refers to filtering of packet header information, such as source and destination IP addresses. If the protocol field encapsulation protocol in the IP header is TCP or UDP, then filter again according to the TCP header information (source port and destination port) or UDP header information (source port and destination port).

When filter type is IP filtering, the filtering conditions available for setting include: Source address, destination IP address, protocol, source port, destination port, action and effective time, etc.

2. URL filtering

URL filtering refers to filtering of URL websites. Filtering according to the keywords in the URL not only can control the Intranet users in access to a site, but also can control user access to the web pages.

When the filter type is URL filtering, the filtering conditions available for setting include: source address, filtering content (refer to URL address), actions, and effective time.

3. Keyword filtering

Keyword filtering refers to keyword filtering in the HTML pages (web pages), which means if you have made a comment (such as pornography, the Falun Gong, gambling, etc.), the comment will not be submitted successfully.

When the filter type is keyword filtering, the filtering conditions available for setting include: source address, filtering content (refers to the keywords on a web page) and the effective time.

4. DNS filtering

DNS filtering refers to filtering of domain names, which is made according to the keywords in the

domain name.

When the filter type is DNS filtering, the filtering conditions available for setting include: source address, filtering content (refers to the domain names to be filtered), action, effective time period.

✚ **Tip:** DNS filtering is implemented through Port 53, while URL filtering is implemented through Port 80.

The actions of access control policy include forwarding and discarding, and the corresponding "actions" are "allow" or "disallow". When the packets to be processed match a defined access control policy, and if the "action" of the policy is "allow", then the device will forward the packet. If the "action" of the policy is "disallow", the device will discard the packet.

What needs to be aware of is that keyword filtering does not provide any "action" options, but "disallow" by default due to its special application.

11.2.2 Access control list

Drag the cross bar below the access control policy list, to view the detailed information of instances.

Enable Access Control Save

Access Control List 0/256

0/0 Lines/Page 10 First Prev Next Last Goto Page Page Search

Rule Name	Enable	Address Group	Action	Schedule	Filtering Type	Filtering Cont

Select All Add Delete All Delete

Rule Move To Mode

Figure 11_3 Access control list

- ▶ Move to: This bLeveloneon allows you to sort the instances accordingly.

⊕ **Tip:**

The user-defined access control policies are matched from top to bottom according to the order in the list.

11.2.3 Access Control Settings

Access control policy is to control the packets flowing through the device. Click <Add new entry> in the above figure, to enter the *Access control policy configuration* page, to configure the required firewall policy. The following will describe the meaning of the parameters in the access control policy configuration under four different filter types, IP filtering, URL filtering, keyword filtering and DNS filtering.

1. Access Control Settings - IP filtering

Rule Name*

Enable

Select the check box to make the rule take effect.

Source IP IP Range To

A group of LAN hosts to which the rule applies.

User Group

Action

Filtering Type

Protocol

Common Service

Dest Port Start* Dest Port End*

Dest IP Start Dest IP End

Source Port Start Source Port End

Schedule Settings

Days Every Day
 Mon Tue Wed Thu Fri Sat Sun

Time All Day
 From : To :

Figure 11_4 Access Control Settings - IP address filtering

- ◆ Policy name: The name of the custom access control policy.
- ◆ Enable this configuration: Enables this access control policy. Selecting it means to enable this policy, while deselecting it means to disable it.
- ◆ Source address: The Intranet users controlled by the access control policy.
- ◆ Action: The implementing action for the access control policy, the options are "allow" or "disallow".
 - Allow: Allows the packet that matches the access control policy to pass, that is, the device will forward the packet.
 - Disallow: Disallows the packet that matches the access control policy to pass, that is, the device will discard the packet.
- ◆ Filter type: Here, "IP filter" is selected.
- ◆ Protocol: The protocol type of the access control policy. The protocols available for choice are as follows: 1 (ICMP), 6 (TCP), 17 (UDP), 51 (AH), all (All). Among them, "all" indicates

all protocols. Appendix C provides a table of commonly used protocol numbers and protocol names.

- ◆ **Common services:** Provides the common service ports using UDP or TCP. Among them, the option "All" means all ports: Ports 1-65535.

After a port number (service) is selected, the system will automatically fill the port number in "Destination starting port" and "Destination ending port". Specifically, if you select "All", then fill in "destination starting port" and "destination ending port" as 1 and 65535 respectively.

Appendix D provides a table of common service ports and service names.

- ◆ **Destination starting port, destination-ending port:** the destination starting port and destination ending port for the access control policy, through which you can specify the destination ports within a segment. If only one destination port is defined, then set them to the same value, with the range of values as 1-65535.
- ◆ **Destination starting address, destination-ending address:** The destination starting IP address and destination ending address for the access control policy, through which you can specify the destination IP addresses within a segment. If only one destination IP address is defined, then they are set to the same value.
- ◆ **Source starting port, source-ending port:** the source starting port and source ending port for the access control policy, through which you can specify the source ports within a segment. If only one source port is defined, then set them to the same value. Value range is 1-65535.
- ◆ **Effective time setting:** The time when the access control policy takes effect. All times are not to be set.

⊕ **Tip:**

The IP address field being 0.0.0.0 to 0.0.0.0 by default means that it takes effect to all clients, that is, there is no limitation to the source address, including the clients in the LAN address field, the clients of the PPPoE Server address pool.

2. Access Control Settings -- URL filtering

Rule Name*

Enable

Select the check box to make the rule take effect.

Source IP IP Range To

A group of LAN hosts to which the rule applies.

User Group

Action

Filtering Type

Filtering Content*

Schedule Settings

Days Every Day

Mon Tue Wed Thu Fri Sat Sun

Time All Day

From : To :

Figure 11_5 Access Control Settings -- URL filtering

"Policy name", "Source address", "Action" and other parameters have the same meaning as the related parameters in the "IP filter", which will not be repeated here. Please refer to the description.

- ◆ Filter type: Here, "URL filtering" is selected.
- ◆ Filter content: The URL address to be filtered for the access control policy.

URL filtering is based on the URL keyword filtering. When the URL of the page to be access contains the fields exactly matching "Filter content", it is considered to match the policy. Here, you can enter a complete domain name; at this time, all pages that start with the domain name are matched. Or you can enter the substring of the domain name, and then all pages that contain the substring in the URL are matched, thus filtering all web pages of a site. Next, let's give a few examples to illustrate:

Instance 1: If you enter `www.sina.com.cn`, then all web pages beginning with `www.sina.com.cn` will match that policy, such as `www.sina.com.cn/index.jsp`, but the web pages beginning with `book.sina.com.cn` will not be matched.

Instance 2: If you enter `www.Levelone.com.cn/bbs/`, then all web pages beginning with `www.Levelone.com.cn/bbs/` will match that policy, thus controlling the LEVELONE's access to BBS page in this site.

Instance 3: if you enter `sina.com`, then all web pages containing `sina.com` are matched, which means the whole sina site is matched. Of course, the pages beginning with `book.sina.com.cn` will

be matched.

⊕ **Tip:**

1. In the URL addresses, the English characters are not case-sensitive. When you enter a URL, please do not include http://.
2. URL filtering cannot control users in using a Web browser to access other services. For example, the URL filtering cannot control the access to ftp://ftp.Levelone.com.cn. In this case, you need to disallow or allow FTP connections by configuring the access control policy of IP filter type.

3. Access Control Settings - Keyword filtering

The screenshot shows a web-based configuration interface for keyword filtering. It contains the following elements:

- Rule Name***: A text input field.
- Enable**: A checked checkbox with the instruction "Select the check box to make the rule take effect."
- Source IP**: A radio button selected for "IP Range" with input fields for "0.0.0.0" and "To 0.0.0.0". Below it is the text "A group of LAN hosts to which the rule applies." There is also a radio button for "User Group" with a dropdown menu showing "All Users".
- Action**: A dropdown menu set to "Deny".
- Filtering Type**: A dropdown menu set to "Keyword Filtering".
- Filtering Content***: A text input field.
- Schedule Settings**:
 - Days**: A checked "Every Day" checkbox and unchecked checkboxes for "Mon", "Tue", "Wed", "Thu", "Fri", "Sat", and "Sun".
 - Time**: A radio button selected for "All Day" and a radio button for "From" with time selection dropdowns (00:00 to 00:00).
- Buttons: "Save", "Cancel", "Help", and "Back" at the bottom.

Figure 11_6 Access Control Settings - Keyword filtering

"Policy name", "Source address", "Action" and other parameters have the same meaning as that of the parameters in the "IP filter" type, which will not be repeated here. Please refer to the related description.

- ◆ Filter type: "Keyword filter" is selected.
- ◆ Filter content: The keywords to be filtered by the access control policy, which refers to the keywords on a web page.

⊕ **Tip:**

1. For the access control policy with the filter type of "Keyword" , "Action" has only the option, "Disallow".
2. The filtered content should exclude: < > , % ' \ " & ; and the characters except spaces.

4. Access Control Settings -- DNS filtering

Rule Name*

Enable

Select the check box to make the rule take effect.

Source IP IP Range To

A group of LAN hosts to which the rule applies.

User Group

Action

Filtering Type

Filtering Content*

Schedule Settings

Days Every Day
 Mon Tue Wed Thu Fri Sat Sun

Time All Day
 From : To :

Figure 11_7 Access Control Settings - DNS filtering

"Policy name", "Source address", "Action" and other parameters have the same meaning as that of the parameters in the "IP filter" type, which will not be repeated here. Please refer to the related description.

- ◆ Filter type: Here, "DNS filtering" is selected.
- ◆ Filter content: Sets the domain name to be filtered.

⊕ Tip:

You can filter more than one domain names by entering the wildcard character, “ * ” in the filter content. For example, enter the domain name “*.163.*” in the filter content, and select "Disallow" in Action, and the intranet users will not be able to access all the web pages with the domain name containing “.163.”

11.2.4 Access Control Settings instance

This section describes two instances of access control.

1. Instance I

Requirements: An enterprise Intranet requires allowing only the users with the IP addresses of 192.168.1.10 - 192.168.1.20 to use WEB services during working hours (Monday to Friday, 9:00-18:00).

Analysis:

Custom policy 1: Allows the DNS application in 192.168.1.10-192.168.1.20.

Custom policy 2: Allows the WEB application in 192.168.1.10-192.168.1.20.

Custom policy 3: Disallows all other applications in 192.168.1.10-192.168.1.20.

What calls for special attention is that (Policy 3) when all services are prohibited, the DNS service is also prohibited. In order to make the users in this address field access the network normally, Policy 3 should be configured to the last.

Access control policy list:

Enable Access Control

Access Control List
2/256

1/1 Lines/Page 10
First Prev Next Last
Goto Page
Page
Search

	Rule Name	Enable	Address Group	Action	Schedule	Filter
<input type="checkbox"/>	test1	<input checked="" type="checkbox"/>	192.168.1.201--192.168.1.211	Allow	Mon. Tue. Wed. Thu. Fri. Sat	IP
<input type="checkbox"/>	test2	<input checked="" type="checkbox"/>	192.168.1.222--192.168.1.233	Block	Mon. Thu. Sun	IP

Select All

Rule

Mode

Figure 11_8 Access Control Settings - Instance I

Enable Access Control

Access Control List 2/256

1/1 Lines/Page 10 Goto Page Page Search

Dest Port Start	Dest Port End	Dest IP Start	Dest IP End	Source Port Start	Source Port End	Edit
2048	2088	0.0.0.0	0.0.0.0	1	65535	
5666	8888	0.0.0.0	0.0.0.0	1	65535	

Select All

Rule test1 Mode test1

Figure 11_9 Access Control Settings - Instance I (Continued Figure 11_8)

2. Instance II

Requirements: An enterprise network wants to prohibit the users in 192.168.1.80-192.168.1.100 from visiting the website <http://www.bbc.com> (IP address is 212.58.246.93) and the website <http://www.cnn.com> (IP address is 157.166.255.18), but allow all other online services of the group.

Analysis:

Configure Policy 1, to disallow the users in the segment of 192.168.1.80-192.168.1.100 to access <http://www.bbc.com>.

Configure Policy 2, to disallow the users in the segment of 192.168.1.80-192.168.1.100 to access <http://www.cnn.com>.

Enable Access Control

Access Control List 2/256

1/1 Lines/Page 10 First Prev Next Last Goto Page Page Search

<input type="checkbox"/>	Rule Name	Enable	Address Group	Action	Schedule	Filtering Type
<input type="checkbox"/>	test-3	<input checked="" type="checkbox"/>	192.168.1.33--192.168.1.44	Allow	Mon, Tue, Wed, Thu	URL Filtering
<input type="checkbox"/>	test-4	<input checked="" type="checkbox"/>	192.168.1.55--192.168.1.66	Block	Every Day	URL Filtering

Select All

Rule test-3 Mode test-3

Figure 11_10 Access Control Settings –Instance II

Enable Access Control

Access Control List 2/256

1/1 Lines/Page 10 First Prev Next Last Goto Page Page Search

	Dest Port Start	Dest Port End	Dest IP Start	Dest IP End	Source Port Start	Source Port End	Edit

Select All

Rule test-3 Mode test-3

Figure 11_11 Access Control Settings – Instance I (Continued Figure 11_10)

11.3 Domain filtering

This section describes the domain name filtering feature of the *Firewall -> Domain filtering* page, including the matters needing attention in the domain name filtering operation steps, domain name filtering configuration process.

