



## Gigabit router UF72N

Carrier Fiber Access Solution

**UNIFIBER**  
GIGAROUTER WiFi - VoIP  
**UF72N**



[WWW.UNIDATA.IT](http://WWW.UNIDATA.IT)



# **GIGAROUTER UF72N**

## **User Manual**

Version: [GIGAROUTER UF72N](#)

---

We are enthusiastic for providing tech support in every way. You can get in touch with local dealer as well as contact to Customer Service Department directly.

**Unidata SpA**

Via Portuense, 1555 - 00148 - Roma (RM)

c/o Commerciti M25 - M26

Tel. (+39) 06 4040 41 (centralino) Fax: (+39) 06 4040 4002

Website: <http://www.unidata.it>

E-mail: [info@unidata.it](mailto:info@unidata.it)

## Copyright

Copyright by Unidata.SpA.

All rights are reserved.

No Part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Unidata SpA.



is the trademarks of Unidata SpA. No the trademarks may be counterfeited.

## Disclaimer

Unidata SpA reserves the right to change the document from time to time at its sole discretion, and not to make the notice to anyone in advance.

# Preface

## Version Statement

This Manual is provided for GIGAROUTER UF72N gateway, the software version must be at least 1.10.

## Brief Introduction

This manual provides technical information on how to configure and operate application for your GIGAROUTER UF72N unit.

Chapter 1: Provides an overview of GIGAROUTER UF72N

Chapter 2: Introduces the product

Chapter 3: Introduces the configuration via WEB-based Management

## Intended Audience


System administrators.

Network engineers.

Maintenance technicians.

## Style Convention

**Table 1 Style convention used in this manual**

Style	Meanings
\	Multi-level catalogs or menus are separated by '\' character. For instance "file\new\directory" means the menu item "directory" in menu "new" which in turn in the menu "file".
	Used to highlight important area in diagrams.
<>	Indicates the input data from operating terminal.
[]	Indicates one parameter configuration or a function.
{ XX   XX }	Indicates a syntax of CLI command options, multiple command options in one "{}", separated by " ", means exclusive single selection.
<i>host</i> (italic)	Indicates user specified parameters. e.g. for command: tftp <i>host</i> {get   put} {sys   cfg} <i>filename</i>  The <i>host</i> and <i>filename</i> should be replaced by user specified real parameters, such as: tftp 138.0.0.1 get sys sysfile.bin

**Table 2 Convention for Mouse Operation**

Operation	Meanings
Click	Press and release a mouse button quickly
Double click	Quickly press and release a mouse button twice



Drag	Press a mouse button and move the mouse
------	---

**Table 3 Convention for Keyboard Operation**

Style	Meanings
Ctrl + C	“+”means an operation which presses down several keys in the keyboard in the same time. E.g. “Ctrl + C” means press down the key of “Ctrl” and “C” in the same time.

# CONTENTS

<b>1</b>	<b>OVERVIEW .....</b>	<b>1</b>
<b>2</b>	<b>PRODUCT INTRODUCTION .....</b>	<b>2</b>
2.1	APPEARANCE.....	2
2.2	HARDWARE INTERFACE.....	3
2.3	FEATURES.....	3
2.4	WORKING ENVIRONMENT.....	4
<b>3</b>	<b>CONFIGURATION INTRODUCTION .....</b>	<b>5</b>
3.1	LOGIN .....	5
3.2	HOME.....	5
3.3	NETWORK CONFIGURATION .....	6
3.3.1	<i>Network Status</i> .....	6
3.3.2	<i>WAN Configuration</i> .....	6
3.3.3	<i>LAN Configuration</i> .....	12
3.3.4	<i>WLAN</i> .....	15
3.3.5	<i>3G Modem</i> .....	22
3.3.6	<i>Port Management</i> .....	24
3.3.7	<i>IPv6 Configuration</i> .....	25
3.4	DATA SERVICE .....	26
3.4.1	<i>Status</i> .....	26
3.4.2	<i>DHCP Server</i> .....	28
3.4.3	<i>NAT Config</i> .....	30
3.4.4	<i>Firewall Config</i> .....	33
3.4.5	<i>QoS</i> .....	44
3.4.6	<i>DDNS</i> .....	49
3.4.7	<i>VPN</i> .....	51
3.4.8	<i>Routing</i> .....	59
3.4.9	<i>Advanced Parameters</i> .....	62
3.4.10	<i>Multicast</i> .....	63
3.4.11	<i>USB Storage</i> .....	63
3.5	VOIP SERVICE.....	65
3.5.1	<i>SIP Service</i> .....	65
3.5.2	<i>User</i> .....	67
3.5.3	<i>Supplementary</i> .....	68
3.5.4	<i>Codec Parameters</i> .....	71
3.5.5	<i>DSP Parameters</i> .....	72
3.5.6	<i>Digitmap</i> .....	73
3.5.7	<i>Signal Tone</i> .....	74
3.5.8	<i>FXS Parameters</i> .....	75
3.5.9	<i>Centrex</i> .....	76
3.5.10	<i>Phone Book</i> .....	78
3.6	SYSTEM .....	78
3.6.1	<i>Time Management</i> .....	78

3.6.2	<i>Upgrade</i> .....	80
3.6.3	<i>Reboot System</i> .....	81
3.6.4	<i>Backup/Restore</i> .....	81
3.6.5	<i>Diagnostic</i> .....	81
3.6.6	<i>User Management</i> .....	83
3.6.7	<i>System Log</i> .....	83
3.6.8	<i>TR069</i> .....	84
3.6.9	<i>SNMP</i> .....	86
3.6.10	<i>User Access Right</i> .....	87
3.7	<i>APPLY</i> .....	88
3.8	<i>PRINT FUNCTION</i> .....	88
<b>4</b>	<b>CLI INTRODUCTION</b> .....	<b>94</b>
4.1	<i>LOGIN</i> .....	94
4.2	<i>NETWORK</i> .....	95
4.2.1	<i>3G Modem</i> .....	95
4.2.2	<i>Port Management</i> .....	97
4.2.3	<i>Wan Parameter</i> .....	98
4.2.4	<i>Lan Parameter</i> .....	108
4.3	<i>DATA SERVICE</i> .....	122
4.3.1	<i>DHCP Server</i> .....	122
4.3.2	<i>NAT Config</i> .....	124
4.3.3	<i>Firewall Config</i> .....	129
4.3.4	<i>QoS</i> .....	145
4.3.5	<i>DDNS</i> .....	153
4.3.6	<i>VPN</i> .....	154
4.3.7	<i>Routing</i> .....	167
4.3.8	<i>Advanced Parameters</i> .....	175
4.3.9	<i>Multicast</i> .....	176
4.4	<i>VOIP SERVICE</i> .....	176
4.4.1	<i>SIP Service</i> .....	176
4.4.2	<i>User</i> .....	180
4.4.3	<i>Supplementary</i> .....	181
4.4.4	<i>Codec Parameters</i> .....	187
4.4.5	<i>DSP Parameters</i> .....	188
4.4.6	<i>Digitmap</i> .....	190
4.4.7	<i>Signal Tone</i> .....	190
4.4.8	<i>Centrex</i> .....	193
4.4.9	<i>Phone Book</i> .....	194
4.4.10	<i>Save and Reload VOIP Parameter</i> .....	196
4.5	<i>SYSTEM</i> .....	196
4.5.1	<i>Time Management</i> .....	196
4.5.2	<i>Reboot System</i> .....	198
4.5.3	<i>Backup/Restore</i> .....	198
4.5.4	<i>Diagnostic</i> .....	198
4.5.5	<i>System Log</i> .....	198
4.5.6	<i>TR069</i> .....	199

4.5.7	SNMP.....	201
-------	-----------	-----

# 1 Overview

A new series of ALL IN ONE INTELLIGENT Gateway GIGAROUTER UF72N is perfectly designed for SOHO, small and medium sized business (SMB) requiring application-based solutions of low-capital investment to communicate with various kinds of users, the complete VoIP features are built in. Comparing with other Voice equipments, GIGAROUTER UF72N has integrated high data capacity of WIFI 300Mbps and GE LAN. Robust VPN functions support office users to create remote multiple accessing of site-site encrypted private connections over public Internet. Multi-access way of GIGAROUTER UF72N has includes Ethernet, Optical and 3G.



## 2 Product Introduction

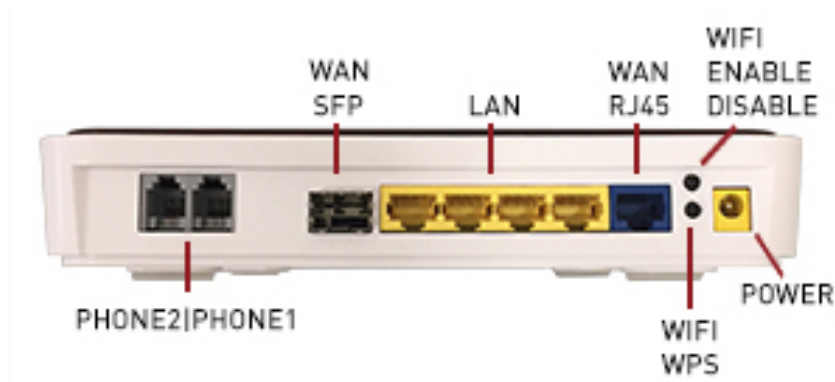
### 2.1 Appearance



**Figure 2-1 GIGAROUTER UF72N Front View**

**Table 2-1 LED**

LED	Status	Indication
PWR	Off	Power is off
	Solid Green	Device is running
INTERNET	Off	Power is off
	Slow Flash Green	INTERNET type WAN PPPoE connection authenticate failed
	Solid Green	INTERNET type WAN connection is up
SFP	Off	No optical signal is detected
	Solid Green	Optical signal is detected
WAN	Off	No Ethernet signal is detected
	Flash Green	User data going through Ethernet port
	Solid Green	Ethernet interface is ready to work
LAN1~LAN4	Off	No Ethernet signal is detected
	Flash Green	User data going through Ethernet port
	Solid Green	Ethernet interface is ready to work
Phone1&2	Off	Phone is onhook
	Solid Green	Phone is offhook
VPN	Off	No VPN connection
	Solid Green	VPN is established
REG	Off	All accounts register failure
	Solid Green	All accounts register successfully
	Flash Green	Some accounts register successfully and rest register fails



**Figure 2-2 GIGAROUTER UF72N Rear View**

- WAN: 1000/100/10Mbps ethernet ports.
- LAN(N): 1000/100/10Mbps ethernet ports.
- SFP: Gigabit fiber interface.
- SD: Interface for SD card.
- FXS: Analog telephone interface.
- POWER: DC power input connector.
- Reset button: Use the button to restore the device to the factory defaults.
- WPS: WIFI WPS switch.