11.3.1 Domain filtering Settings

Figure 11_12 Domain filtering page

Steps of configuring domain name filtering:

1. Check the "Enable domain name filtering".
2. Select the way for the domain name filtering policy to take effect.
3. Select the intranet objects for the domain name filtering to take effect.

4. Select the time period for the domain name filtering to take effect.
5. In the text box corresponding to "Domain name", enter the appropriate domain name, and click < Add new entry > bLeveloneon. A corresponding domain name will appear in the "Domain name list".
6. Click <Save>.

 **Tip:**

1. The device supports setting of the filtering of 100 domain names.
2. Domain name filtering is of matching whole word only. When the domain name entered by an intranet user in the browser matches the one as displayed in the "Domain list" in whole word, it will not be able to access the web page corresponding to that domain name.
3. You can filter multiple domain names by entering the wildcard character, "*", in the domain name, for example, enter the domain name, "www.163.*" in the domain name list, and intranet users will not be able to access all web pages beginning with "www.163".

11.3.2 Domain Block Notification

This section focuses on *Firewall->Domain filtering-> Domain Block Notification* function. When a web site is prohibited from access, it hopes to give users a hint that this web site being prohibited is not a network problem. Click on the domain name filtering notification tab, to enter the page as shown in Figure 12-13.

Figure 11_13 Domain Block Notification page

- ◆ Enable domain name filtering notification feature: Checking it means to enable this feature. After this feature is enabled, the device will send a notice to the user when the intranet users access the prohibited domain names, and after the set time, it will skip to a specific web site.
- ◆ Notice title: The title of the notification information pushed by the device.
- ◆ Redirecting time: Sets the redirecting time for accessing the domain name as listed in the domain name list. Blank means no redirecting while 0 means redirecting immediately
- ◆ Redirecting URL: Sets the domain name address redirected when accessing to the domain names as listed in the domain name list;
- ◆ Notice content: the content of the notification information pushed by the device.
- ▶ Save: The global configuration parameters domain name filtering take effect.
- ▶ Preview page: Previews the configured notification content, as shown in the figure below:

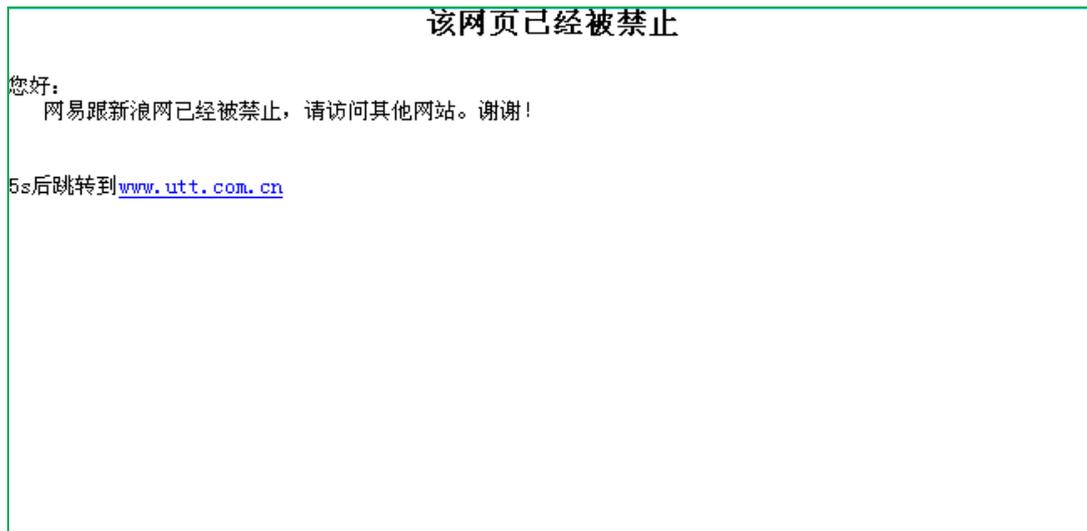


Figure 11_14 Domain Block Notification page

11.4 MAC Address Filtering

This section describes the MAC address filtering function of the *Firewall -> MAC address filtering* page, including: The steps of MAC address filtering and the points for attention to the process of MAC address filter configuration.

11.4.2 MAC Address Filtering Settings

Enter the MAC address filtering information list, click "Add new entry", to enter the MAC address filtering configuration page, as shown in the figure below.



Figure 11_16 MAC Address Filtering Settings

- ◆ User name: Displays the user name of the configured MAC address filtering.
- ◆ MAC address: Configures the MAC address to be filtered.

Users can configure in batch in the *Firewall -> MAC address filtering -> MAC Address Filtering Settings* page.

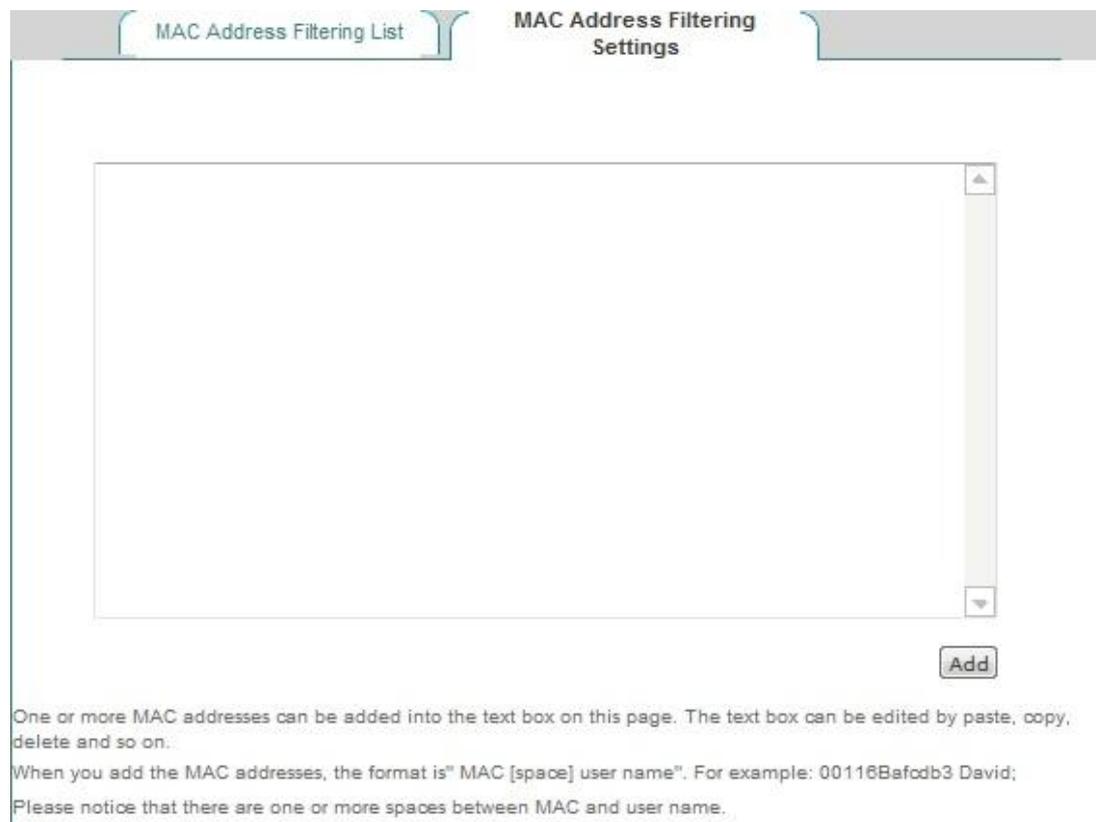


Figure 11_17 MAC address filtering

- ◆ Text box: Sets the corresponding MAC address information in the text box.

The input format is "MAC+ user name".

- MAC address: The user's MAC address (which can be obtained using the `ipconfig /all` command under the DOS environment on Windows platforms).
- User name: It can be ignored, because the system will automatically assign a name for it.

⊕ **Tip:**

1. In the above input format, there may be one or more spaces between the MAC address and the user name.
2. For the invalid entries, the system will skip the invalid configuration entries in binding.

Chapter 12. VPN

VPN (Virtual Private Network): VPN refers to the technology for establishing a dedicated data communication network in the public network (such as Internet) based on ISP (Internet Service Provider) and NSP (Network Service Provider).

12.1 PPTP

12.1.1 PPTP overview

PPTP (Point-to-Point Tunneling Protocol): PPTP is a virtual private networking protocol, belonging to the second layer protocol. PPTP encapsulates the PPP (Point-to-Point Protocol) frames in the IP datagrams, and sends them by IP networks, such as Internet or corporate Intranet.

The basic function of the PPTP is to transmit user data packets encapsulated using PPP in the IP network. PPTP client is responsible for receiving the raw data from users, and encapsulates it to the PPP packet, and then establishes a PPTP tunnel between the PPTP client and the server for sending the PPP packet.

Typical application is to deploy the PPTP clients in the PC software of remote offices or mobile office users, and they are used to launch the PPTP tunnel. The PPTP server is deployed in Enterprise Center or office, used to receive a call from the PPTP client. When a PPTP tunnel connection is established, the PPTP server receives the PPP packets from the PPTP client and restores user's data packets, and then sends the restored packets to the end user's PC.

NAT, and after the PPTP configuration is complete, the system will automatically generate a static NAT mapping to TCP 1723 port (which can be viewed in the "Static mapping information list" of *Advanced Configuration->NAT static mapping and DMZ*, named as "PPTP"). Please do not edit, delete them, or it may even cause the PPTP tunnel not to be connected and not to transmit data.

12.1.3 PPTP server configuration

Enter the *VPN configuration ->PPTP* page, click <Add a server>in the page as shown in Figure 12_2, and enter the *PPTP server* page.

12.1.3.1 Global Settings

Figure 12_3 PPTP server - Global Settings

- ◆ Enable PPTP server: Check to enable the service.
- ◆ Password authentication mode: Sets the password authentication mode to establish PPTP VPN. The options include MS-CHAPV2, PAP, CHAP, ANY (automatically negotiate with the peer device on password authentication mode).
- ◆ Address pool starting address: Configures the starting IP address assigned by the PPTP server to the PPTP client, to ensure that the network segment to which the address belongs does not repeat with any of the network segments in LAN.

- ◆ Number of address pool addresses: Sets the total number of the addresses in the address pool.
- ◆ Server IP address: The virtual interface IP address of the tunnel server. This address is not included in the address pool. Please confirm that the address and the address pool that is configured are located on the same network segment.
- ◆ Master/standby DNS server: When the device is configured as the PPTP/L2TP server, it can assign the DNS address for the PPTP/L2TP clients, so that users can browse web pages through the DNS address assigned on the server line after connecting to the server, which can solve the problem that users can open the internal network of the server after dialing through the VPN but cannot open the web pages.
- ◆ Encryption mode: Sets the data encryption mode, with the options of MPPE encryption, no encryption. Note: In the use of MPPE encryption mode, MS-CHAPV2 password authentication method must be selected.

12.1.3.2 Account Settings

The following describes the meaning of the parameters for the PPTP server to configure accounts for the PPTP client.

Figure 12_4 PPTP server - Account Settings

- ◆ Tunnel name: Custom tunnel name: Customizes the name of the tunnel, which must not repeat with the existing instance name in the device.
- ◆ User type: The options include LAN to LAN, mobile users.
 - LAN to LAN: An incoming PPTP user is the user of a network segment, which often is dialed through via a router, to implement communications in the LAN at both ends of the PPTP tunnel.
 - Mobile user: The dialed-in VPN user is an individual user, which is often dialed in by a

single PC, to implement the communications between the PPTP tunnel remote PC and the local LAN.

- ◆ User name: The user name used when the custom client is dialing.
- ◆ Password: The password used when the custom client is dialing.
- ◆ Fixed IP address: Sets up the IP address assigned by the PPTP server to the client, and the address must be in the PPTP server address pool.
- ◆ Remote Intranet network address: Fills in the IP addresses used by the LAN at the opposite end of the PPTP tunnel (which may be the LAN IP address of the device at the opposite end of the VPN tunnel).
- ◆ Remote Intranet subnet mask: Fills in the subnet mask used by the LAN at the opposite end of the PPTP tunnel.

12.1.4 PPTP client Settings

Enter the *VPN configuration* ->*PPTP* page, and click <Add a client> in the page as shown in Figure 12_2, to enter the *PPTP client* page. The following describes the meaning of the parameters for configuring the PPTP client.