## 2.2 Hardware Interface

**Table 2-2 Hardware interface**

LAN	4 100/1000BASE-T ports
WAN	1 FE ethernet port or 1 GE optical port
WIFI	4 WIFI access point, support 802.11b/g/n
SFP	1 Gigabit fiber interface
USB	1 USB 2.0 port, use for storage or 3G modem

## 2.3 Features

### Data Network

- **WAN:** 1xGE, 1xSFP and 1xUSB port for 2G/3G USB Modem Connectivity
- **LAN:** 2x10/100/1000 Mbps Ethernet Port
- **WAN Access Mode:** Static IP address, PPPoE, DHCP, PPTP and L2TP
- **Networking Interface:** Multi WAN, Bridge Mode, 802.1Q
- **QOS:** Destination/Source MAC/IP, Application, DSCP, Supports Bandwidth Control
- **Advance Routing:** Static Route, Policy Route, DNS Proxy, RIP
- **Internal Address Management:** DHCP Server, IP and MAC Address Bind, DHCP Relay
- **Networking Protocols:** TCP/IP (IPv4/v6), UDP, RTP, SNTP, NAT, DHCP, DNS, DDNS, DLNA
- **VPN:** IPSEC, PPTP, L2TP
- **IPTV:** IGMP Proxy/Snooping, IPTV Bridge

### Management

- **Management Protocol:** CLI,SNMPV1/2,Tr069,Web
- **LED Indications:** Total 12LEDS for Power, WAN/LAN, Phone
- **Control Button:** WPS Button, WLAN Button, Power Switch, Reset Button

### NAT

- **Supports ALG, DMZ, PAT**

### Firewall & Security

- **Firewall Protection:** IDS&IPS, Block Ping/ICMP/IDENT, SPI Firewall, Portscan restriction
- **Access control:** Blocking by URL,IP Address, Mac Address, Protocol Type, Port

### WIFI WLAN

- **Standard:** IEEE 802.11b/g/n(2.4GHz)
- **Security:** WEP,WPA,WPA2,PWA-PSK,WPA2-PSK
- **WIFI Features:** WMM,WLAN-LAN Isolation, Multi SSID(X4), AP Isolation
- **Antenna Type:** 2R2T

### Voice Capacity and Functions

- **Analog User/Co line:** 2/4/8xLines FXS/FXO

### Centrex Functions List

- Call Forward on Busy
- Call Forward on No Answer
- Call Forward Unconditional
- Caller ID
- Caller ID on Call Waiting
- Call Waiting
- Three-way Calling
- Ring groups

### USB storage/Print

- Support USB storage
- Support print sharing

## 2.4 Working Environment

Environment requirement includes storage temperature, working temperature and humidity.

- Storage Temperature: -40°C - 70°C
- Long Time Working Temperature: -10°C - 50°C
- Short Time Working Temperature: -15°C - 60°C
- Environment Humidity: 5% - 95% RH, no coagulation

## 3 Configuration Introduction

### 3.1 Login

The Web interface is ready for accessing about one minute after the device power on. The default LAN IP address is 192.168.100.1, you can access the Web interface via either WAN port or LAN port. Enter IP address in the address bar of web browser and then press ENTER, you can get access to the Login interface. There are two languages provided: Chinese and English.

Figure 3-1 Login Interface

### 3.2 Home

After successful login, you will see the main menus on the top of the Web-based GUI.

The **System Status** page provides the current status information about the Gateway. All information is read-only.

Choose the menu **Home** to load the following page.

Home   Network   Data Service   VoIP Service   System   Apply   Logout	
System Status	
Serial Number:	1111111111
Software Version:	R3621-W1_AM_v1.1.7
CPU Usage(%):	0%
Memory Usage(used/total):	47%
System Time:	2000-01-02 00:01:44
Uptime:	01 Day 00 Hour 01 Min
WAN MAC Address:	00:0e:b4:09:ad:20
Connection Mode:	Static IP
IP Address:	10.55.1.1
Netmask:	255.255.0.0
Default Gateway:	--
DNS:	--
LAN MAC Address:	00:0e:b4:09:ad:21
IP Address:	192.168.1.1
Netmask:	255.255.255.0
<input type="checkbox"/> Autorefresh <input type="button" value="Refresh"/>	

Figure 3-2 System Status

### 3.3 Network Configuration

#### 3.3.1 Network Status

The Status page shows all WAN and LAN interfaces configuration, and all physical ports connection status related to this device.

##### 3.3.1.1 WAN Status

Choose the menu **Network**→**Status**→**WAN** to load the following page.

Network ==> Status

WAN LAN Link Status

Name	Mode	Status	IP Address	Netmask	Gateway	VLAN		
DATA	Static IP	--	10.55.1.1	255.255.0.0	--	Enable	VID	PRI
VOICE	--	--	--	--	--	--	--	--
MGMT	--	--	--	--	--	--	--	--
OTHER1	--	--	--	--	--	--	--	--
OTHER2	--	--	--	--	--	--	--	--

Figure 3-3 WAN Status

##### 3.3.1.2 LAN Status

Choose the menu **Network**→**Status**→**LAN** to load the following page.

Network ==> Status

WAN LAN Link Status

IP Address	Netmask	NAT	Description
192.168.1.1	255.255.255.0	Yes	VLAN1

Figure 3-4 LAN Status

##### 3.3.1.3 Link Status

Choose the menu **Network**→**Status**→**Link Status** to load the following page.

Network ==> Status

WAN LAN Link Status

Port	Auto Negotiation	Connect Status	Speed	Duplex Mode
WAN	Enable	Link Up	1000Mbps	Full Duplex
LAN1		Link Down		
LAN2		Link Down		
LAN3	Enable	Link Up	100Mbps	Full Duplex
LAN4	Enable	Link Up	100Mbps	Full Duplex

Figure 3-5 Link Status

#### 3.3.2 WAN Configuration

The device supports 5 WAN interfaces: DATA, VOICE, MGMT, OTHER1, OTHER2; Every WAN interface provides the following five Internet connection types: Static IP, DHCP, PPPoE, PPTP, L2TP.



Choose the menu **Network**→**WAN** to load the configuration show page.

Network ==> WAN						
Interface Name	Enable	Type	VLAN Enable	VID	PRI	
<a href="#">DATA</a>	Yes	Static IP	No	--	--	
<a href="#">VOICE</a>	No	--	Yes	7	6	
<a href="#">MGMT</a>	No	--	Yes	10	2	
<a href="#">OTHER1</a>	No	--	No	--	--	
<a href="#">OTHER2</a>	No	--	No	--	--	

**Figure 3-6 WAN page**

Select an **Interface Name** to load the configuration page.

### 1) Static IP

If a static IP address has been provided by your ISP, please choose the Static IP connection type to configure the parameters for WAN port manually.

Network ==> WAN	
Interface Name	DATA
Enable	<input checked="" type="checkbox"/>
Type	Static IP
VLAN Enable	<input checked="" type="checkbox"/>
VLAN ID	1 (1,4094)
Priority Level	0 (0,7)
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
IP Address	0.0.0.0 *
Netmask	0.0.0.0 *
Gateway	<input checked="" type="checkbox"/> 0.0.0.0
<div> <div>Save</div> <div>Return</div> </div>	

**Figure 3-7 WAN-Static IP**

The following items are displayed on this screen:

- ▶ **Enable:** Enable this WAN interface (DATA can't be disabled).
- ▶ **Type:** Select Static IP if your ISP has assigned a static IP address for your.
- ▶ **VLAN Enable:** Optional. Enable VLAN to configure VLAN ID and VLAN Priority Level.
- ▶ **VLAN ID:** Optional. VLAN ID of this WAN interface.
- ▶ **Priority Level:** Optional. VLAN Priority Level of this WAN interface.
- ▶ **Primary DNS:** Enter the IP address of your ISP's Primary DNS (Domain Name Server). If you are not clear, please consult your ISP. It's not allowed to access the Internet via domain name if the Primary DNS field is blank.
- ▶ **Secondary DNS:** Optional. If a Secondary DNS Server address is available, enter it.
- ▶ **IP Address:** Enter the IP address assigned by your ISP. If you are not clear, please consult your ISP.
- ▶ **Netmask:** Enter the Subnet Mask assigned by your ISP.

- **Gateway:** Optional. Enter the Gateway assigned by your ISP.

## 2) DHCP

If your ISP (Internet Service Provider) assigns the IP address automatically, please choose the DHCP connection type to obtain the parameters for WAN port automatically.

Interface Name	DATA
Enable	<input checked="" type="checkbox"/>
Type	DHCP
VLAN Enable	<input checked="" type="checkbox"/>
VLAN ID	1 (1,4094)
Priority Level	0 (0,7)
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Appoint Server IP	<input type="checkbox"/>
Vendor Class Identifier	<input type="checkbox"/>
Enterprise Code	
Manufacture Name	
Device Class	
Device Type	
Device Version	

Save Return

**Figure 3-8 WAN-DHCP**

The following items are displayed on this screen:

- **Enable:** Enable this WAN interface (DATA can't be disabled).
- **Type:** Select DHCP if your ISP assigns the IP address automatically.
- **VLAN Enable:** Optional. Enable VLAN to configure VLAN ID and VLAN Priority Level.
- **VLAN ID:** Optional. VLAN ID of this WAN interface.
- **Priority Level:** Optional. VLAN Priority Level of this WAN interface.
- **Primary DNS:** Enter the IP address of your ISP's Primary DNS (Domain Name Server) manually. If you are not clear, please consult your ISP. It's not allowed to access the Internet via domain name if the Primary DNS field is blank.
- **Secondary DNS:** Optional. If a Secondary DNS Server address is available, enter it.
- **Appoint Server IP:** Optional. If network has multiple DHCP servers, enter the IP address of your ISP'S DHCP server
- **Vendor Class Identifier:** Optional. This option (60) is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client.
- **Enterprise Code:** Optional.
- **Manufacture Name:** Optional.
- **Device Class:** Optional.