Enable

Enable NAT

Tunnel Name *

User Name *

Password *

PPP Authentication ANY ▼

Encryption None ▼

Remote Subnet IP Address *

Remote Subnet Mask *

Server IP/Domain Name *

MTU * 1478 Byte
(MTU Range: 1-1492)

Save Cancel Help Back

Figure 12_5 PPTP client

- ◆ Enable the configuration: Check it to enable this configuration.
- ◆ Enable NAT: After NAT is enabled, the PPTP client will do NAT to the PPTP tunnel, that is, translate the LAN IP address to the IP address assigned by the peer PPTP server, so that LAN users will be connected to the LAN at the opposite end of the tunnel with the IP address assigned by the PPTP server, and the device at the opposite end of the tunnel need not to set the local route.
- ◆ Tunnel name: The name of the tunnel, which cannot repeat with the instance name existing in the device.
- ◆ User name: The user name when dialing this tunnel.
- ◆ Password: The password used when dialing the tunnel.
- ◆ Password authentication mode: Sets the password authentication mode to establish PPTP VPN. The options include MS-CHAPV2, PAP, CHAP, ANY (automatically negotiate with the peer device on password authentication mode). Make sure that the password authentication mode is consistent with that of the server.
- ◆ Encryption mode: Sets the data encryption mode, with the options of MPPE encryption, no encryption. Note: In the use of MPPE encryption mode, MS-CHAPV2 password authentication mode must be selected.
- ◆ Remote Intranet network address: Fills in the IP address of the remote Intranet, which can be the LAN IP address of the remote VPN gateway.
- ◆ Remote Intranet subnet mask: The subnet mask of the remote Intranet.
- ◆ Tunnel server address (name): Fills in the IP address or domain name of the WAN port of the remote VPN gateway.

12.1.5 PPTP configuration instance

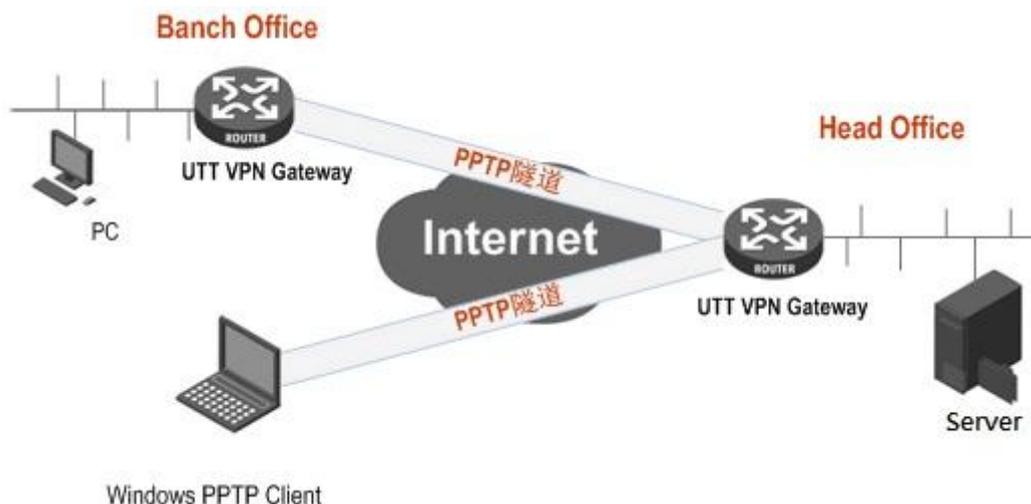


Figure 12_6 PPTP instance topology

In this scenario, a company is based in Shanghai. It has a branch office in Beijing, and hopes to achieve a mutual access to the internal resources of the LAN in two places. The company also has some mobile users in business trips and using remote office hoping to remotely access the company's internal resources of LAN.

The scenario uses the PPTP to establish VPN tunnels, and the VPN gateway in both places are using HiPER router, and the mobile users using the built-in PPTP client software of the Windows operating systems at the following addresses:

Shanghai gateway (PPTP server):

Intranet network segment: 192.168.1.0/24.

LAN IP address: 192.168.1.1/24.

WAN domain name: 200.200.202.126/24.

Beijing gateway (PPTP client):

Intranet network segment: 192.168.16.0/24.

LAN IP address: 192.168.16.1/24.

WAN IP address: 200.200.202.127/24.

Mobile client (PPTP client):

A PPTP tunnel connection is established using the Windows operating system through the PPTP dial-up.

The configuring steps are follows:

1. Configure Shanghai VPN gateway

Global Settings | Account Settings

Enable PPTP Server

PPP Authentication MS-CHAPV2 ▼

IP Pool Start Address 192.168.55.40

Number of Addresses 50

Server IP Address 192.168.55.0

Primary DNS Server 200.200.200.251

Secondary DNS Server 8.8.8.8

Encryption MPPE ▼

MTU 1478
(MTU Range: 1-1492)

Save Cancel Help Back

Figure 12_7 PPTP server Settings

Create an account for the Beijing Branch, user type: LAN to LAN. User name: Test2. Password: 123456. Password authentication mode: MS-CHAPV2. Remote Intranet network addresses: 192.168.16.1. Remote Intranet subnet mask: 255.255.255.0.

Global Settings | Account Settings

Tunnel Name * Head1

Tunnel Type * LAN-to-LAN ▼

User Name * test-1

Password * ●●●●●●

Static IP Address 192.168.55.40

Remote Subnet IP Address * 192.168.16.1

Remote Subnet Mask * 255.255.255.0

Save Cancel Help Back

Figure 12_8 PPTP server Settings - LAN to LAN

Create an account for mobile users, user types: Mobile users. User name: Test1. Password: 123456. And assign a fixed IP address of 192.168.55.41 for the mobile user.

Global Settings | Account Settings

Tunnel Name * Head2

Tunnel Type * Mobile User ▼

User Name * test-2

Password * ●●●●●●

Static IP Address 192.168.55.41

Save Cancel Help Back

Figure 12_9 PPTP server Settings - Mobile users

2. Configure Beijing PPTP Client

Enable

Enable NAT

Tunnel Name *

User Name *

Password *

PPP Authentication ANY ▼

Encryption None ▼

Remote Subnet IP Address *

Remote Subnet Mask *

Server IP/Domain Name *

MTU * 1478 Byte

(MTU Range: 1-1492)

Save Cancel Help Back

Figure 12_10 PPTP client Settings

PPTP clients are configured as shown in the above figure, user name: test1. Password: 123456. Password authentication mode: MS-CHAPV2. Remote Intranet network addresses: 192.168.1.1. Remote subnet mask: 255.255.255.0, tunnel server address: 200.200.202.126.

3. Mobile user configuration

Follow these steps to configure a Windows XP computer, allowing it to connect to the PPTP server.

The first step is to create a PPTP dial-up connection:

- 1) Enter the Windows XP ->"Start"→-> "Settings"→ -> "Control Panel", and select "Switch to category view".
- 2) Select "Network and Internet connections".
- 3) Select "Set up a network connection to your work location".
- 4) Select "Virtual private network connection (V)", and click "Next".
- 5) Enter a name for the connection, "Banch2", and click "Next".
- 6) Select "Do not dial this initial connection", and click "Next".
- 7) Enter the IP address "200.200.202.126" of the PPTP server ready to connect, and click "Next".
- 8) Click "Finish".
- 9) Double-click the "Banch2" connection, and in the Banch2 window, click "Properties".
- 10) Select the "Security" property page, select "Advanced (Custom settings)", and click "Settings".
- 11) In the "Data encryption", select "Optional encryption (which can connect without encryption)".
- 12) In "Allow these protocols", check "Unencrypted password (PAP)", "Challenge Handshake Authentication Protocol (CHAP)", "Microsoft CHAP (MS-CHAP)," "Microsoft CHAP (MS-CHAP v2) version", and click "OK".
- 13) Select the "Network" property page, and in "VPN Type", select "PPTP VPN".
- 14) Make sure that "Internet protocol (TCP/IP)" is selected.
- 15) Click "OK" and save your changes.

The second step is to connect to the PPTP server using the device PPTP tunnel:

- 1) Confirm that your PC is already connected to the Internet (probably a dial-up connection or a fixed IP access).
- 2) Start up the "Banch2" dial-up connection created in the first step.
- 3) Enter the PPTP user name "Test2" and the password "123456".
- 4) Click "Connect".
- 5) When the connection is successful, type "ipconfig" in MS-DOS mode, and you can see the addresses in the PPTP server address pool, which are the IP addresses assigned by the PPTP server to the local machine.

4. Viewing connection information

emerge, but IPSec VPN is currently one of the most widely used VPN security technologies. IPSec is a set of open standards, protocols to create and maintain IP network secure communication that provides two security mechanisms: encryption and authentication. Encryption mechanism ensures the confidentiality of data, while authentication mechanism ensures that data come from the original sender and are not destroyed and tampered with during transmission.

IPSec can provide the following services:

- **Data confidentiality:** The IPSec sender encrypts the packets before transmission across the network.
- **Data integrity:** The IPSec receiver authenticates the packets sent by the sender, to ensure that the data has not been tampered with during transmission.
- **Data source authentication:** IPSec can authenticate if the sending end for transmitting the IPSec packet is legitimate in order to ensure the authenticity of data.
- **Anti-replay:** The IPSec receiver can detect and reject to receive duplicate packets.

12.2.1.1 Abbreviations and terminology

IPSec (IP Security Protocol): IPSec is a series of protocols formulated by IETF, to ensure the security and confidentiality of the data sent across the Internet, and the communicating parties can guarantee the confidentiality, integrity and authenticity of packets sent across the Internet through encryption and data origin authentication at the IP layer.

IKE (Internet Key Exchange): IKE is used for both communicating parties to negotiate and establish security alliances, exchange keys. IKE defines the method for two parties to authenticate, negotiate encryption algorithm, and generate shared keys.

DES (Data Encryption Standard): DES is a data encryption algorithm used by IPSec to encrypt the packets.

3DES (Triple Data Encryption Standard): 3DES is a data encryption algorithm used by IPSec, to encrypt the packets with a higher strength than DES.

AES (Advanced Encryption Standard): AES is a data encryption algorithm used by IPSec. Compare with DES and 3DES, AES is more efficient and safer.

DH (Diffie-Hellman Group): Each party generates a pair of public and private keys, and only needs to exchange the public key with the other party, and after calculation, a set of private keys can be obtained for secure communications, which avoids the risk of direct transmission of keys in the communications, thus improving the security of the whole IPSec system. DH has an important property: group (components). There are 5 basic groups, and the commonly used groups are: MODP Group (Group2) with the modulus of 1024 bits and MODP Group (Group5) with the modulus of 1536 bits.

MD5 (Message Digest 5): The algorithm for generating a 128-bit hash (also known as a digital signature or information arrangement) from any length information and the 16-byte key. The

generated hash (as the input fingerprints) is used to validate the authenticity and integrity of the contents and sources.

SHA-1 (Secure Hash Algorithm1): The algorithm for generating a 160-bit hash from any length information and the 20-byte key. It is generally considered more secure than MD5 because it generates a larger hash.

SA (Security Association): Before an IPSec VPN tunnel is established between the two devices, through which secure communications can be made, they must agree on the security parameters required during the communication, namely establish a security association SA. SA will specify the authentication and encryption algorithms to be used, the key used during the call and the time to be maintained by the Security Alliance itself, and SA is unidirectional.

SPI (Security Parameter Index): SPI is actually a data entity with the length of 32 bits, used to uniquely identify a SA on the receiver.

AH (Authentication Header): A protocol of IPSec. This protocol is used to provide data integrity, packet source address authentication service for the IP packets. Compared with the ESP, AH do not provide communication data encryption services.

ESP (Encapsulating Security Payload): A protocol of IPSec. It is used to ensure the confidentiality of IP packets (not visible to any third parties), data integrity, and data source authentication, as well as the anti-replay feature.

PSK (Pre-Shared Key): One of the IKE authentication methods, which requires that each IKE peer use a predefined and shared key to authenticate the IKE exchange.

Phase I and Phase II: Establish an IPSec Channel Security Alliance (SA) using the Internet Key Exchange Protocol (IKE), which requires two stages of negotiation. In the first phase, participants authenticate each other and negotiate the establishment of a secure channel used to negotiate on the later IPSec SA. In the second phase, participants negotiate and establish IPSec SA that is used to encrypt and authenticate user data.

Main Mode and Aggressive Mode: IKE automatically negotiates the first phase of the channel, which can be done in two modes, main mode and aggressive mode. In main mode, the initiator and the responder have three bi-directional information exchanges between them, with a total of six messages. In aggressive mode, the initiator and the responder acquire the same objects, but have only two exchanges, with a total of three messages.

DPD (Dead Peer Detect): Using the DPD, you can regularly check SA as to whether the other party is normal, and the network connection is normal.

IPSec NAT-T (NAT-Traversal): This technique implements IPSec protocol penetrating the NAT device.

12.2.1.2 Security Alliance

Before an IPSec VPN tunnel is established between the two devices, through which secure communications can be made, they must agree on the security parameters required during the

communication, namely establish a security association SA. SA consists of a pair of specified security parameter indexes (SPI), the destination IP address and the used security protocol.

Through SA, the IPSec tunnel provides the following security features:

- Confidentiality (through encryption)
- Content integrity (through data authentication)
- Sender authentication and accreditation (through authentication)

I. Establishment of Security Alliance

Security Association (SA) is a one-way protocol of related methods and parameters used by both parties of the IPSec tunnel to ensure tunnel security. For IPSec two-way communication, there must be at least two SAs, one is used to receive data from the peer end, and the other one is used to send data to the other party.

The establishment of SA requires two phases of negotiations:

- In the first phase, both communicating parties negotiate on how to protect the future communications and to establish an authentication and security protection channel (namely, IKE SA), this channel will be used to protect the negotiation process of IPSec SA later.
- In the second phase, both parties negotiate about encryption algorithms, keys, life cycle, as well as authentication of IPSec, and establish a channel for encryption and authentication of user data (IPSec SA).