- **Device Type:** Optional.
- **Device Version:** Optional.

### 3) PPPoE

If your ISP (Internet Service Provider) has provided the account information for the PPPoE connection, please choose the PPPoE connection type (Used mainly for DSL Internet service).

Network ==> WAN

Interface Name	VOICE
Enable	<input checked="" type="checkbox"/>
Type	PPPoE
VLAN Enable	<input checked="" type="checkbox"/>
VLAN ID	7 (1,4094)
Priority Level	6 (0,7)
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
Username	123 *
Password	●●● *
AC Name	
Service Name	
LCP Interval	10 [1,3000]; default:10
LCP Max Fails	5 [1,10]; default:5

Save Return

**Figure 3-9 WAN-PPPoE**

The following items are displayed on this screen:

- **Enable:** Enable this WAN interface (DATA can't be disabled).
- **Type:** Select PPPoE if your ISP provides xDSL Virtual Dial-up connection.
- **VLAN Enable:** Optional. Enable VLAN to configure VLAN ID and VLAN Priority Level.
- **VLAN ID:** Optional. VLAN ID of this WAN interface.
- **Priority Level:** Optional. VLAN Priority Level of this WAN interface.
- **Primary DNS:** Enter the IP address of your ISP's Primary DNS (Domain Name Server) manually. If you are not clear, please consult your ISP. It's not allowed to access the Internet via domain name if the Primary DNS field is blank.
- **Secondary DNS:** Optional. If a Secondary DNS Server address is available, enter it.
- **Username:** Enter the Account Name provided by your ISP. If you are not clear, please consult your ISP.
- **Password:** Enter the Password provided by your ISP.
- **Service Name /AC Name:** Optional. The service name and AC (Access Concentrator) name, which should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- **LCP Interval:** PPPoE will send an LCP echo-request frame to the peer every **LCP interval** seconds.
- **LCP Max Fails:** PPPoE will presume the peer to be dead if **LCP Max Fails** LCP

echo-requests are send without receiving a valid LCP echo-reply.

#### 4) L2TP

If your ISP (Internet Service Provider) has provided the account information for the L2TP connection, please choose the L2TP connection type.

**Figure 3-10 WAN-L2TP**

The following items are displayed on this screen:

- ▶ **Enable:** Enable this WAN interface (DATA can't be disabled).
- ▶ **Type:** Select L2TP if your ISP provides a L2TP connection.
- ▶ **VLAN Enable:** Optional. Enable VLAN to configure VLAN ID and VLAN Priority Level.
- ▶ **VLAN ID:** Optional. VLAN ID of this WAN interface.
- ▶ **Priority Level:** Optional. VLAN Priority Level of this WAN interface.
- ▶ **Primary DNS:** Enter the IP address of your ISP's Primary DNS (Domain Name Server). If you are not clear, please consult your ISP. It's not allowed to access the Internet via domain name if the Primary DNS field is blank.
- ▶ **Secondary DNS:** Optional. If a Secondary DNS Server address is available, enter it.
- ▶ **Server IP:** Enter the Server IP provided by your ISP.
- ▶ **Username:** Enter the Account Name provided by your ISP. If you are not clear, please consult your ISP.
- ▶ **Password:** Enter the Password provided by your ISP.

**Secondary Connection:** Here allow you to configure the secondary connection. DHCP and Static IP connection types are provided.

If **Static** is selected:

- ▶ **IP Address:** If Static IP is selected, configure the IP address of WAN port.

- ▶ **Netmask:** If Static IP is selected, configure the subnet mask of WAN port.
  - ▶ **Gateway:** Optional. If Static IP is selected, configure the default gateway of WAN port.
- If **DHCP** is selected:
- ▶ **Appoint Server IP:** Optional. If network has multiple DHCP servers, enter the IP address of your ISP's DHCP server.
  - ▶ **Vendor Class Identifier:** Optional. This option (60) is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client.
  - ▶ **Enterprise Code:** Optional.
  - ▶ **Manufacture Name:** Optional.
  - ▶ **Device Class:** Optional.
  - ▶ **Device Type:** Optional.
  - ▶ **Device Version:** Optional.

## 5) PPTP

If your ISP (Internet Service Provider) has provided the account information for the PPTP connection, please choose the PPTP connection type.

Network ==> WAN

Interface Name	VOICE	
Enable	<input checked="" type="checkbox"/>	
Type	PPTP	
VLAN Enable	<input checked="" type="checkbox"/>	
VLAN ID	7	(1,4094)
Priority Level	6	(0,7)
Primary DNS	0.0.0.0	
Secondary DNS	0.0.0.0	

---

☐ Static
☒ DHCP

Appoint Server IP	<input type="checkbox"/>	<input type="text"/>
Vendor Class Identifier	<input type="checkbox"/>	<input type="text"/>
Enterprise Code	<input type="text"/>	
Manufacture Name	<input type="text"/>	
Device Class	<input type="text"/>	
Device Type	<input type="text"/>	
Device Version	<input type="text"/>	
Server IP	<input type="text"/>	*
Username	<input type="text"/>	*
Password	<input type="text"/>	*
Enable Encryption	<input type="checkbox"/>	

Save
Return

**Figure 3-11 WAN-PPTP**

The following items are displayed on this screen:



- ▶ **Enable:** Enable this WAN interface (DATA can't be disabled).
- ▶ **Type:** Select PPTP if your ISP provides a PPTP connection.
- ▶ **VLAN Enable:** Optional. Enable VLAN to configure VLAN ID and VLAN Priority Level.
- ▶ **VLAN ID:** Optional. VLAN ID of this WAN interface.
- ▶ **Priority Level:** Optional. VLAN Priority Level of this WAN interface.
- ▶ **Primary DNS:** Enter the IP address of your ISP's Primary DNS (Domain Name Server) manually. If you are not clear, please consult your ISP. It's not allowed to access the Internet via domain name if the Primary DNS field is blank.
- ▶ **Secondary DNS:** Optional. If a Secondary DNS Server address is available, enter it.
- ▶ **Server IP:** Enter the Server IP provided by your ISP.
- ▶ **Username:** Enter the Account Name provided by your ISP. If you are not clear, please consult your ISP.
- ▶ **Password:** Enter the Password provided by your ISP.
- ▶ **Enable Encryption:** Enable PPTP link encryption.

**Secondary Connection:** Here allow you to configure the secondary connection. DHCP and Static IP connection types are provided.

If **Static** is selected:

- ▶ **IP Address:** If Static IP is selected, configure the IP address of WAN port.
- ▶ **Netmask:** If Static IP is selected, configure the subnet mask of WAN port.
- ▶ **Gateway:** Optional. If Static IP is selected, configure the default gateway of WAN port.

If **DHCP** is selected:

- ▶ **Appoint Server IP:** Optional. If network has multiple DHCP servers, enter the IP address of your ISP's DHCP server.
- ▶ **Vendor Class Identifier:** Optional. This option (60) is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client.
- ▶ **Enterprise Code:** Optional.
- ▶ **Manufacture Name:** Optional.
- ▶ **Device Class:** Optional.
- ▶ **Device Type:** Optional.
- ▶ **Device Version:** Optional.

### 3.3.3 LAN Configuration

On this page, you can configure the parameters for LAN port.

Choose the menu **Network**→**LAN** to load the following page. There are three parts on this page.

Network ==> LAN

<input type="checkbox"/>	Interface Name	IP	Netmask	NAT	VID	LAN Bind	WAN Bind
<input type="checkbox"/>	VLAN1	192.168.1.1	255.255.255.0	Yes	--	1,2,3,4	D

1 Total 1 Pages, 1 Rows

WAN Bind Note: D(DATA); V(VOICE); M(MGMT); O1(OTHER1); O2(OTHER2);

Port	Route/Bridge	VLAN ID List	Note Message
LAN1	Route		Route:route to WAN
LAN2	Route		Transparent bridge:not modify the packets;
LAN3	Route		Tagged bridge:LAN untagged, WAN tagged; only 1 VID supported
LAN4	Route		Promisc Mode:Tagged packets in bridge mode, untagged packets in route mode;most 5 VIDs supported(e.g. 8,10,13).

[-Advanced Parameters](#)

☐ LAN Isolate

Auto Bridge	DHCP Vendor ID		STB Data Service		IPTV VLAN		STB Data VLAN
			IP Address	Netmask	VID	PRI	
<input checked="" type="checkbox"/>	albis	sagem	192.168.111.1	255.255.255.0	6	4	Automatic <input type="checkbox"/> 7

Figure 3-12 LAN page

### 1) Part 1: Configure LAN interfaces

Click the **Interface Name** of existent LAN interface you want to modify. If you want to delete the entry, select it and click the **Del** (the VLAN1 is default existed, can't be removed).

Click the **Add** button to add a new entry.

Network ==> LAN==> Static IP

Interface Name: VLAN1 \*

IP Address: 192.168.1.1 \*

Netmask: 255.255.255.0 \*

NAT: ☒

Assign NAT IP: ☐ 0.0.0.0

Enable DHCP Server: ☒

Start IP: 192.168.1.100

End IP: 192.168.1.200

Netmask: 255.255.255.0

Gateway: 192.168.1.1

Primary DNS: 192.168.1.1

Secondary DNS:

Lease Time(Second): 86400

[-Advanced Parameter](#)

LAN Port: ☒ LAN1 ☒ LAN2 ☒ LAN3 ☒ LAN4

WAN Subinterface: ☒ DATA ☐ VOICE ☐ MGMT ☐ OTHER1 ☐ OTHER2

### Figure 3-13 Configure LAN Interface

The following items are displayed on this part.

- ▶ **Interface Name:** Name of this LAN interface.
- ▶ **IP Address:** Enter the IP address for this LAN interface.
- ▶ **Netmask:** Enter the subnet mask for this LAN interface.
- ▶ **NAT:** Optional Enable or disable NAT for this LAN interface
- ▶ **Assign NAT IP:** Optional If NAT is selected. NAT IP address can be assigned.
- ▶ **Enable DHCP Server:** Enable or disable DHCP server on this LAN interface.
- ▶ **Start IP:** If **Enable DHCP Server** is selected, enter the Start IP address to define a range for the DHCP server to assign dynamic IP addresses. This address should be in the same IP address subnet with the IP address of this LAN interface.
- ▶ **End IP:** If **Enable DHCP Server** is selected, enter the End IP address to define a range for the DHCP server to assign dynamic IP addresses. This address should be in the same IP address subnet with the IP address of this LAN interface.
- ▶ **Netmask:** If **Enable DHCP Server** is selected, enter the **Netmask** to define a range for the DHCP server to assign dynamic IP addresses.
- ▶ **Gateway:** Optional .If **Enable DHCP Server** is selected, enter the Gateway address to be assigned.
- ▶ **Primary DNS:** Optional. If **Enable DHCP Server** is selected, enter the Primary DNS server address to be assigned.
- ▶ **Secondary DNS:** Optional. If **Enable DHCP Server** is selected, enter the Secondary DNS server address to be assigned.
- ▶ **Lease Time(Second):** If **Enable DHCP Server** is selected, specify the length of time the DHCP server will reserve the IP address for each client. After the IP address expired, the client will be automatically assigned a new one.

#### Advanced Parameter

- ▶ **LAN Port:** Select the physical LAN port to bind the IP address of this LAN interface.
- ▶ **WAN Subinterface:** Select the WAN subinterface which the packet from this LAN interface can be sending to.

### 2) Part 2: Configure LAN Route/Bridge mode

The following items are displayed on this part.

- ▶ **Port:** The physical LAN port name (LAN1~LAN4).
- ▶ **Route/Bridge:** Mode of this physical LAN port. The following four modes are provided:
  - Route:** route to WAN
  - Transparent bridge:** not modify the packets;
  - Tagged bridge:** LAN untagged, WAN tagged; only 1 VID supported
  - Promisc Mode:** Tagged packets in bridge mode, untagged packets in route mode; most 5 VIDs supported (e.g. 8, 10, 13).
- ▶ **VLAN ID List:** If Tagged bridge/Promisc Mode is selected, configure the VID/VIDs.

### 3) Part 3: Configure IPTV

Choose the menu **Network**→**LAN**→**Advanced Parameters** to load this page.

The following items are displayed on this part.

- ▶ **LAN Isolate:** Check the box to prohibit the access between LAN interfaces.
- ▶ **Auto Bridge:** Check the box to dynamically create IPTV bridge for STB.
- ▶ **DHCP Vendor ID:** Vendor class identifier List (DHCP 60 option), support at most two vendor IDs.
- ▶ **IPAddress:** IP address of interface for STB data service.
- ▶ **Netmask:** Subnet mask of interface for STB data service.
- ▶ **VID:** VID of IPTV VLAN.
- ▶ **PRI:** Priority level of IPTV VLAN.
- ▶ **Automatic:** Check the box to automatically detect the VID of STB data service.

### 3.3.4 WLAN

**Wi-Fi** is a **WLAN** (Wireless Local Area Network) technology. It provides short-range wireless high-speed data connections between mobile data devices (such as laptops, PDAs or phones) and nearby Wi-Fi access points (special hardware connected to a wired network).

#### 3.3.4.1 Basic Settings

Choose the menu **Network**→**WLAN**→**Basic Settings** to load the following page.

Enable	SSID Name	Bind Interface	Enable Broadcast	Isolated	LAN Isolated	Max Client
<input checked="" type="checkbox"/>	Eltek-0-09AD21	VLAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	32
<input checked="" type="checkbox"/>	Eltek-1-09AD21	VLAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	32
<input type="checkbox"/>	Eltek-2-09AD21	VLAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	32
<input type="checkbox"/>	Eltek-3-09AD21	VLAN1	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	32

**Figure 3-14 Configure WIFI Basic Settings**

The following items are displayed on this screen:

- ▶ **Enable WiFi:** Enable or disable the WIFI AP function globally.
- ▶ **Channel:** This field determines which operating frequency will be used. The default channel is set to **AutoSelect**, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- ▶ **Wireless Mode:** Select the desired mode.
  - 11b:** Select if all of your wireless clients are 802.11b.
  - 11g:** Select if all of your wireless clients are 802.11g.
  - 11n:** Select only if all of your wireless clients are 802.11n.
  - 11b/g:** Select if you are using both 802.11b and 802.11g wireless clients.
  - 11b/g/n:** Select if you are using a mix of 802.11b, 11g and 11n wireless clients.

- **Channel Width:** Select any channel width from the drop-down list. The default setting is automatic, which can automatically adjust the channel width for your clients. If you choose to **11n** or **11b/g/n** Wireless mode, this configuration is required. Two values of width are provided: **20MHz** and **20/40MHz**.

The **Service Set Identifier (SSID)** is used to identify an 802.11 (Wi-Fi) network and it's discovered by network sniffing/scanning. GIGAROUTER UF72N provides up to four SSID.

- **Enable:** Enable or disable this entry of SSID. SSID1 can't be disabled.
- **SSID Name:** Enter the name of SSID. The name of SSID must be unique in all wireless networks nearby.
- **Bind Interface:** Select a network interface to be bridged to the SSID.
- **Enable Broadcast:** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device. If you select the **Enable Broadcast** checkbox, the device will broadcast its name (SSID) on the air.
- **Isolated:** Enable or disable isolate different clients from the same wireless station.
- **LAN Isolated:** Enable or disable isolation between the LAN and SSID.
- **Max Client:** Enter the maximum number of clients allowed to connect to the SSID.
- **SSID AP Isolated:** This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

### 3.3.4.2 Security

Choose the menu **Network**→**WLAN**→**Security** to load the Security page. There are nine wireless security modes supported by the device: Open WEP, Shared WEP, WEP Auto, WPA-PSK, WPA2-PSK, WPAPSK/WPA2PSK, WPA, WPA2 and WPAWPA2.

If you do not want to use wireless security, select **Disable**, but it's strongly recommended to choose one of the following modes to enable security.

**1) WPA-PSK, WPA2-PSK, WPAPSK/WPA2PSK:** It's the WPA/WPA2 authentication type based on pre-shared passphrase. Choose one of these types, the following page is loaded.

Network ==> WLAN

Basic Settings Security WPS Advanced Settings Clients Info MAC Filtering

SSID1: Eltek-11

Authentication: WPAPSK/WPA2PSK

Algorithm: AES

WPA Pre-Shared Key: [Masked] (8~64characters)

Renew Interval: 3600 [0,2592000]s, 0:not renew

Save Refresh

**Figure 3-15 Configure WIFI PSK Security**

The following items are displayed on this screen:

- **SSID:** The SSID enabled in **WLAN**→**Basic Settings** page. Read only
- **Authentication:** The authentication type selected: WPA-PSK, WPA2-PSK, WPAPSK/WPA2PSK.
- **Algorithm:** When WPA2-PSK or WPAPSK/WPA2PSK is set as the Authentication Type,



you can select either **TKIP**, or **AES** or **TKIP/AES** as Encryption. When WPA-PSK is set as the Authentication Type, you can select either TKIP or AES as Encryption.

- **WPA Pre-Shared Key:** You can enter ASCII characters between 8 and 64 characters.
- **Renew Interval:** Specify the group key update interval in seconds. Enter 0 to disable the update.

**2) Open WEP, Shared WEP, WEP Auto:** It is based on the IEEE 802.11 standard. Choose one of these types, the following page is loaded.

**Figure 3-16 Configure WIFI WEP Security**

The following items are displayed on this screen:

- **SSID:** The SSID enabled in **WLAN**→**Basic Settings** page. Read only
- **Authentication:** The authentication type selected: Open WEP, Shared WEP, WEP Auto.
- **Default Key:** Select the default WEP key configure below.
- **Key:** Provide up to four key. You can select the key type HEX(10/26 char) or ASCII(5/13 char)) for encryption and then enter the key. HEX(10/26 char) and ASCII(5/13 char) formats are provided.
  - Hex(10/26 char):** format stands for any combination of hexadecimal digits (0-9, a-f, A-F) in the specified length.
  - ASCII(5/13 char):** format stands for any combination of keyboard characters in the specified length.

**3) WPA, WPA2, WPA/WPA2:** It's based on Radius Server. Choose one of these types, the following page is loaded.

Network ==> WLAN

Basic Settings Security WPS Advanced Settings Clients Info MAC Filtering

SSID1: Eltek-11

Authentication: WPA/WPA2

Algorithm: AES

Renew Interval: 3600 [0,2592000]s, 0:not renew

PMK Cache Period: 10 [0,43200]min, default:10

Enable Pre-Auth: ☐

Radius Server IP: 1.1.1.1

Radius Server Port: 1812 [0,65535], default:1812

Shared Secret: ●●●●●●●● (8~64characters)

Session Timeout: 65500 [0,65500]s, default:65500

Save Refresh

**Figure 3-17 Configure WIFI WPA Security**

The following items are displayed on this screen:

- ▶ **SSID:** The SSID enabled in **WLAN**→**Basic Settings** page.Read only
- ▶ **Authentication:** The authentication type selected: WPA, WPA2, WPA/WPA2.
- ▶ **Algorithm:** You can select either **TKIP**, or **AES** or **TKIP/AES**.
- ▶ **Renew Interval:** Specify the update interval in seconds. Enter 0 to disable the update.
- ▶ **PMK Cache Period:** Pairwise Master Key, PMK. Set WPA2 PMKID cache timeout period, after time out, the cached key will be deleted.This parameter is valid when you select WPA2 or WPA/WPA2.
- ▶ **Enable Pre-Auth:** This is used to speed up roaming before pre-authenticating IEEE 802.1X/EAP part of the full RSN authentication and key handshake before actually associating with a new AP. Default is disable. This parameter is valid when you select WPA2 or WPA/WPA2.
- ▶ **Rasius Server IP:** Enter the IP address of the Radius Server.
- ▶ **Rasius Server Port:** Enter the port that radius service used.
- ▶ **Shared Seret:** Enter the password for the Radius Server.
- ▶ **Session Timeout:** Specify the session timeout in seconds, Enter 0 to not limit the timeout.