1. Phase I

In the first phase, Aggressive Mode or Main Mode can be used, and both parties will exchange the security proposals acceptable to each other, for example:

- Encryption algorithm (DES, 3DES and AES128/192/256) and authentication algorithm (MD5 and SHA-1)
- Diffie-Hellman group (please refer to "Diffie-Hellman Exchange" in this section)
- Pre-shared key

When both ends of the tunnel agreed to accept at least a group of security parameters for the first phase, and process the related parameters, a successful first-phase negotiation will end. When the device is used as the initiator, currently up to 8 kinds of proposes for the first-stage negotiation are supported to allow user to define a series of security parameters. While acting as a responder, the device can accept proposals for the first phase negotiation in any combination forms.

➤ Main Mode / Aggressive Mode

First stage can take place under the main mode or aggressive mode, and these two modes are described as follows:

Main mode: Initiator and responder make three bi-directional information exchange (a total of six messages) between them, in order to complete the following functions:

- The first exchange, (Messages 1 and 2): Provides and accepts encryption and authentication algorithms.
- The second exchange, (Messages 3 and 4): Implements the Diffie-Hellman exchange, both the initiator and the responder provide a current number (which is randomly generated).
- The third exchange, (Messages 5 and 6): Sends and verifies their identity.

The information sent at the third exchange of information is protected by the encryption algorithm established in the first two exchanges. Therefore, there is no identity of participants in transmission, thereby providing the maximum extent of protection.

In aggressive mode, the initiator and the responder acquire the same objects, but have only two exchanges, with a total of three messages:

- The first message: The initiator recommends SA, to initiate Diffie-Hellman exchange, and send a current number and its IKE identity.
- The second message: The responder accepts SA, authenticates the initiator, sends a current number and its IKE identity, and sends the responder's certificate (if you are using a certificate).
- The third message: The initiator authenticates the responder, and confirms the exchange.

Since the participants' identities are exchanged in the plain text (in the first two messages), the aggressive mode provides no identity protection.

 **Tip:**

When the IPSec tunnel is connected by the other dynamically connecting to the local, dynamically connecting to the gateway, the aggressive mode must be used for negotiations.

➤ **Diffie-Hellman Exchange**

Diffie-Hellman exchange, also known as "DH exchange", allows both parties to generate a shared key. The advantage of this technology is that it allows both parties to create a key on the non-secure media, without having to transmit the pre-shared keys over the network. There are five basic DH groups (the device supports Groups 2 and Group 5), and the size of the main modulus used in the calculation of the groups vary, as described below:

- DH Group 2: 1024-bit modulus
- DH Group 5: 1536-bit modulus

The larger the modulus is, the more secure the generated key is. However, the larger the modulus is, the longer the key generation process takes.

 **Tip:**

Since the modulus size of each DH group is different, therefore both communication parties of the IPSec tunnel must use the same group.

2. Phase II

When both communication parties establish an authenticated secure channel, the second phase will continue to be implemented, and in this phase, IPsec SA will be negotiated to protect user data to be transmitted through the IPsec tunnel.

Similar to the process of the first phase, both parties exchanged proposals to determine the security parameters used in the SA. The second-phase proposal also includes a security protocol (the device currently supports ESP) and the selected encryption and authentication algorithms.

Regardless of the mode used in the first stage, the second stage is always operated in the "fast" mode, and includes the exchange of three messages.

II. Maintenance of security alliances

Once the SA establishment is complete, both parties of IPsec SA must also maintain SA, to ensure that SA is secure and effective. IPsec SA test the effectiveness of SA with the following methods:

1. SA survival time

In the establishment of SA negotiation, the two parties will negotiate the SA's survival time, when such time reaches the pre-set value, the renegotiation is required to establish a new SA. Periodic renegotiation is equivalent to change of passwords on a regular basis.

In the WEB UI mode, you can configure the "Survival time" and "Maximum flow" in the "Advanced options" of *VPN configuration -> IPsec*.

The efficiency of data transfer will be lowered due to the frequent rebuilding SA that needs to consume large amounts of system resources (mainly DH exchanges and generation of current numbers). So the survival time of SA is usually set to relatively long (1 hour to 1 day typically). Within the validity period, the two communicating parties can only "assume" that the other party works normally since they cannot detect each other (similar to the PING function), and in case a party has a foreseeable problem or the network connecting both of them has fault, the other party does not know that the connection line between them is interrupted, and will continue to send data to the other party that does not exist, thus causing a false connection (SA is normal and sends data normally, but is unable to complete the two-way communications), so there must be an effective way to detect that both parties participating in the IPsec SA are fully functional, and the network connection between them is completely normal. The overhead of this testing method is less than that for renegotiating the IPsec SA, so a higher density can be used for test. This technology is IPsec "DPD", which exists as a complement to SA negotiation.

2. DPD (Dead Peer Detect)

IPsec DPD regularly detects SA to find out whether the other party still exists. Within the survival time and maximum flow range of SA, it regularly detects if the other's network is reachable, and the program is normal, so as to find out communications faults caused by network changes or avoid to keep SA with a "Mars people" host that already does not exist. This detection cycle is usually 20 seconds or 1 minutes around, and both parties can detect the other party by sending a "heartbeat" packet. After continuously losing multiple heartbeat packets, IPsec DPD will forcibly initiate a SA negotiation again.

In the WEB UI mode, you can enable the DPD function by selecting the "DPD" option, and determine the test cycle by configuring "heartbeat" in the "Advanced options" of *VPN configuration*—>*IPSec*.

12.2.1.3 IPSec NAT traversal

Due to historical reasons, one of the problems in deploying an IPSec VPN network in the NAT mode lies in the impossibility to locate the IPSec peers after network address translation (NAT). Internet service providers and Small Office/Home Office (SOHO) networks typically use NAT to share a single public IP address. Although NAT helps to save the remaining IP address space, but they also bring troubles to the end-to-end protocols such as IPSec.

One of the main reasons for IPSec disruption caused by NAT is that, for "Encapsulating Security Protocol (ESP)", the NAT devices cannot identify the location (because it has been encrypted) of the Layer 4 header for port translation (the 4th layer). For the "Authentication header (AH)" protocol, the NAT devices can modify the port number, but cannot modify the authentication check, so the authentication check of the entire IPSec packet will fail.

A new technology known as IPSec NAT Traversal (NAT-T) is under standardization by the IPSec network of the Internet Engineering Task Force.

In the IPSec negotiation process, the two peers can be determined automatically according to the following two conditions to support IPSec NAT-T:

- One party (usually a client computer) to initiate the IPSec session and one party to respond to the IPSec session (usually a server) can perform IPSec NAT-T or not.
- Any NAT exists in the path between them.

If both of these conditions are true, then both parties will use IPSec NAT-T to send the IPSec-protected traffic through NAT. If one party does not support IPSec NAT-T, then the IPSec negotiation and IPSec protection are to be performed (after the first two messages). If both parties support IPSec NAT-T, but there is no NAT between them, then the normal IPSec protection is to be performed.

Tip: IPSec NAT-T is only defined for ESP traffic, but AH traffic cannot pass through NAT devices.

The device can use the NAT traversal (NAT-T) function. In the first-phase exchange, NAT-T will add a layer of UDP encapsulation (UDP4500 port is usually used) when it discovers by detecting along the data path that there is one or more NAT devices, and passes through the NAT device.

In the WEB UI mode, the NAT traversal feature can be enabled by selecting "NAT traversal" option in the "Advanced options" of *VPN configuration* ->*IPSec*.

12.2.2 IPsec list

Enter the *VPN configuration->IPsec* page to view the information about associated IPsec tunnels, such as SA status, remote gateway address, remote Intranet address, locally bound interfaces, etc.

ID	Enable	SA Status	Remote Gateway	Remote Subnet	Bind to	Local Subnet	Edit

0/0 Lines/Page 10 First Prev Next Last Goto Page Page Search

Select All

Figure 12_15 IPsec list

⊕ **Tip:** If the IPsec connection mode is "The other party dynamically connects to the local", the "Establish" bLeveloneon is invalid.

12.2.3 IPsec Settings

IPsec supports three ways of connection, namely: gateway to gateway, dynamic connection to the gateway, the other party dynamically connects to the local. The following describes the meaning of the configuration parameters for three types of connection.

When one end of the IPsec tunnel is dynamic IP access (when no DDNS is applied for), "Dynamic connection to the gateway", "The other party dynamically connects to the local" are used at both ends of the tunnel. Here, one end of the dynamic IP access adopts "Dynamic connection to the gateway" and is used as the initiator, and then the other end adopts "The other party dynamically connects to the local" and is used as the responder.

12.2.3.1 Gateway to gateway

The screenshot shows a configuration window for a VPN connection. It is divided into several sections:

- Connection Type:** A dropdown menu set to "Bidirectional".
- Remote:**
 - Gateway IP/Domain Name: [Empty text box]
 - Subnet IP Address: 0.0.0.0
 - Subnet Mask: 255.255.255.0
- Local:**
 - Bind to: WAN1 (dropdown)
 - Subnet IP Address: 192.168.1.1
 - Subnet Mask: 255.255.255.0
- Security Options:**
 - Pre-shared Key: [Empty text box]
 - P2 Encrypt/Auth Algorithms 1: esp-aes128 (dropdown)
- Advanced Options:** A section that is currently collapsed.

At the bottom of the window are four buttons: "Save", "Cancel", "Help", and "Back".

Figure 12_16 Gateway to gateway

- ◆ Connection mode: Here, gateway to gateway is selected.

Remote end

- ◆ Gateway address (domain name): The address of the remote gateway address (or domain name) of the IPSec tunnel. When set to a domain name, a DNS server needs to be configured on the device, and then the device will periodically resolves the domain name. If the IP address is changed, the device will renegotiate the IPSec tunnel again.
- ◆ Intranet address: Any IP address of the Intranet protected at the remote end of the IPSec tunnel, if the remote end is a mobile single user, then fill in the IP address of the device.
- ◆ Network mask: The subnet mask of the Intranet protected at the remote end of the IPSec tunnel, if the remote end is a mobile single user, then fill in 255.255.255.255.

Local

- ◆ Local binding: Select the type of local interfaces, which can be an Ethernet interface or PPTP dial-up interface. If the IPSec tunnel is configured to be bound to the interface, then all packets passing through the interface will be checked by IPSec to determine whether the packet is subject to encryption and decryption operations.
- ◆ Intranet address: Any IP address of Intranet locally protected.

- ◆ Intranet mask: Subnet mask of locally protected Intranet.

Security options:

- ◆ Pre-shared key: Pre-shared key used by negotiation, with the maximum of 128 characters.
- ◆ Encryption and authentication algorithm 1: The preferred encryption and authentication algorithm that can be used for negotiation in the second phase.

Phase 1

Exchange Mode

SA Lifetime Seconds

Encrypt/Auth Algorithms 1

Encrypt/Auth Algorithms 2

Encrypt/Auth Algorithms 3

Encrypt/Auth Algorithms 4

Phase 2

Encrypt/Auth Algorithms 2

Encrypt/Auth Algorithms 3

Encrypt/Auth Algorithms 4

SA Lifetime Seconds

Other Options

Enable Anti-replay

Enable DPD

Heartbeat Interval Seconds

Enable NAT-traversal

Port

Keepalive Frequency Seconds

Figure 12_17 IPSec Advanced options -- Main mode

First phase

- ◆ Negotiation mode: Sets the negotiation mode in the first phase, with the options: main mode and aggressive mode. When selecting gateway-to-gateway connection, select the main mode. When the connection mode is dynamic connection to the gateway, other party dynamically connecting to the local machine, select the aggressive mode.
- ◆ Survival time: Sets the survival time of IKE SA, which is at least 600 seconds. When the remaining time is 540 seconds, the IKE SA will be negotiated again.

- ◆ Encryption and authentication algorithm (1-4): Sets the encryption and authentication algorithm used for negotiation in the first phase. You can select four groups, each of which the combination of different encryption algorithms and authentication algorithms and DH groups.

Phase II

- ◆ Encryption and authentication algorithm (2-4): Sets the encryption and authentication algorithm used for negotiation the second phase, and three groups can be selected, together with a group that has been configured in the basic parameter configuration, so there is a total of four groups.
- ◆ Survival time: Sets the survival time of IPSec SA, which is at least 600 seconds. When the remaining time is 540 seconds, the SA will expire and the IPSec SA will be negotiated again.

Others

- ◆ Anti-replay: Sets whether or not anti-replay is enabled. When enabled, the gateway will support the anti-replay feature, to reject the received packets or copies of packets in order to protect themselves from attacks.
- ◆ DPD: Sets whether to enable DPD. After enabled, the device sends a heartbeat packet on a regular basis to detect whether each other's network is reachable, and whether the program is normal. If multiple heartbeat packets are lost continuously, then IPSec DPD will launch SA negotiation again forcibly.
- ◆ Heartbeat: Sets the time interval for sending heartbeat packets, whose default value is 20 seconds. After configuring this value, the gateway will send detection messages to the peer end at an interval of unit time ("heartbeat"), to determine whether the peer end still survives.
- ◆ NAT traversal: Enables or disables the feature of NAT traversal.
- ◆ Port: Sets the port number of UDP encapsulation packets in NAT traversal, whose default value is 4500.
- ◆ Maintain: After NAT traversal feature is enabled, the device will send a packet to the NAT device to maintain NAT mapping at an interval of unit time ("keep"), so that the NAT mapping needs no change until SA in the first phase and second phase expires. Its default value is 20 seconds.