### 3.3.4.3 WPS

**Wi-Fi Protected Setup (WPS; originally Wi-Fi Simple Config)** is a computing standard that attempts to allow easy establishment of a secure wireless home network.WPS currently supports two methods: Personal Information Number (PIN) and Push Button Configuration (PBC).The difference between the two methods is much pretty described in their names.

The **PIN** method involves entering a client device PIN, obtained either from a client application GUI or a label on a device, into the appropriate admin screen on a Registrar device.

The **PBC** method requires the user to push buttons on the Registrar and Client devices within a two-minute period to connect them. (The two-minute period also applies to the PIN method.) The buttons can be physical, as they typically are on AP / router devices or virtual, as is normal on client devices.

Choose the menu **Network**→**WLAN**→**WPS** to load the WPS page.

#### 1) PIN Mode

If PIN mode is selected, the following page is loaded.

**Figure 3-18 Configure WIFI WPS-PIN**

The following items are displayed on this screen:

- ▶ **Enable WPS:** Enable or disable the WIFI WPS function globally.
- ▶ **WPS Mode:** Choose the WPS mode: PIN.
- ▶ **PIN Code:** If PIN mode is chosen, enter the 8 digit PIN code, and then click Connect.

## 2) PBC Mode

If PBC mode is selected, the following page is loaded.

**Figure 3-19 Configure WIFI WPS-PBC**

The following items are displayed on this screen:

- ▶ **Enable WPS:** Enable or disable the WIFI WPS function globally.
- ▶ **WPS Mode:** Choose the WPS mode: PBC.
- ▶ **PBC Set:** If PBC mode is chosen, then click **Simulation Connect**.

### 3.3.4.4 Advanced Settings

Choose the menu **Network**→**WLAN**→**Advanced Settings** to load the following page.

**Figure 3-20 Configure WIFI Advanced Settings**

The following items are displayed on this screen:

- ▶ **Fragmentation Threshold:** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- ▶ **RTS Threshold:** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the device will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2347.
- ▶ **Transmit Power:** Here you can specify the transmit power of device. 100 is the default setting and is recommended.
- ▶ **Enable WMM:** Enable or disable the WIFI WMM function globally. WMM function can guarantee the packets with high-priority messages, being transmitted preferentially. It is strongly recommended enabled.

### 3.3.4.5 Clients Info

Choose the menu **Network**→**WLAN**→**Clients Info** to load the following page.

MAC	AID	Bandwidth	SSID
00:66:4b:2e:00:52	1	20MHz	Eltek-11

1 Total 1 Pages, 1 Rows

Refresh

**Figure 3-21 View Wifi Clients Info**

This page shows all connected WIFI client information, read only.

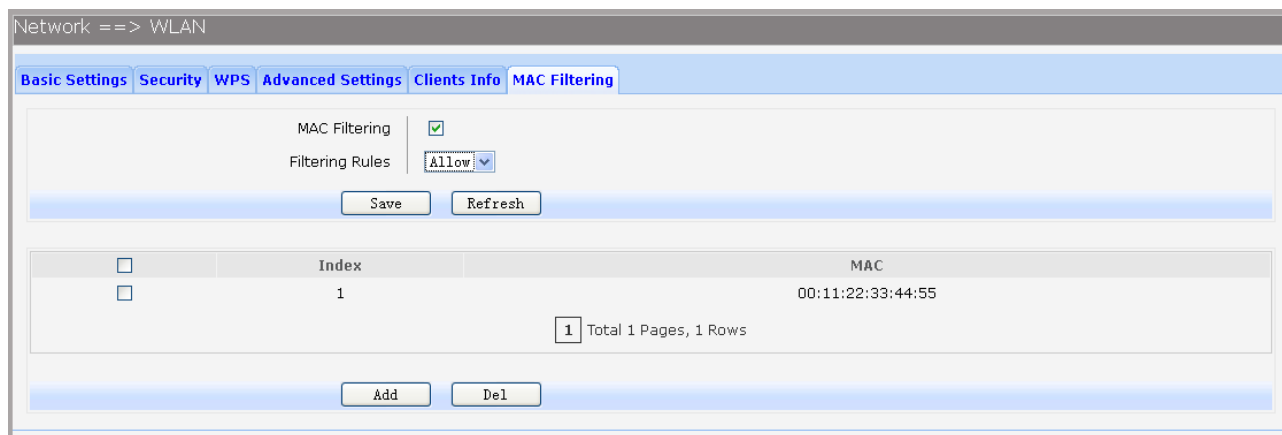
The following items are displayed on this screen:

- ▶ **MAC:** The MAC address of this client entry.
- ▶ **AID:** The AID(Association ID) field is a value assigned by an AP during association that represents the 16-bit ID of a STA.
- ▶ **Bandwidth:** Band width this client entry used.
- ▶ **SSID:** The SSID this client entry used when connecting WIFI.

### 3.3.4.6 MAC Filtering

You can control the wireless access by configuring the Wireless MAC Filtering function.

Choose the menu **Network**→**WLAN**→**MAC Filtering** to load the following page.



Network ==> WLAN

Basic Settings Security WPS Advanced Settings Clients Info **MAC Filtering**

MAC Filtering ☒

Filtering Rules **Allow**

Save Refresh

<input type="checkbox"/>	Index	MAC
<input type="checkbox"/>	1	00:11:22:33:44:55

1 Total 1 Pages, 1 Rows

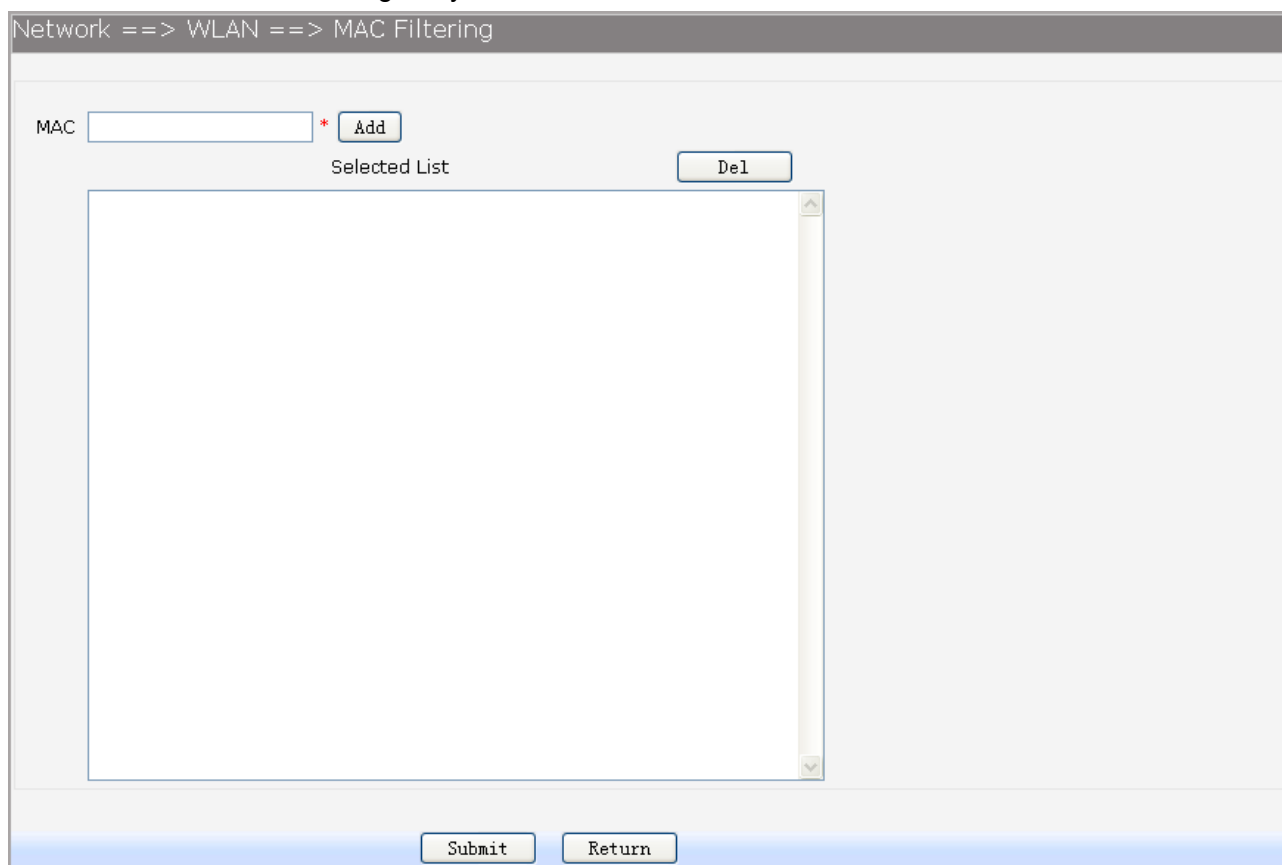
Add Del

**Figure 3-22 View Wifi MAC Filtering**

The following items are displayed on this screen:

- ▶ **MAC Filtering:** Enable or disable the Wifi MAC filtering function globally.
- ▶ **Filtering Rules:** Two MAC filtering rules are provided:
  - Allow:** allow the stations specified by entries in the list to access.
  - Deny:** deny the stations specified by entries in the list to access.

To delete Wireless MAC Address filtering entries, select the entries and click the **Del** button. To Add a Wireless MAC Address filtering entry, click the **Add** button.



Network ==> WLAN ==> MAC Filtering

MAC  \* **Add**

Selected List **Del**

Submit Return

**Figure 3-23 Add WIFI MAC Filtering Entry**

Enter the appropriate MAC Address into the **MAC** field. The format of the MAC Address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit). Click **Add** button to add MAC address to the **Selected List**, click **Del** button to delete the selected MAC address in the **Selected List**.

### 3.3.5 3G Modem

Typically, 3G Modem WAN is used as uplink port as a backup. When inserting 3G Modem into USB port, the system recognized the SIM card and charges no problem. After dialing successful, 3G Modem will serve as a backup uplink usage.

#### 1) Basic Settings

Choose the menu **Network→3G Modem** to load the following page.

The screenshot shows a web-based configuration interface for a 3G Modem. The title bar reads 'Network ==> 3G Modem'. Below it, the section 'Basic Settings' is displayed. The settings are as follows:

Field	Value	Notes
SP Network	Other (dropdown)	
Username	card	(Maximum 32 Characters)
Password	••••	(Maximum 32 Characters)
Dial Number	*99#	(Maximum 32 Characters)
APN	3GNET	(Maximum 32 Characters)
PIN	1234	(Maximum 32 Characters)
Connect Mode	Auto (dropdown)	
Online Mode	Always Online (dropdown)	

**Figure 3-24 Configure 3G Modem-Basic Settings**

The following items are displayed on this screen:

- ▶ **SP Network:** **Other** or **Swisscom**. If it is not the target user, you need to select the other.
- ▶ **Connect Mode:** **Manual** or **Auto**. The default is Auto.
- ▶ **Online Mode:** **always online** and **disconnect after idle interval**. The default is “always online”.  
The default idle interval is 60 seconds.

If **Other** is selected, the following parameters appear:

- ▶ **Username:** 3G network dial-up username.
- ▶ **Password:** 3G network dial-up password.
- ▶ **Dial Number:** 3G network dial numbers.
- ▶ **APN:** 3G network access APN.
- ▶ **PIN:** 3G networks need to use dial-up PIN code, if not, can be set to empty.

#### 2) Advanced Parameters

Choose the menu **Network→3G Modem→Advanced Parameters** to load the following page.

[Advanced Parameters](#)

Authentication	Auto
DNS	
TCP MSS	1460 [128,2048],default:1460
MTU	1500 [128,1500],default:1500
Data Link Backup	<input type="checkbox"/>
Heartbeat Address	

**Figure 3-25 Configure 3G Modem-Advanced Parameters**

The following items are displayed on this screen:

- ▶ **Authentication:** 3G dial-up authentication, **CHAP**, **PAP**, **Auto** are provided. Default is **Auto**.
- ▶ **DNS:** The default is obtained from the dial-up network devices automatically. You can also configure DNS manually.
- ▶ **TCP MSS:** Configure TCP maximum segment, we recommend using the default value.
- ▶ **MTU:** Configure 3G link MTU, the default value is recommended
- ▶ **Data Link Backup:** When enabled, if WAN uplink port is disconnected, the routing switches to the 3G link.
- ▶ **Heartbeat Address:** Set the heartbeat detecting address of the link, the default configuration is not required.

### 3) Status

Status

Device Status	Ready
SIM Card Status	Ready
Product Name	E353
Manufacturer Name	huawei
SP Name	CHN-CUGSM
Signal Quality	17 
Connection Status	Connected

**Figure 3-26 Configure 3G Modem-Status**

The following items are displayed on this screen:

- ▶ **Device Status:** Indicates whether to insert 3G module.
- ▶ **SIM Card Status:** Indicates whether to insert 3G modem in the SIM card, the ready state means the SIM card is detected.
- ▶ **Product Name:** 3G modem Product Type.
- ▶ **Manufacturer Name:** 3G modem vendor name.
- ▶ **SP Name:** 3G modem service provider name.
- ▶ **Signal Quality:** Signal quality of 3G Modem, up to 31.
- ▶ **Connection Status:** Connected or disconnected.

### 3.3.6 Port Management

#### 3.3.6.1 Port Mirror

Port Mirror, the packets obtaining technology, functions to forward copies of packets from one/multiple ports (mirrored port) to a specific port (mirroring port). Usually, the mirroring port is connected to a data diagnose device, which is used to analyze the mirrored packets for monitoring and troubleshooting the network.

Choose the menu **Network**→**Port Management**→**Port Mirror** to load the following page.

The screenshot shows the 'Port Mirror' configuration page. At the top, there is a breadcrumb 'Network ==> Port Management'. Below it are two tabs: 'Port Mirror' (selected) and 'Media Type'. The main content area contains the following settings:

- Enable Port Mirror:** A checkbox that is checked.
- Destination Port:** Radio buttons for WAN, LAN 1, LAN 2, LAN 3, and LAN 4. LAN 1 is selected.
- Source Port:** Checkboxes for WAN, LAN 2, LAN 3, and LAN 4. WAN is checked.

At the bottom right of the form is a 'Save' button.

**Figure 3-27 Port Mirror**

The following items are displayed on this screen:

- ▶ **Enable Port Mirror:** Enable or disable port mirror.
- ▶ **Destination Port:** The duplicate of packets from **Source Port** will send to this destination port.
- ▶ **Source Port:** All packets received from **Source Port** will be duplicated and the duplicate will be send to **Destination Port**.

#### 3.3.6.2 Media Type

Choose the menu **Network**→**Port Management**→**Media Type** to load the following page.

The screenshot shows the 'Media Type' configuration page. At the top, there is a breadcrumb 'Network ==> Port Management'. Below it are two tabs: 'Port Mirror' and 'Media Type' (selected). The main content area is divided into two sections:

- Media Type:** A table with columns for port labels and their configured media types.
- Current Status:** A table showing the current operational status of each port.

Port	Media Type	Current Status
WAN	Auto-Negotiation	1000Mbps, Full Duplex
LAN1	Auto-Negotiation	Link Down!
LAN2	Auto-Negotiation	Link Down!
LAN3	Auto-Negotiation	100Mbps, Full Duplex
LAN4	Auto-Negotiation	100Mbps, Full Duplex

At the bottom of the page are 'Save' and 'Refresh' buttons.



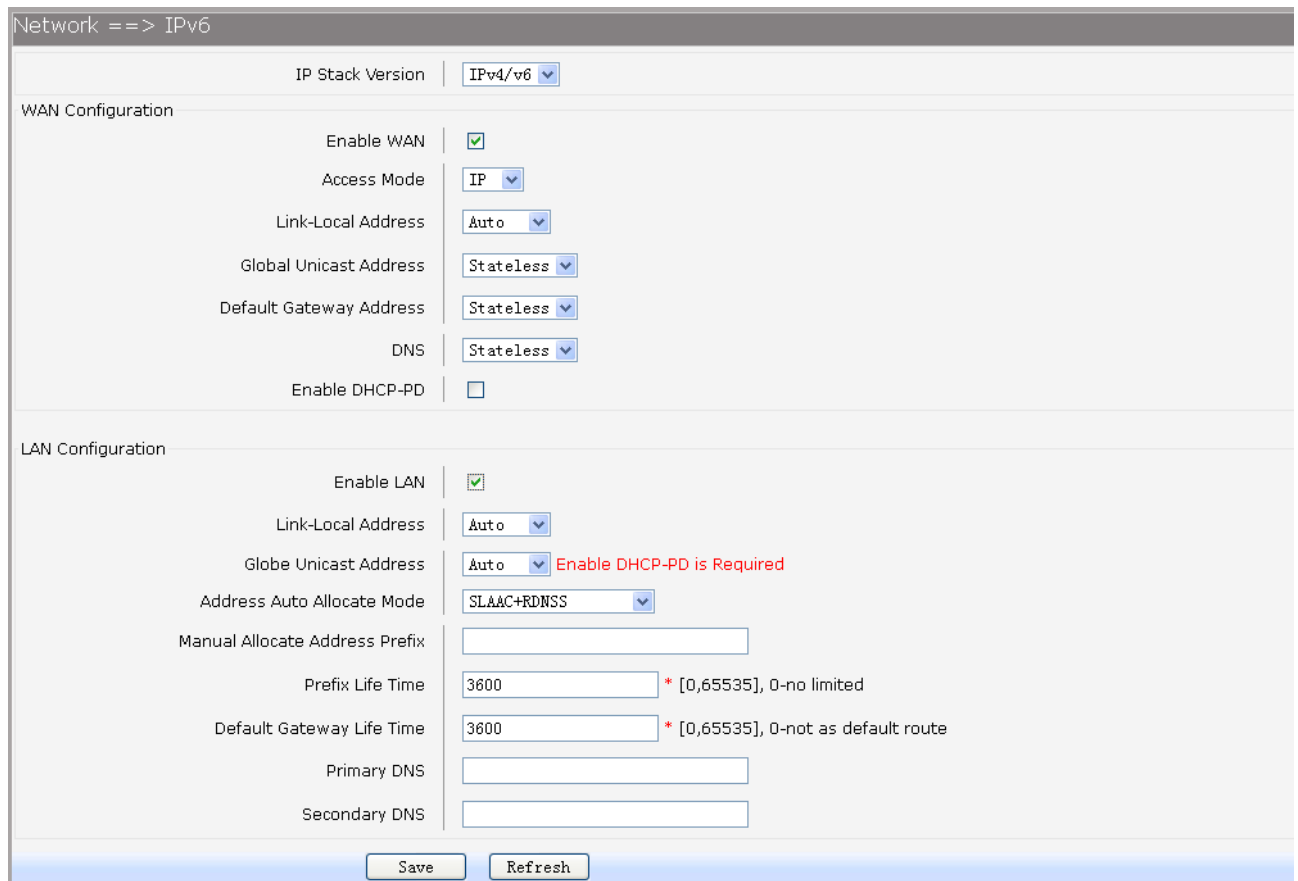
**Figure 3-28 Media Type**

The following items are displayed on this screen:

- ▶ **Media Type:** provides the following six modes to all physical ports: 10M Half Duplex, 10M Full Duplex, 100M Half Duplex, 100M Full Duplex, 1000M Full Duplex, Auto-Negotiation.
- ▶ **Current Status:** Current link status of all physical ports. Read only.

### 3.3.7 IPv6 Configuration

Choose the menu **Network**→**IPv6** to load the following page.


**Figure 3-29 Configure IPv6**

The following items are displayed on this screen:

- ▶ **IP Stack Version:** Choose the IP stack version to use. Provides the following three types: **IPv4**, **IPv6**, **IPv4/v6**.