12.2.3.2 Dynamic connection to the gateway

The screenshot shows a configuration interface for a dynamic connection to a gateway. It is divided into four sections: Connection Type, Remote, Local, and Security Options, with an Advanced Options section at the bottom.

- Connection Type:** A dropdown menu set to "Originate-Only".
- Remote:**
 - Gateway IP/Domain Name: [Empty text box]
 - Subnet IP Address: 0. 0. 0. 0
 - Subnet Mask: 255. 255. 255. 0
 - ID Value: [Empty text box]
 - ID Type: Domain Name (dropdown)
- Local:**
 - Bind to: WAN1 (dropdown)
 - Subnet IP Address: 192. 168. 1. 1
 - Subnet Mask: 255. 255. 255. 0
 - ID Value: [Empty text box]
 - ID Type: Domain Name (dropdown)
- Security Options:**
 - Pre-shared Key: [Empty text box]
 - P2 Encrypt/Auth Algorithms 1: esp-aes128 (dropdown)
- Advanced Options:** [Section header]

At the bottom of the form are four buttons: Save, Cancel, Help, and Back.

Figure 12_18 Dynamic connection to the gateway

The parameters described in the "gateway to gateway" connections are no longer to be described again one by one.

- ◆ Connection mode: Here, dynamic connection to the gateway is selected. In this case, this device can only be used as the initiator when establishing an IPSec tunnel, and the IPSec tunnel should have the aggressive mode selected at both ends for the IKE negotiation in the first phase.

Remote end

- ◆ Identity ID: Sets the identity ID used to authenticate remote ends.
- ◆ Identity type: The type of remote identity ID, including three options: "Email address", "Domain name" and "IP address".

Local

- ◆ Identity ID: Identity ID sent locally to the remote end for authentication.
- ◆ Identity type: The type of local identity ID, including three options: "Email address",

"Domain name" and "IP address".

12.2.3.3 Other party dynamically connects to local machine

Connection Type	Answer-Only
Remote	
Gateway IP/Domain Name	0.0.0.0
Subnet IP Address	0.0.0.0
Subnet Mask	255.255.255.0
ID Value	
ID Type	Domain Name
Local	
Bind to	WAN1
Subnet IP Address	192.168.1.1
Subnet Mask	255.255.255.0
ID Value	
ID Type	Domain Name
Security Options	
Pre-shared Key	
P2 Encrypt/Auth Algorithms 1	esp-aes128
Advanced Options	
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/> <input type="button" value="Back"/>	

Figure 12_19 Other party dynamically connects to local machine

The parameters for the other party to dynamically connect to local machine has been described in the previous two sections, so there is no need to repeat any more. When selecting "Other party dynamically connects to the local", the remote gateway address (domain name) needs not be configured. In this case, this device can only be used as the responder in establishing an IPSec tunnel, and the IPSec tunnel should have the aggressive mode selected at both ends for the IKE negotiation in the first phase.

12.2.4 IPSec configuration instance

12.2.4.1 Gateway to gateway

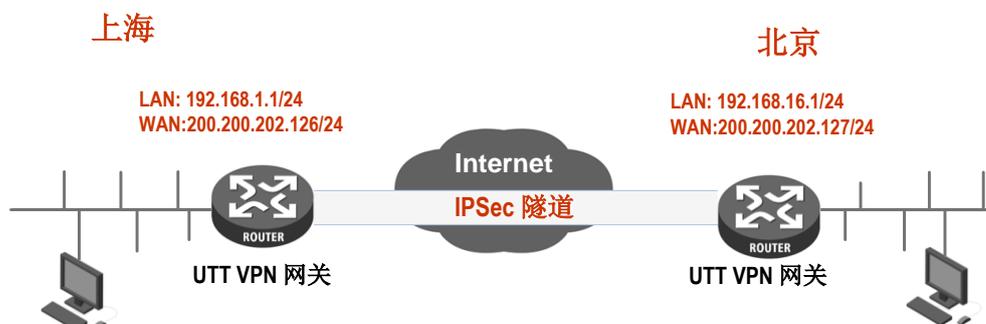


Figure 12_20 Gateway to gateway topology

Requirements:

In this scenario, a company is based in Shanghai. It has a branch office in Beijing, and hopes to achieve a mutual access to the internal resources of the LAN in two places. This scenario uses the IPSec protocol to establish VPN tunnels, and the HiPER router is used by the VPN gateway in two places at the following addresses:

Shanghai gateway:

Intranet network segment: 192.168.1.0/24.

LAN IP address: 192.168.1.1/24.

WAN1 domain name: 200.200.202.126/24.

Beijing gateway:

Intranet network segment: 192.168.16.0/24.

LAN IP address: 192.168.16.1/24.

WAN1 IP address: 200.200.202.127/24.

The configuring steps are follows:

1. Configure Shanghai gateway

Connection Type	Bidirectional ▼
Remote	
Gateway IP/Domain Name	200.200.202.127
Subnet IP Address	192.168.16.1
Subnet Mask	255.255.255.0
Local	
Bind to	WAN1 ▼
Subnet IP Address	192.168.1.1
Subnet Mask	255.255.255.0
<hr/>	
Security Options	
Pre-shared Key	••••••
P2 Encrypt/Auth Algorithms 1	esp-aes128 ▼
<hr/>	
<u>Advanced Options</u>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/> <input type="button" value="Back"/>	

Figure 12_21 Gateway to gateway configuration 1

Remote gateway address is set as the WAN IP address of Beijing gateway, 200.200.202.127, and remote Intranet address is the LAN IP address of Beijing gateway, 192.168.1.1, which is locally bound at WAN1 port. Set the preshared key for the first phase to testing, and the encryption and authentication algorithms for the second phase is esp-ase-128.

2. Configure Beijing gateway

Connection Type	Bidirectional ▼
Remote	
Gateway IP/Domain Name	200.200.202.126
Subnet IP Address	192.168.1.1
Subnet Mask	255.255.255.0
Local	
Bind to	WAN1 ▼
Subnet IP Address	192.168.16.1
Subnet Mask	255.255.255.0
Security Options	
Pre-shared Key	*****
P2 Encrypt/Auth Algorithms 1	esp-aes128 ▼
<u>Advanced Options</u>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/> <input type="button" value="Back"/>	

Figure 12_22 Gateway to gateway configuration 2

Remote gateway address is set as the WAN IP address of Shanghai gateway, 200.200.202.126, and remote Intranet address is the LAN IP address of Shanghai gateway, 192.168.1.1, which is locally bound at WAN1 port. Set the preshared key for the first phase to testing, and the encryption and authentication algorithms for the second phase is esp-ase-128.

View connection status:

Enter the corresponding pages respectively, to view the IPSec instance connection information. As shown in the figure below, you can view the SA status, remote gateways, remote Intranet, local binding interfaces, and other information of the IPSec instances.

12.2.4.2 Dynamic on one party



Figure 12_25 "Dynamic on one party" topology

Requirements:

In this scenario, a company is based in Shanghai. It has a branch office in Beijing, and hopes to achieve a mutual access to the internal resources of the LAN in two places. This scenario uses the IPsec protocol to establish VPN tunnels, and the HiPER router is used by the VPN gateway in two places at the following addresses:

Shanghai gateway:

Intranet network segment: 192.168.1.0/24.

LAN IP address: 192.168.1.1/24.

WAN domain name: 200.200.202.126/24.

Beijing gateway:

Intranet network segment: 192.168.16.0/24.

LAN IP address: 192.168.16.1/24.

IP address of WAN1 port: Acquired dynamically.

The configuring steps are follows:

1. Configure Shanghai gateway

Connection Type	Originate-Only ▾
Remote	
Gateway IP/Domain Name	0. 0. 0. 0
Subnet IP Address	192. 168. 16. 1
Subnet Mask	255. 255. 255. 0
ID Value	test@com. cn
ID Type	Email Address ▾
<hr/>	
Local	
Bind to	WAN1 ▾
Subnet IP Address	192. 168. 1. 1
Subnet Mask	255. 255. 255. 0
ID Value	test. levelone. com. cn
ID Type	Domain Name ▾
<hr/>	
Security Options	
Pre-shared Key	••••••
P2 Encrypt/Auth Algorithms 1	esp-aes128 ▾
<hr/>	
<u>Advanced Options</u>	
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/> <input type="button" value="Back"/>	

Figure 12_26 Dynamic on one party - The other party dynamically connects to local machine

Set the connection mode to the other party dynamically connecting to the local machine, and Beijing gateway dynamically connecting to Shanghai gateway. Meanwhile, set the Beijing gateway information, such as Intranet addresses, identity ID. Locally bound at WAN1 port, set the preshared key for the first phase to testing, and the encryption and authentication algorithm for the second phase is esp-ase-128.

2. Configure Beijing gateway

Connection Type

Remote

Gateway IP/Domain Name

Subnet IP Address

Subnet Mask

ID Value

ID Type

Local

Bind to

Subnet IP Address

Subnet Mask

ID Value

ID Type

Security Options

Pre-shared Key

P2 Encrypt/Auth Algorithms 1

Advanced Options

Figure 12_27 Dynamic on one party - Dynamically connects to the gateway

Sets the connection mode of Beijing gateway to a dynamic connection to the gateway. Meanwhile, sets up Shanghai gateway - related information, such as gateway address, Intranet address, identity ID. Locally bound at the WAN1 port, set the preshared key for the first phase to testing, and the encryption and authentication algorithm for the second phase is esp-ase-128.

View the connection status:

IPSec List 3/50

1/1 Lines/Page 10 First Prev Next Last Goto Page Page Search

ID	Enable	SA Status	Remote Gateway	Remote Subnet	Bind to	Local Subnet	Edit
<input type="checkbox"/> ID1	<input checked="" type="checkbox"/>	Unestablished	200.200.202.127	192.168.16.1	WAN1	192.168.1.1	
<input type="checkbox"/> ID2	<input checked="" type="checkbox"/>	Unestablished	200.200.202.126	192.168.1.1	WAN1	192.168.16.1	
<input type="checkbox"/> ID3	<input checked="" type="checkbox"/>	Unestablished	0.0.0.0	192.168.16.1	WAN1	192.168.1.1	

Select All

Figure 12_28 IPSec connection status -- Other party connects to local host dynamically

IPSec信息列表 1/4

1/1 每页显示行数 10 第一页 上一页 下一页 最后一页 前往 第 页 搜索

ID	允许	SA状态	远端网关	远端内网	本地绑定	本地内网	编辑
<input type="checkbox"/> ID1	<input checked="" type="checkbox"/>	已建立	200.200.202.126	192.168.1.1	WAN1	192.168.16.1	

全选 / 全不选

Figure 12_29 IPSec connection status -- Connect to local host dynamically

Chapter 13. System

In the *System Management* main menu, you can enter the *Administrator configuration, Language selection, clock management, configuration management, software upgrade, remote management, scheduled task* page. This chapter mainly describes how to change administrator user name and password. How to set the device clock. How to back up and import configuration files. How to upgrade the device. How to enable remote management, etc.

13.1 Administrator

1. Administrator list

The screenshot shows the 'Administrator List' interface. At the top right, it indicates '1/5' pages. Below the title bar, there are navigation controls: '1/1', 'First', 'Prev', 'Next', 'Last', 'Goto', 'Page' (with an input field), 'Page', and 'Search' (with an input field). The main area is a table with two columns: 'User Name' and 'Edit'. The first row contains the user 'admin' and an 'Edit' link with a pencil icon and a trash icon. Below the table, there is a 'Select All' checkbox and three buttons: 'Add', 'Delete All', and 'Delete'.

Figure 13-1 Administrator list

2. Administrator Settings

The screenshot shows the 'Administrator Settings' form. It contains three input fields: 'User Name *', 'Password *', and 'Confirm Password *'. Below the fields is a note: 'Note: To ensure security, it is strongly recommended that you change the default administrator password and keep it safe. The user name can only contain letters, numbers and underscores (_); and it must be at most 31 characters long.' At the bottom, there are four buttons: 'Save', 'Cancel', 'Help', and 'Back'.

Figure 13-2 Administrator Settings

- ◆ User name: Customizes the user name of the administrator who logs in the WEB interface.
- ◆ Password, confirming password: Customizes the password of the administrator who logs in the WEB interface.

3. Modification of administrators' factory user name, password

For security reasons, we strongly recommend to modify the initial administrator user name and password, and to keep them with care.

Enter into the *System Management-> Administrator configuration* page, click on the edit icon with the user name of "admin", and enter into the configuration page to modify the factory user name and password for login. After modification, you must use the new user name and password to log into the device.

13.2 Language

This section describes the *System management-> Language selection* page. Select the device's WEB interface language through the configuration in this page.

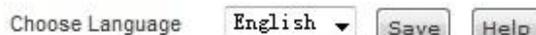


Figure 13_3 Language

13.3 Time

This section describes the *System > Time* page.

In order to guarantee that the functions of the device relating to time work normally, the clock of the device needs to be accurately set, to make it synchronize with the local standard time.

The device provides two ways of setting system time, "Manual setup time" and "Network time synchronization". It is recommended to use the "Network time synchronization" function to obtain the standard time from the Internet, and the device will automatically get the standard time from the Internet after it connects to the Internet in startup.