#### WAN Configuration

- ▶ **Enable WAN:** If IPv6 or IPv4/v6 is chosen, select this to enable IPv6 stack on WAN.
- ▶ **Access Mode:** Select access mode of WAN: **IP** or **PPP**.
- ▶ **Link-Local Address:** Select type of Link-Local address: **Auto** or **Manual**. If Manual is selected, you should specify address manually.
- ▶ **Global Unicast Address:** **Stateless**, **Manual**, **DHCPv6**. If Manual is selected, you should specify address manually.
- ▶ **Default Gateway Address:** **Stateless**, **Manual**. If Manual is selected, you should specify address manually.
- ▶ **DNS:** **Stateless**, **Manual**, **DHCPv6**. If Manual is selected, you should specify

DNS manually.

- **Enable DHCP-PD:** Whether to enable **DHCP-PD**(prefix delegation) on WAN.

### LAN Configuration

- **Enable LAN:** If IPv6 or IPv4/v6 is chosen, select this to enable IPv6 stack on LAN.
- **Link-Local Address:** Select type of Link-Local address: **Auto** or **Manual**. If Manual is selected, you should specify address manually.
- **Global Unicast Address:** **Manual,Auto**. If Manual is selected, you should specify address manually.
- **Address Auto Allocate Mode:** **SLAAC+RDNSS**(Recursive DNS Server)  
**SLAAC**(Stateless address autoconfiguration)+**DHCPv6**  
**DHCPv6**
- **Manual Allocate Address Prefix:** Configure the manual allocate address prefix.
- **Prefix Life Time:** Enter the life time of prefix.
- **Default Gateway Life Time:** Enter the life time of default gateway.
- **Primary DNS:** Enter the primary DNS address.
- **Secondary DNS:** Enter the secondary DNS address.

## 3.4 Data Service

### 3.4.1 Status

The Status page shows the data services information, all information is read only.

#### 3.4.1.1 Service State

The Service State page show all switch status of data services.

Choose the menu **Data Service**→**Status**→**Service State** to load the following page.

**Figure 3-30 Service State**

#### 3.4.1.2 ARP Table

This page displays the ARP List;

Choose the menu **Data Service**→**Status**→**ARP Table** to load the following page.

Data Service ==> Status

Service State	ARP Table	Route Table	Net State
IP Address	Flag	HW Address	Interface
192.168.111.221	0x2	00:22:33:44:55:02	eth2.7
192.168.1.66	0x0	00:00:00:00:00:00	br0
192.168.1.121	0x2	00:0d:88:48:b4:1f	br0
192.168.1.65	0x0	00:00:00:00:00:00	br0

1 Total 1 Pages, 4 Rows

Figure 3-31 ARP Table

### 3.4.1.3 Route Table

Choose the menu **Data Service**→**Status**→**Route Table** to load the following page.

Data Service ==> Status

Service State	ARP Table	Route Table	Net State
Index	interface		
1	from all lookup local		
2	from all lookup 1		
3	from all fwmark 0x3e8 lookup 2		
4	from all fwmark 0x3e9 lookup 3		
5	from all fwmark 0x3ea lookup 4		
6	from all lookup main		
7	from all lookup default		

1 Total 1 Pages, 7 Rows

Figure 3-32 Route Table

### 3.4.1.4 Net State

Choose the menu **Data Service**→**Status**→**Net State** to load the following page.

Data Service ==> Status

Protocol	Local Address	Foreign Address	State
TCP	0.0.0.0:1900	0.0.0.0:0	TCP_LISTEN
TCP	0.0.0.0:9100	0.0.0.0:0	TCP_LISTEN
TCP	0.0.0.0:80	0.0.0.0:0	TCP_LISTEN
TCP	0.0.0.0:22	0.0.0.0:0	TCP_LISTEN
TCP	0.0.0.0:23	0.0.0.0:0	TCP_LISTEN
TCP	0.0.0.0:24	0.0.0.0:0	TCP_LISTEN
TCP	192.168.1.1:80	192.168.1.1:2742	TCP_TIME_WAIT
TCP	192.168.1.1:80	192.168.1.1:2739	TCP_TIME_WAIT
TCP	192.168.1.1:80	192.168.1.1:2746	TCP_TIME_WAIT
TCP	192.168.1.1:80	192.168.1.1:2744	TCP_TIME_WAIT
TCP	192.168.1.1:80	192.168.1.1:2766	TCP_ESTABLISHED
TCP	192.168.1.1:80	192.168.1.1:2740	TCP_TIME_WAIT
TCP	192.168.1.1:80	192.168.1.1:2753	TCP_TIME_WAIT
TCP	192.168.1.1:80	192.168.1.1:2752	TCP_TIME_WAIT
TCP	192.168.1.1:80	192.168.1.1:2743	TCP_TIME_WAIT
TCP	192.168.1.1:80	192.168.1.1:2750	TCP_TIME_WAIT
TCP	192.168.1.1:80	192.168.1.1:2751	TCP_TIME_WAIT
TCP	192.168.1.1:80	192.168.1.1:2749	TCP_TIME_WAIT
TCP	192.168.1.1:80	192.168.1.1:2748	TCP_TIME_WAIT
TCP	192.168.1.1:80	192.168.1.1:2755	TCP_TIME_WAIT

Navigation: |< << 1 2 >> >| Total 2 Pages, 40 Rows

Figure 3-33 Net State

### 3.4.2 DHCP Server

#### 3.4.2.1 Static Address Assign

Choose the menu **Data Service**→**DHCP Server**→**Static Address Assign**, and then you can view and add address which is assigned for clients. When you specify a static IP address for a client on the LAN, that client will always receive the same IP address each time when it accesses the DHCP server. The Reserved IP addresses should be assigned to the devices that require permanent IP settings.

Data Service ==> DHCP Server

Static Address Assign					
	Index	IP	Netmask	MAC	Description
<input type="checkbox"/>	1	192.168.0.30	255.255.0.0	01:02:03:04:05:06	Client1

Navigation: 1 Total 1 Pages, 1 Rows

Buttons: Add Del

Figure 3-34 View Static Address Assign Configuration

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

Data Service ==> DHCP

Client IP Address	<input type="text" value="192.168.0.30"/>	* For example: 192.168.0.30
Client Mask	<input type="text" value="255.255.0.0"/>	* For example: 255.255.0.0
Client MAC	<input type="text" value="01:02:03:04:05:06"/>	* For example: 01:02:03:04:05:06
Description	<input type="text" value="Client1"/>	

**Figure 3-35 Add or Modify An Static Address Assign Entry**

The following items are displayed on this screen:

- ▶ **Client IP Address:** The IP address reserved.
- ▶ **Client Mask:** The subnet mask of IP address reserved.
- ▶ **Client MAC:** The MAC address you want to reserve IP address.
- ▶ **Description:** The description of the entry to add or modify.

### 3.4.2.2 Status

Choose the menu **Data Service**→**DHCP Server**→**Status**, and then you can view the information about the clients attached to the DHCP server.

Data Service ==> DHCP Server

<b>Static Address Assign</b>	<b>Status</b>	<b>DHCP Relay</b>
------------------------------	---------------	-------------------

Index	IP	MAC	Host Name
1	192.168.111.220	00:66:4b:2e:00:52	android-317afa1415717027

1 Total 1 Pages, 1 Rows

**Figure 3-36 DHCP Client Status**

### 3.4.2.3 DHCP Relay

A DHCP relay agent is any host that forwards DHCP packets between clients and servers. Relay agents are used to forward requests and replies between clients and servers when they are not on the same physical subnet. Relay agent forwarding is distinct from the normal forwarding of an IP router, where IP datagrams are switched between networks somewhat transparently. By contrast, relay agents receive DHCP messages and then generate a new DHCP message to send on another interface. It listens for client requests and adds vital configuration data, such as the client's link information, which is needed by the server to allocate the address for the client. When the DHCP server responds, the DHCP relay agent forwards the reply back to the DHCP client.

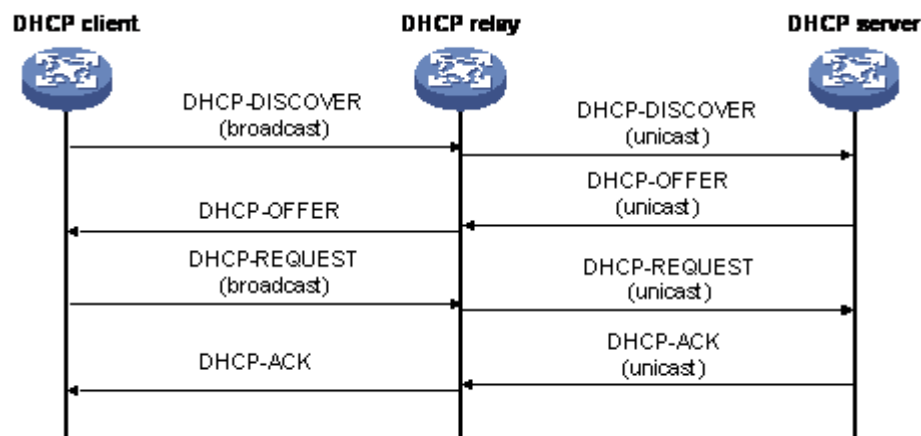


Figure 3-37 DHCP Relay Overview

Choose the menu **Data Service**→**DHCP Server**→**DHCP Relay** to load the following page.

Data Service ==> DHCP Server	
Static Address Assign Status <b>DHCP Relay</b>	
Enable DHCP Relay	<input checked="" type="checkbox"/>
Client Interface 1	VLAN1
Client Interface 2	none
Client Interface 3	none
Client Interface 4	none
Server Interface	DATA
Server IP	138.0.60.2
<input type="button" value="Save"/> <input type="button" value="Refresh"/>	

Figure 3-38 Configure DHCP Relay

The following items are displayed on this screen:

- ▶ **Enable DHCP Relay:** Enable or disable DHCP Relay.
- ▶ **Client Interface:** The interface to listen for DHCP client requests. Up to four interfaces can be selected.
- ▶ **Server Interface:** Choose the interface which connects DHCP server.
- ▶ **Server IP:** Configure the DHCP server IP address.