Current System Time Date 2016-1-22 Time 17:54:36

Time Zone UTC+0800(Beijing,Chongqing,Hongkong,Urumchi)

Set Time Manually 2016 1 22 Day 17:54:36
 Year Month

Synchronize with SNTP Server

DST

SNTP Server 1 IP * 192.43.244.18

Server 2 IP Address * 216.45.57.38

Server 3 IP Address 0.0.0.0

Note : To ensure that SNTP operates properly, you should select the correct time zone

Figure 13-4 Time

- ◆ Current system time: Displays the current date and time information of the device (unit: Y-M-D, H:M:S).
- ◆ Time zone selection: Selects the international time zone in which the device resides. Only choosing a correct time zone can the network time synchronization function work properly.
- ◆ Manual time setting: Manually enters the current date and time (unit: Y-M-D, H:M:S).
- ◆ Network time synchronization: After using the network time synchronization function to set up a right NTP server, and when the device is connected to the Internet, it will automatically synchronize the time with the set NTP server. The addresses of two NTP servers preset by the system by default are 192.43.244.18, 216.45.57.38, which generally requires no change. If you need to know more about the NTP knowledge and the server, just visit <http://www.ntp.org>.

⊕ **Tip:**

It is recommended to set the device clock to synchronize with network time. Only when the system time is properly configured can the settings related to time, such as firewall, etc. work normally!

13.4 Configuration

This section describes the configuration methods of *System -> Configuration*. In this page, you can back up the current configuration files to a local PC, import the new configuration file to the device and restore the factory settings of the device.

The screenshot shows a web interface for configuration management. At the top, there is a section for 'Backup Configuration to Local PC' with a 'Save' button. Below that is the 'Import Configuration' section, which includes a checked checkbox for 'Reset to Defaults before Importing', a text input field for 'Select a Configuration File', a 'Browse...' button, and an 'Import' button. At the bottom of this section, there is a 'Reset to Factory Defaults' section with 'Reset' and 'Help' buttons.

Note: After performing the reset operation, you must restart the Device for the default settings to take effect. This operation will clear all custom settings, so you'd better backup the current configuration before resetting.

Figure 13-5 Configuration management

1. Back up configuration files

Click the <Save> button in the above figure, to back up the configuration files to the local PC, and the format of the configuration file is .xml.

2. Import configuration files

In the above figure, click < Browse ... >, and select the configuration files stored on the local PC. Then click <Import> again. If you have checked the check box "Restore factory settings before import", click the <Import> button, and the device will be restored to the factory settings.

Tip: Do not cut off the device's power supply in loading configuration, to avoid unexpected errors.

3. Restore to factory settings of the device

If users need to restore the device to its factory settings, enter into the *Systems management -> Configuration management* page, and click <Restore>.

Tip:

1. It is strongly recommended that before restoring the factory settings, first back up its configuration files.
2. After clicking <Restore>, the device continues to run in the current configuration, and it needs to be restarted manually to restore it to its factory settings.
3. The user name and password of the device's factory administrator are as follows: admin, and the default LAN IP address/subnet mask is: 192.168.1.1/ 255.255.255.0.

13.5 Firmware Upgrade

This section describes the *System > Firmware Upgrade* page and the software upgrading procedure. In this page, you can view the information of the currently running version, and download the latest version of software from the LEVELONE official website.

The screenshot shows a web interface for firmware upgrade. It displays the following information and controls:

- Hardware Version:** V1.0
- Firmware Version:** GBR-4001v1.7.0-160119
- [Download Firmware](#) (blue hyperlink)
- Select a Firmware File:** A text input field followed by a **Browse...** button.
- Restart after Upgrade:** A checkbox that is checked.
- Upgrade** and **Help** buttons.

Below the form, there are two lines of instructional text:

- The firmware upgrade file must match the current hardware version. You'd better go to System > Configuration page to backup the current system configuration before upgrade.
- To avoid unrecoverable errors, Do NOT turn off the power during upgrading.

Figure 13_6 Firmware Upgrade

- ◆ **Version information:** Displays the information of the current hardware version, software version used by the device.
- ◆ **Download the latest version:** Links to the official website of LEVELONE to download the latest version of the software.

Upgrading steps:

Step 1: Download the latest version of software

Click on the hyperlink "Download the latest version" and go to the official site of LEVELONE to download the latest version of the software to your local PC.

⊕ **Tip:**

1. Please select the most appropriate type of the latest software. The applicable hardware version for the downloaded software must be consistent with the hard versions of the current products.
2. It is recommended that before upgrading, enter into *Systems management -> Configuration management* to back up the current configuration of the system.

Step 2: Select the path where the upgraded software resides

In the "Select the upgrade file" text box, enter the path for upgrading the software on the local PC,

or select the new software on the local PC by clicking < Browse ... >.

Step 3: Update device software

After selecting the software, click on the <Upgrade> button, to update the device software.

Tip:

1. It is strongly recommended to upgrade when the device load is low (less users).
2. Upgrading device software on a regular basis enables the device to get more functions or to have a better working performance. The right software upgrading will not change the current device settings.
3. During the upgrading process, the device's power supply cannot be cut off; otherwise, it will cause unpredictable errors and even irreversible damages to the hardware.
4. After the completion of upgrading, the software will be automatically restarted to take effect, without the need of human intervention.

13.6 Remote Management

This section describes the *System -> Remote management* page. To facilitate the network maintenance by remote administrators on this page, you can configure the remote management function of the device in the *Systems management -> Remote administration* page.



Enable HTTP

It allows you to manage the Device from anywhere over the Internet. URL format: http://IP address: port.

Management Port *

Note: To ensure security, you'd better not enable HTTP remote management unless necessary.

Figure 13_7 Remote Management

- ◆ Enable HTTP: Allow or disallow to manage the device from the Internet through the WEB interface, and the default WEB management external port of the device is 8081. To manage the device from the Internet through the WEB interface, you must use the mode of "IP address: Port" (For instance http://218.21.31.3:8081) to log on to the device.
- ◆ External port: Changes the default external port (default is 8081) of the device. Note that after the port is changed to 80, a TCP80 port mapping will be added in the "Static NAT mapping list" of *Advanced Configuration->NAT and DMZ configuration*, at this point, it will cause a conflict if the mapping to the Intranet WEB server is to be added.

⊕ **Tip:**

1. The device's Internet address can be obtain from the "Line connection information list" of *Network configuration -> WAN port configuration*.
2. If "WAN1" adopts PPPoE dial-up, its IP address is dynamic, and you can configure the DDNS function in the *Network parameters -> DDNS configuration*.
3. For security purposes, unless absolutely necessary, do not enable the remote management function. In looking for LEVELONE's customer service engineer's service, please enable the remote management function.

13.7 Scheduled task

This section describes the *System management-> Scheduled task* page. By configuring scheduled tasks, administrators can predefine the actions completed by the device at a specified time.

1. List of scheduled tasks

The scheduled task list is an editable list. You can operate the instances in the list.

The screenshot displays the 'Scheduled Task List' page. At the top, there are two tabs: 'Scheduled Task' (selected) and 'Scheduled Task Settings'. Below the tabs is a header bar with 'Scheduled Task List' on the left and '0/5' on the right. A navigation bar contains buttons for '0/0', 'First', 'Prev', 'Next', 'Last', 'Goto', 'Page' (with an input field), 'Page', and 'Search' (with an input field). The main area is a table with the following columns: 'Task Name', 'Repeat', 'Start Time', and 'Task Content'. The table is currently empty. At the bottom of the page, there is a 'Select All' checkbox, and three buttons: 'Add', 'Delete All', and 'Delete'.

Figure 13_8 Scheduled task list 1

计划任务信息列表			
1/1 第一页 上一页 下一页 最后一页 前往 第 <input type="text"/> 页 搜索 <input type="text"/>			
启动类型	运行时间	任务内容	编辑
每星期	星期一 23:59:00	重启设备	 

全选 / 全不选

Figure 13_9 Scheduled task list 2

2. Description of scheduled task parameters

Scheduled Task	Scheduled Task Settings
<p>Task Name * <input type="text"/></p> <p>Repeat <input type="text" value="Weekly"/></p> <p>Start Time <input type="text" value="Monday"/> <input type="text" value="00"/> : <input type="text" value="00"/> : <input type="text" value="00"/></p> <p>Task Content <input type="text" value="Restart"/></p> <p><input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/> <input type="button" value="Back"/></p>	

Figure 13-10 Scheduled Task Settings

- ◆ Task name: Name of the custom tasks.
- ◆ Startup type: Indicates time cycle, and the options are: per week, per day, per hour, per minute.
- ◆ Running time: Means the specific time for implementing these tasks and its settings vary based on different startup types.
- ◆ Task content: Selects the appropriate task content.

Chapter 14.

System

In System status, you can easily view the running state of the device, and the system information and history of the device.

14.1 Interface Status

The running status page described in this section is the same as 5.2 Interface status, so it is not to be detailed again here.

14.2 System information

In the *System status* -> *System information* page, network administrators can understand the system-related information and view the system history. Through system information, network administrators can understand the problems occurring to the network or the potential ones, which helps improve the network performance and enhance network security.

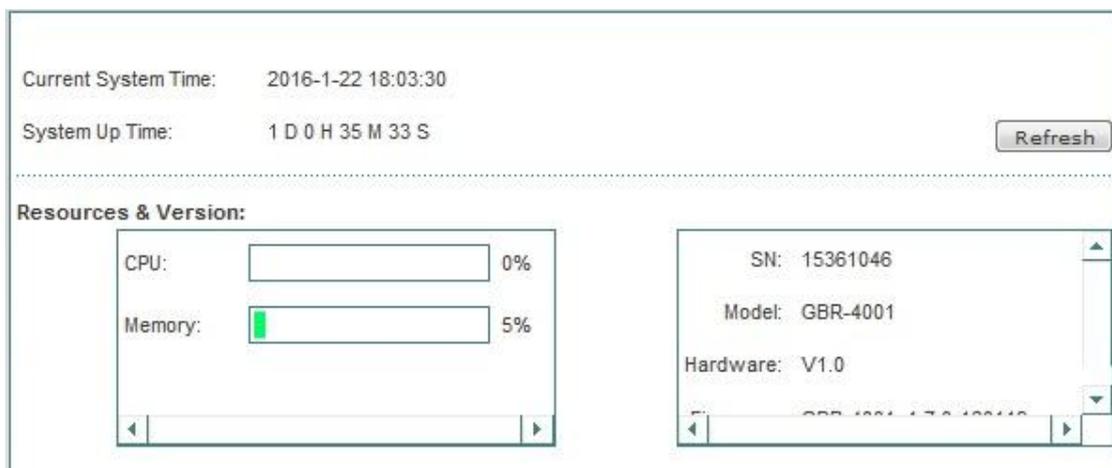


Figure 14_1 System information

◆ Current system time: Displays the current date and time information of the device (Unit: Y-M-D, H:M:S).

-
- ◆ System running time: Displays the time from starting of the device at this time to viewing the time.
 - ◆ CPU utilization: Shows the percentage of the current CPU utilization.
 - ◆ Memory usage: Shows the percentage of the current memory usage.
 - ◆ Serial number: Shows the internal serial number of product (which may be different from the surface serial number).
 - ◆ Device model: Displays the product model of the device.
 - ◆ Hardware version: Displays the hardware version number of the device.
 - ◆ Software version: Displays the software version number of the device.
 - ▶ Refresh: Click <Refresh>, to view the latest system information.

⊕ **Tip:**

Figure 14_1 The usage of CPU, memory is different and the displayed colors are different:

- Green when the usage is (0, 50%).
- Orange when the usage is (50%, 70%).
- Red when the usage is (70%, 100).

14.3 System log

In the *System status* -> *System log* page, network administrators can view the system-related log information and configure the log management.

14.3.1 System log information

```

Jan 22 17:36:51 pluto[24570]: WARNING: 1DES is enabled
Jan 22 17:36:51 pluto[24570]: LEAK_DETECTIVE support [enabled]
Jan 22 17:36:51 pluto[24570]: SAref support [disabled]: Protocol not available
Jan 22 17:36:51 pluto[24570]: SAbind support [disabled]: Protocol not available
Jan 22 17:36:51 pluto[24570]: NSS support [disabled]
Jan 22 17:36:51 pluto[24570]: HAVE_STATSD notification support not compiled in
Jan 22 17:36:51 pluto[24570]: Setting NAT-Traversal port-4500 floating to on
Jan 22 17:36:51 pluto[24570]:   port floating activation criteria nat_t=1/port_float=1
Jan 22 17:36:51 pluto[24570]:   NAT-Traversal support [enabled]
Jan 22 17:36:51 pluto[24570]: using /dev/urandom as source of random entropy
Jan 22 17:36:51 pluto[24570]: ike_alg_register_enc(): Activating OAKLEY_TWOFISH_CBC_SSH:
Ok (ret=0)
Jan 22 17:36:51 pluto[24570]: ike_alg_register_enc(): Activating OAKLEY_TWOFISH_CBC: Ok
(ret=0)
Jan 22 17:36:51 pluto[24570]: ike_alg_register_enc(): Activating OAKLEY_SERPENT_CBC: Ok
(ret=0)
Jan 22 17:36:51 pluto[24570]: ike_alg_register_enc(): Activating OAKLEY_AES_CBC: Ok
(ret=0)
Jan 22 17:36:51 pluto[24570]: ike_alg_register_enc(): Activating OAKLEY_BLOWFISH_CBC: Ok
(ret=0)
    
```

Figure 14_2 System information

The common log information displayed in the device is as follows:

Content of logs	Details	Meaning of information
DHCP:IP conflicted	arp:[IP address]	Means DHCP address conflicts: The device discovers the IP address already existing in the Intranet when its DHCP Server is ready to assign it to a user, at this point, the system will assign another IP address to the user.
ARP	Spoof mac [MAC address] New IP [IP address] mac [MAC address] Old IP [IP address] mac [MAC address]	Means the spoofing of gateway addresses. The MAC address table learns a new MAC address again. MAC address times out and ages.
PPPoE	Local IP address [IP address] Primary DNS address [primary DNS address] Secondary DNS address[backup DNS address]	IP address issued under the PPPoE dial-up. Primary DNS address issued by PPPoE dial-up. Backup DNS address issued by PPPoE dial-up.

notice	Give notice to user: [IP address]	Push notification messages to the IP address.
--------	-----------------------------------	---

Figure 14- 1 Log information

14.3.2 Log Management Settings

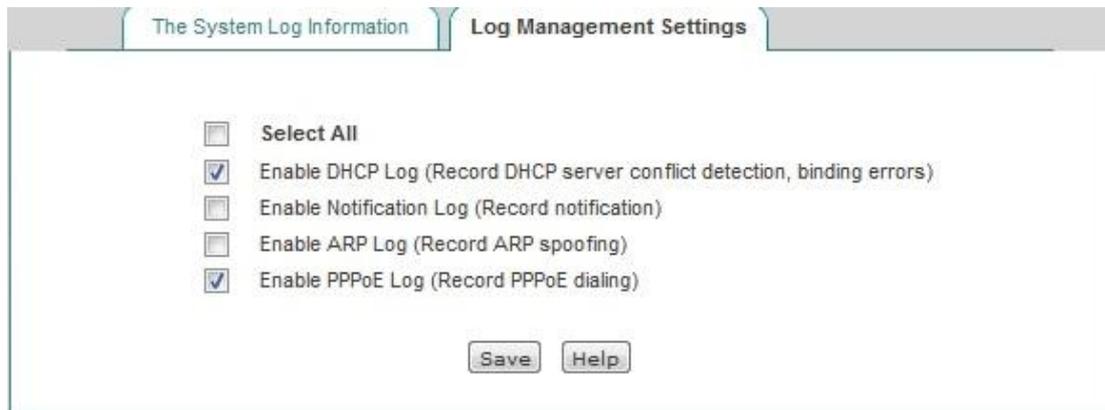


Figure 14_3 Log Management Settings

- ◆ Enable DHCP logging: Check to enable DHCP logging, for recording the conflicts of the DHCP server and DHCP Distribute the address conflicts, and other messages.
- ◆ Enable notification logging: Check to enable notification logging, recording the notification log information.
- ◆ Enable ARP logs: Check to enable the ARP logging, and record the information of ARP cheat.
- ◆ Enable PPPoE logging: Check to enable PPPoE logging, recording the PPPoE dial-up log information.

Chapter 15.

Customer service

On the Customer service page, you can easily link to LEVELONECare, Product discussion, Knowledge base, Appointment service and other columns of the LEVELONE company's official website, so that you can get to know LEVELONE services system in a faster way, and enjoy its intimate services.

- **LEVELONECare**– Link to the customer service page of LEVELONE's official website, to acquire customer services and technical supports.
- **Product Discussion**– Link to the discussion forums of LEVELONE's official website to participate in discussions about the product.
- **Knowledge Base**– Link to the knowledge base of LEVELONE's official website for searching related technical information.
- **Booking Service**– Link to the booking service page of LEVELONE's official website, for advance reservation of the customer service in a certain working period.

Appendix A Configuration of LAN computers

This chapter describes how to configure the TCP/IP properties of the computer in the Windows XP environment.

Step I Check network IP status

1. Click "Start" → "Control panel".
2. Double click on the "Network connections" icon, right click on "Local connection" and select "Properties". In the "Local connection Properties" → "This connection uses the following items", check to see if TCP/IP is already installed, as shown in Figure A-1, and if there is "Internet Protocol (TCP/IP)" option, this means that it is already installed:

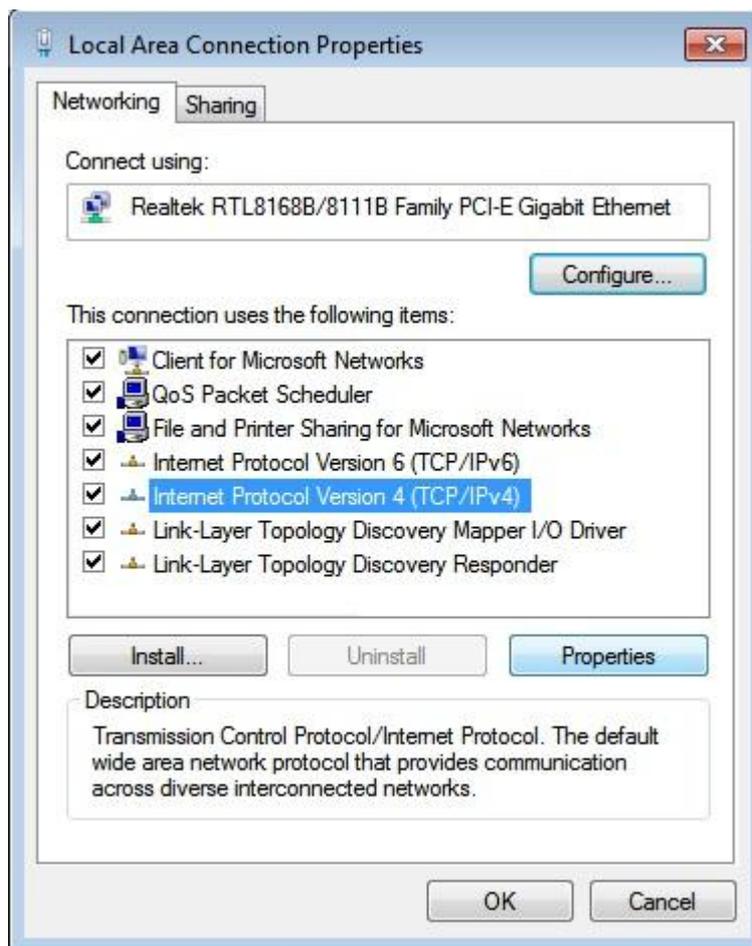


Figure A-1 Network configuration window

3. If the TCP/IP is not installed, first install the TCP/IP, and select "Internet Protocol (TCP/IP)"

in the "Local connection Properties" and click "Install (R)" bLeveloneon, to install the TCP/IP. After adding the TCP/IP, you need to restart the computer to update the system's network settings for it to take effect.

Step II Configure TCP/IP properties

The following introduces the steps for configuring TCP/IP properties in two cases, setting IP addresses manually and setting IP addresses by DHCP server.

Method I Manually setting the IP address

1. Click "Start" → "Control panel".
2. Double-click the "Network connections" icon, right-click the "Local connection", select Properties, enter the "Local connection Properties" window, as shown in Figure A-1, select "Internet Protocol (TCP/IP)" option in "This connection uses the following items" , and then click the "Properties" bLeveloneon.
3. Enter the "Internet Protocol TCP/IP properties" window, select "Use the following IP address" in the General tab, as shown in Figure A-2, and then type in: 192.168.1.X (X is between 2 and 254) in the "IP address", type in 255.255.255.0 in the "Subnet mask", and type in 192.168.1.1 in the "Gateway address".
4. Select the "Use the following DNS server addresses" option, as shown in Figure A-2. Type in the IP address (which can be provided by the ISP) of the DSN server provided by the ISP in the "Preferred DNS server", and the "Standby DNS server" is optional. When the preferred DNS cannot be connected, the device automatically uses the standby DNS server. Click the "OK" bLeveloneon, and the TCP/IP properties are configured successfully.

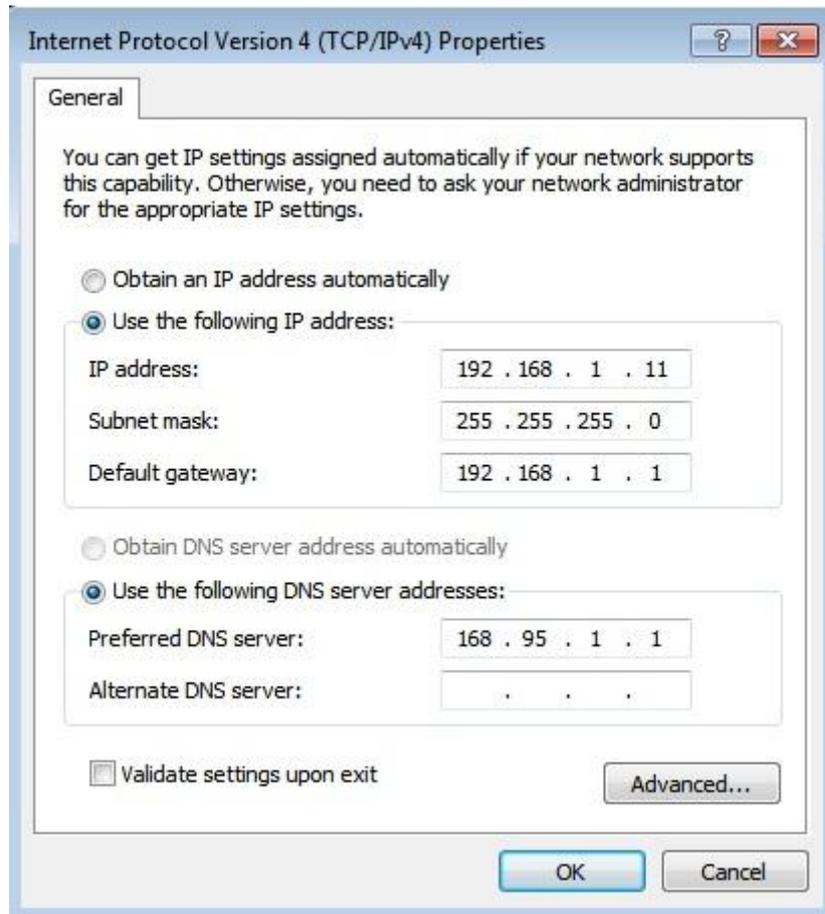


Figure A-2 TCP/IP properties IP address configuration window

Method II Setting IP addresses by the DHCP server

1. Before using this feature, you must ensure that the DHCP Server function is activated in the *Network parameters* -> *DHCP server* of the device.
2. Click "Start" → "Control panel".
3. Double-click the "Network connections" icon, right-click the "Local connection", select Properties, enter the "Local connection Properties" window, as shown in Figure A-1, select "Internet Protocol (TCP/IP)" option in "This connection uses the following items", and then click the "Properties" button.
4. Enter the "Internet Protocol TCP/IP properties" window, as shown in Figure A-2, and select "Obtain the IP address automatically" and "Obtain the DNS server address automatically" in the General tab.
5. The above configuration is completed; click the "OK" button, to complete the configuration of the TCP/IP properties.

Appendix A FAQ

B-1. How ADSL users go online?

1. First, set the ADSL Modem to Bridge mode (1483 bridge mode).
2. Confirm that the PPPoE line is a standard dial-up type (you can use the PPPoE dial-up software that comes with the computer system for testing).
3. Connect the ADSL Modem to the WAN port of the device with a network cable, and connect the telephone cord to the Line port of the ADSL Modem.
4. In the *Network parameters -> WAN configuration*, you can configure the parameters related to PPPoE Internet line.
5. If you are an Internet user paying a monthly package fee, you can select the type of dial-up as "Auto dial". If not, you can select the type of dial-up as "Dial on demand" or "Manual dial", and you can type in the idle time to prevent forgetting line breakage and wasting time.
6. If "Manual dial-up" is selected, you can dial up manually in the "Line connection information list" of the *Network parameters -> WAN configuration*.
7. After a successful dial-up, you can view the configuration and status information (Figure B-1) of the line in the "Line connection information list" of the *Network parameters -> WAN configuration* page, such as "Connection status" (which is displayed as "Connected" after a successful dial-up), the "IP address" assigned by ISP, and other information.

Internet Connection List							4/4	
1/1	First	Prev	Next	Last	Goto	Page <input type="text"/>	Page	Search <input type="text"/>
Interface	Connection Type	Status		IP Address	Subnet Mask	Gateway IP	R	
WAN1	PPPoE	Connected	7Hours47Minute49Seconds	118.166.197.63	255.255.255.255	168.95.98.254		
WAN2	DHCP	Connected	24Hours43Minute18Seconds	192.168.10.57	255.255.255.0	192.168.10.1		
WAN3	Static IP	Connected		111.111.111.12	255.255.255.0	111.111.111.1		
WAN4	DHCP	Disconnected						

Figure B- 1 Line connection information list - View the PPPoE dial-up line information

Interface: WAN1

Connection Type: PPPoE

ISP Policy: ISP Policy

User Name*: 84685158@hinet.net

Password*: ●●●●●●●●

PPP Authentication: EITHER

Dial Type: Always On

Dial Mode: Normal Mode

Idle Timeout*: 0 Minutes

MTU*: 1480 Byte
(MTU Range: 1-1492)

Advanced Options (MAC address, etc.)