### 3.4.3 NAT Config

**Network Address Translation (NAT)** is a network protocol used in IPv4 networks that allows multiple devices to connect a network protocol using the same public IPv4 address. NAT was originally designed in an attempt to help conserve IPv4 addresses. NAT modifies the IP address information in IPv4 headers while in transit across a traffic routing device.

#### 3.4.3.1 Basic Settings

Choose the menu **Data Service**→**NAT Config**→**Basic Settings** to load the following page.

Data Service ==> Basic Settings

Max Nat Connections	<input type="text" value="16000"/> [512~16000]
Enable MSS Auto Adaptive	<input type="checkbox"/>
TCP MSS	<input type="text" value="1260"/> [1260~1460]

**Figure 3-39 Basic Settings**

The following items are displayed on this screen:

- ▶ **Max Nat Connections:** Specify the maximum number of NAT connections.
- ▶ **Enable MSS Auto Adaptive:** Enable or disable auto adaptive the value of MSS(Maximum Segment Size).
- ▶ **TCP MSS:** If **Enable MSS Auto Adaptive** is not selected, configure this to specify the maximum segment size of the TCP protocol.

### 3.4.3.2 PAT Settings

Several internal addresses can be NATed to only one or a few external addresses by using a feature called overload, which is also referred to as PAT. PAT is a subset of NAT functionality, where it maps several internal addresses to a single external address. PAT statically uses unique port numbers on a single outside IP address to distinguish between the various translations.

Choose the menu **Data Service**→**NAT Config**→**PAT Settings** to load the following page.

Data Service ==>PAT Settings

Enable PAT ☒

<input type="checkbox"/>	Index	Enable	Protocol	Internet Interface	Internet Port	Intranet IP	Intranet Port	Description
<input type="checkbox"/>	1	Enable	TCP	DATA	90	10.0.1.2	9090	test

Total 1 Pages, 1 Rows

**Figure 3-40 View PAT Settings**

The following items are displayed on this screen:

- ▶ **Enable PAT:** Enable or disable PAT globally.

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

Data Service ==> PAT Settings

Enable	<input checked="" type="checkbox"/>
Internet Port	<input type="text" value="90"/> * [1~65535]
Intranet Port	<input type="text" value="9090"/> * [1~65535]
Intranet IP	<input type="text" value="10.0.1.2"/> * e.g.155.55.0.23
Protocol	<input type="text" value="TCP"/>
Internet Interface	<input type="text" value="DATA"/>
Description	<input type="text" value="test"/>

**Figure 3-41 Add or Modify PAT Entry**

The following items are displayed on this screen:

- ▶ **Enable:** Enable or disable this PAT entry.
- ▶ **Internet Port:** Enter the service port provided for accessing external network. All the requests from internet to this service port will be redirected to the specified server in local network.
- ▶ **Intranet Port:** Specify the service port of the LAN host as virtual server.
- ▶ **Intranet IP:** Enter the IP address of the specified internal server for the entry. All the requests from the internet to the specified LAN port will be redirected to this host.
- ▶ **Protocol:** Specify the protocol used for the entry.
- ▶ **Internet Interface:** Specify the interface to receive requests from the internet for the entry.
- ▶ **Description:** Enter a name for Virtual Server entry.

### 3.4.3.3 DMZ Settings

In computer security, a DMZ or Demilitarized Zone (sometimes referred to as a perimeter network) is a physical or logical network that contains and exposes an organization's external-facing services to a larger and insecure network, usually the Internet. The purpose of a DMZ is to add an additional layer of security to an organization's local area network (LAN); an external attacker only has direct access to equipment in the DMZ, rather than any other part of the network.

Choose the menu **Data Service**→**NAT Config**→**DMZ Settings** to load the following page.

The screenshot shows the 'Data Service ==> DMZ Settings' page. At the top, there is a checkbox for 'Enable DMZ' which is currently unchecked. Below this are 'Save' and 'Refresh' buttons. A table lists DMZ entries with columns for 'Index', 'Public IP', 'Private IP', and 'Description'. The table contains one entry with Index 1, Public IP 10.0.11.11, Private IP 192.168.1.2, and Description 'test'. Below the table is a pagination bar showing '1 Total 1 Pages, 1 Rows'. At the bottom are 'Add' and 'Del' buttons.

	Index	Public IP	Private IP	Description
<input type="checkbox"/>	1	10.0.11.11	192.168.1.2	test

**Figure 3-42 View DMZ Settings**

The following items are displayed on this screen:

- ▶ **Enable DMZ:** Enable or disable DMZ globally.

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

The screenshot shows the 'Data Service ==> DMZ Settings' page for adding or modifying an entry. It features three input fields: 'DMZ Public IP' with the value '10.0.11.11', 'DMZ Private IP' with the value '192.168.1.2', and 'Description' with the value 'test'. Each IP field has a red asterisk indicating it is required. At the bottom are 'Save' and 'Return' buttons.

**Figure 3-43 Add or Modify DMZ Entry**

The following items are displayed on this screen:



- ▶ **DMZ Public IP:** The public IP address for this DMZ entry.
- ▶ **DMZ Private IP:** The private IP address for this DMZ entry.
- ▶ **Description:** Enter a description string for this DMZ entry

#### 3.4.3.4 ALG Settings

**Application Layer Gateway (ALG)** allows customized Network Address Translation (NAT) traversal filters to be plugged into the gateway to support address and port translation for certain application layer "control/data" protocols such as FTP, H.323, PPTP, etc.

Choose the menu **Data Service**→**NAT Config**→**ALG Settings** to load the following page.

Data Service ==> ALG Parameter	
Enable SIP	<input type="checkbox"/>
Enable H323	<input checked="" type="checkbox"/>
Enable FTP	<input checked="" type="checkbox"/>
Enable PPTP	<input checked="" type="checkbox"/>
Enable RTSP	<input checked="" type="checkbox"/> Server Port <input type="text" value="554"/> [1,65535]

Save Refresh

**Figure 3-44 ALG Settings**

The following items are displayed on this screen:

- ▶ **Enable SIP:** Enable or disable SIP ALG.
- ▶ **Enable H323:** Allow Microsoft NetMeeting clients to communicate across NAT if selected.
- ▶ **Enable FTP:** Allow FTP clients and servers to transfer data across NAT if selected.
- ▶ **Enable PPTP:** Enable or disable PPTP ALG.
- ▶ **Enable RTSP:** Enable or disable RTSP ALG.

#### 3.4.4 Firewall Config

##### 3.4.4.1 Attack Defense

With Attack Defense function enabled, the device can distinguish the malicious packets and prevent the port scanning from external network, so as to guarantee the network security. Configure this for abnormal packets defense and flood attack defense. Flood attack is a commonly used DoS (Denial of Service) attack, including TCP SYN, UDP, ICMP, and so on.

Choose the menu **Data Service**→**Firewall Config**→**Attack Defense** to load the following page.

Data Service ==> Attack Defense

Enable Broadcast Storm Defense	<input type="checkbox"/>
Enable Block Ping	<input type="checkbox"/>
Enable TCP SYN Flood Defense	<input checked="" type="checkbox"/> 20 [1~1000](packets/second)
Enable UDP Flood Defense	<input type="checkbox"/> 50 [1~1000](packets/second)
Enable ICMP Defense	<input checked="" type="checkbox"/> 10 [1~1000](packets/second)
Enable ARP Attack Defense	<input type="checkbox"/>
Enable Port Scan Defense	<input type="checkbox"/>
Enable Land Based Defense	<input type="checkbox"/>
Enable Ping Of Death Defense	<input type="checkbox"/>
Enable Teardrop Defense	<input type="checkbox"/>
Enable Fraggle Defense	<input type="checkbox"/>
Enable Smurf Defense	<input type="checkbox"/>

Save Refresh

**Figure 3-45 Attack Defense**

The following items are displayed on this screen:

- ▶ **Enable Broadcast Storm Defense:** Enable or disable **Broadcast Storm Defense**.
- ▶ **Enable Block Ping:** Enable or disable **Block Ping** function.
- ▶ **Enable TCP SYN Flood Defense:** Enable or disable **TCP SYN Flood Defense**.
- ▶ **Enable UDP Flood Defense:** Enable or disable **UDP Flood Defense**.
- ▶ **Enable ICMP Defense:** Enable or disable **ICMP Defense**.
- ▶ **Enable ARP Attack Defense:** Enable or disable **ARP Attack Defense**.
- ▶ **Enable Port Scan Defense:** A port scanner is a software application designed to probe a server or host for open ports. Check the box to prevent port scanning.
- ▶ **Enable Land Based Defense:** The Land Denial of Service attack works by sending a spoofed packet with the SYN flag - used in a "handshake" between a client and a host - set from a host to any port that is open and listening. If the packet is programmed to have the same destination and source IP address, when it is sent to a machine, via IP spoofing, the transmission can fool the machine into thinking it is sending itself a message, which, depending on the operating system, will crash the machine. Check the box to enable **Land Based Defense**.
- ▶ **Enable Ping Of Death Defense:** Ping of death is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol. Check the box to enable **Ping of Death Defense**.
- ▶ **Enable Teardrop Defense:** Teardrop is a program that sends IP fragments to a machine connected to the Internet or a network. Check the box to enable **Teardrop Defense**.
- ▶ **Enable Fraggle Defense:** A fraggle attack is a variation of a Smurf attack where an attacker sends a large amount of UDP traffic to ports 7 (echo) and 19 (chargen) to an IP Broadcast Address, with the

► **Enable Smurf Defense:**

intended victim's spoofed source IP address. Check the box to enable **Fraggle Defense**.

The Smurf Attack is a denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Check the box to enable **Smurf Defense**.

### 3.4.4.2 Service Type

**Service Type** defines the entry with protocol and port range, which can be chosen in Internet Access-Ctrl page. Choose the menu **Data Service→Firewall Config→Service Type** to load the following page.

<input type="checkbox"/>	Index	Name	Protocol	Port Range	Description
<input type="checkbox"/>	1	type1	TCP	1000-2000	test

1 Total 1 Pages, 1 Rows

Add Del

**Figure 3-46 View Service Type Configuration**

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

Data