Save Cancel Help

Figure B- 2 PPPoE dial-up configuration

8. Configure the LAN computer as described in Appendix A of this manual.

B-2. How the Fixed IP access users go online?

1. Confirm that the line is normal (which can be tested by a PC).
2. Connect the WAN port of the device to the ISP network device with a network cable.
3. In the *Network parameters -> WAN configuration* page, configure the parameters of the fixed IP access line.
4. Configure the LAN computer as described in Appendix A of this manual.

B-3. How the Dynamic IP (Cable Modem) access users go online?

1. Confirm that the line is normal (which can be tested by a PC).

2. Connect the WAN port of the device to the ISP network device with a network cable.
3. In the *Network parameters -> WAN configuration* page, configure the parameters of the dynamic IP access line.

 **Tip:**

When some dynamic IP is connected (such as a cable modem), Cable Modem will record the MAC address of the network devices (such as network adapters) originally used the line, this will cause the device to fail to obtain IP addresses normally, in this case, the WAN port MAC address of the device needs to be set to be the same as that of the original network device. In the *Network parameters -> WAN configuration*, Click on the "Advanced options" to modify the MAC address of the WAN port to that of the former network device, and click <Save>.

4. In the "Line connection information list" of *Network parameters -> WAN configuration*, you can view the configuration and status information for the line (Figure B-3) when a dynamic IP is connected, such as "Connection status" (which is displayed as "Connected" in normal connection, with the connection time displayed), the ISP-assigned "IP address", the uplink rate and downlink rate and other information.

Internet Connection List						4/4		
1/1	First	Prev	Next	Last	Goto	Page <input type="text"/>	Page <input type="text"/>	Search <input type="text"/>
Interface	Connection Type	Status		IP Address	Subnet Mask	Gateway IP	R	
WAN1	PPPoE	Connected 7Hours47Minute49Seconds		118.166.197.63	255.255.255.255	168.95.98.254		
WAN2	DHCP	Connected 24Hours43Minute18Seconds		192.168.10.57	255.255.255.0	192.168.10.1		
WAN3	Static IP	Connected		111.111.111.12	255.255.255.0	111.111.111.1		
WAN4	DHCP	Disconnected						

Figure B- 3 Line connection information list - View the information of dynamic IP access line

5. Configure the LAN computer as described in Appendix A of this manual.

B-4. How to restore the device to its factory settings?

 **Tip:** The following method is used to delete all original settings of the device, so please use it with care.

The following describes the method to restore the device to its factory settings by knowing the administrator password and forgetting the administrator password respectively.

Case I: Knowing the administrator password

If you know the administrator password, you can restore the factory settings through the WEB interface. The steps are as follows: Directly enter the *System management- > Configuration*

management page, and then click the “Restore” button in the column of “Restore factory settings” to manually restart the device, to restore the device to its factory settings.

Case II: Forget the administrator password

If you forget the administrator password, you will not be able to enter the WEB interface, and now you can only use the Reset button to restore the factory settings of the device. The steps are as follows: In the process of the device's charged operation, hold down the Reset button for more than 5 seconds, and then release the button, the device will be restored to its factory settings, and automatically restarted.

Appendix B Figure Index

Figure 2_1 Front Panel - GBR-4001.....	4
Figure 2_2 Rear Panel - GBR-4001	4
Figure 2_3 Product rack installation drawing I	6
Figure 2_4 Product rack installation drawing II	7
Figure 2_5 Establish a connection to LAN and WAN.....	7
Figure 3_1 WEB login interface.....	10
Figure 3_2 Homepage of the WEB interface.....	10
Figure 4_1 Home page of configuration wizard.....	12
Figure 4_2 Configuration Wizard - Dynamic IP access.....	13
Figure 4_3 Configuration Wizard - Static IP access.....	13
Figure 4_4 Configuration wizard - PPPoE access	14
Figure 5_1 Information about Interface status.....	15
Figure 5_2 Interface Traffic.....	16
Figure 5_3 Restart device.....	17
Figure 6_1 Configuration of WAN port	19
Figure 6_2 Static IP access	20
Figure 6_3 PPPoE access.....	21
Figure 6_4 Internet Connection List	22
Figure 6_5 Internet Connection List information (Continued Figure 6_4).....	23
Figure 6_6 Internet Connection List - PPPoE access.....	24
Figure 6_7 Internet Connection List - Dynamic IP access	24
Figure 6_8 Full Load Balancing.....	27
Figure 6_9 Partial Load Balancing	27
Figure 6_10 Load Balancing List.....	28
Figure 6_11 Detection and Bandwidth.....	29
Figure 6_12 Enabling identity binding	30
Figure 6_13 Configuration of LAN port.....	30
Figure 6_14 Configuration of DHCP service	32
Figure 6_15 Static DHCP list	34
Figure 6_16 Static DHCP configuration.....	34
Figure 6_17 DHCP auto binding.....	35
Figure 6_18 DHCP client list.....	36
Figure 6_19 DHCP service settings - Instance.....	37
Figure 6_20 Static DHCP configuration - Instance A.....	37
Figure 6_21 Static DHCP configuration - Instance B.....	38
Figure 6_22 Static DHCP information list - Instance	38
Figure 7_1 Port Forwarding list	43
Figure 7_2 Port Forwarding Settings	44

Figure 7_3 List of NAT rules information.....	45
Figure 7_4 Easy IP	46
Figure 7_5 One2One	46
Figure 7_6 DMZ configuration	47
Figure 7_7 Port Forwarding Settings.....	48
Figure 7_8 NAT rules Settings—EasyIP	49
Figure 7_9 NAT rule Settings —One2One	50
Figure 7_10 Static Route List.....	51
Figure 7_11 Static Route Settings	51
Figure 7_12 Policy routing list	53
Figure 7_13 Policy routing configuration	54
Figure 7_14 Anti-NetSniper	55
Figure 7_15 Port mirroring.....	56
Figure 7_17 Port VLAN list	57
Figure 7_18 Port VLAN settings	57
Figure 7_19 SYSLOG configuration	58
Figure 8_1 User Status	59
Figure 8_2 User status information list.....	60
Figure 8_3 IP/MAC binding global configuration	62
Figure 8_4 Modification of IP/MAC instances	62
Figure 8_5 IP/MAC binding configuration.....	63
Figure 8_6 IP/MAC binding information list – Instance I	65
Figure 8_7 IP/MAC binding information list – Instance II	66
Figure 8_8 IP/MAC binding information list – Instance III	66
Figure 8_9 Basic workflow of Discovery stage	67
Figure 8_10 PPPoE Global Settings	69
Figure 8_11 PPPoE account info list	70
Figure 8_12 PPPoE account settings.....	71
Figure 8_13 PPPoE User Status List.....	73
Figure 8_14 Export PPPoE Accounts.....	74
Figure 8_15 Import PPPOE Accounts	74
Figure 8_16 Instance - PPPoE Global Settings	75
Figure 8_17 PPPoE account Settings	76
Figure 8_18 Instance - PPPoE User Status List.....	76
Figure 8_19 WebAuth Global Settings	77
Figure 8_22 Web Authentication Account List	78
Figure 8_23 Web Authentication Account List - Add new entry	78
Figure 8_24 WEB Authentication Client Status	80
Figure 8_25 User group list	81
Figure 8_26 User group Settings.....	81
Figure 9_1 Schedule list	82
Figure 9_2 Schedule Settings	83
Figure 9_3 Application Management List	84
Figure 9_4 Internet Application Management Settings	86

Figure 9_5 Internet Application Management.....	88
Figure 9_6 Internet Application Management (Continued Figure 9_5).....	88
Figure 9_7 QQ white list	89
Figure 9_8 Import QQ Accounts	90
Figure 9_10 Trademanager Whitelist	91
Figure 9_11 Daily Routine Notification	92
Figure 9_12 Account expiration notification.....	93
Figure 9_13 Log management	94
Figure 9_14 Internet Audit	95
Figure 9_15 Policy Database list	96
Figure 10_1 Fixed Rate Limiting list	97
Figure 10_2 Fixed Rate Limiting Rule Settings	98
Figure 10_3 Flexible Bandwidth	99
Figure 11_1 Attack Prevention - Internal Attack Prevention	102
Figure 11_2 Attack Prevention - External Attack Prevention	103
Figure 11_3 Access control list	105
Figure 11_4 Access Control Settings - IP address filtering	107
Figure 11_5 Access Control Settings -- URL filtering	109
Figure 11_6 Access Control Settings - Keyword filtering	110
Figure 11_7 Access Control Settings - DNS filtering	111
Figure 11_8 Access Control Settings - Instance I.....	112
Figure 11_9 Access Control Settings - Instance I (Continued Figure 11_8)	113
Figure 11_10 Access Control Settings –Instance II.....	114
Figure 11_11 Access Control Settings – Instance I (Continued Figure 11_10).....	114
Figure 11_12 Domain filtering page.....	115
Figure 11_13 Domain Block Notification page	117
Figure 11_14 Domain Block Notification page	118
Figure 11_15 MAC Address Filtering List	119
Figure 11_16 MAC Address Filtering Settings.....	120
Figure 11_17 MAC address filtering	120
Figure 12_1 PPTP typical application.....	123
Figure 12_2 PPTP list.....	123
Figure 12_3 PPTP server - Global Settings	124
Figure 12_4 PPTP server - Account Settings.....	125
Figure 12_5 PPTP client.....	126
Figure 12_6 PPTP instance topology	128
Figure 12_7 PPTP server Settings	129
Figure 12_8 PPTP server Settings - LAN to LAN.....	129
Figure 12_9 PPTP server Settings - Mobile users	130
Figure 12_10 PPTP client Settings.....	130
Figure 12_11 PPTP List 1	132
Figure 12_12 PPTP List 2.....	132
Figure 12_13 PPTP Client Info List 1	133
Figure 12_14 PPTP Client Info List 2	133

Figure 12_15 IPSec list.....	140
Figure 12_16 Gateway to gateway	141
Figure 12_17 IPSec Advanced options -- Main mode.....	142
Figure 12_18 Dynamic connection to the gateway	144
Figure 12_19 Other party dynamically connects to local machine.....	145
Figure 12_20 Gateway to gateway topology	146
Figure 12_21 Gateway to gateway configuration 1	147
Figure 12_22 Gateway to gateway configuration 2.....	148
Figure 12_23 IPSec connection status - Shanghai gateway	149
Figure 12_24 IPSec connection status - Beijing gateway	149
Figure 12_25 "Dynamic on one party" topology	150
Figure 12_26 Dynamic on one party - The other party dynamically connects to local machine	151
Figure 12_27 Dynamic on one party - Dynamically connects to the gateway	152
Figure 12_28 IPSec connection status -- Other party connects to local host dynamically	153
Figure 12_29 IPSec connection status -- Connect to local host dynamically	153
Figure 13-1 Administrator list.....	154
Figure 13-2 Administrator Settings.....	154
Figure 13_3 Language.....	155
Figure 13-4 Time.....	156
Figure 13-5 Configuration management.....	157
Figure 13_6 Firmware Upgrade.....	158
Figure 13_7 Remote Management.....	159
Figure 13_8 Scheduled task list 1	160
Figure 13_9 Scheduled task list 2	161
Figure 13-10 Scheduled Task Settings.....	161
Figure 14_1 System information.....	162
Figure 14_2 System information.....	164
Figure 14_3 Log Management Settings	165

Appendix C LICENSE STATEMENT / GPL CODE STATEMENT

This product resp. the here (<http://global.level1.com/downloads.php?action=init>) for downloading offered software includes software code developed by third parties, including software code subject to the GNU General Public License Version 2 (“GPLv2”) and GNU Lesser General Public License 2.1 („LGPLv2.1“).

WRITTEN OFFER FOR GPL/LGPL SOURCE CODE

We will provide everyone upon request the applicable GPLv2 and LGPLv2.1 source code files via CDROM or similar storage medium for a nominal cost to cover shipping and media charges as allowed under the GPLv2 and LGPLv2.1. This offer is valid for 3 years. GPLv2 and LGPLv2 inquiries: Please direct all GPL and LGPL inquiries to the following address:

Digital Data Communications GmbH
Zeche-Norm-Str. 25
44319 Dortmund
Deutschland

Phone: [+49 231 9075 - 0](tel:+4923190750)
Fax: [+49 231 9075 - 184](tel:+492319075184)
Email: support@level1.com
Web: www.level1.com

NO WARRANTY

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA

BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent

licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all. The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that

users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

we use this doubled UL to get the sub-sections indented, while making the bullets as unobvious as possible.

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major

components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or

she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns. Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM

(INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.

Copyright (C) yyyy name of author

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but **WITHOUT ANY WARRANTY**; without even the implied warranty of **MERCHANTABILITY** or **FITNESS FOR A PARTICULAR PURPOSE**. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA. Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author

Gnomovision comes with **ABSOLUTELY NO WARRANTY**; for details

type ``show w'`. This is free software, and you are welcome

to redistribute it under certain conditions; type ``show c'`

for details.

The hypothetical commands ``show w'` and ``show c'` should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than ``show w'` and ``show c'`; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright
interest in the program `Gnomovision'
(which makes passes at compilers) written
by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the [GNU Lesser General Public License](#) instead of this License.

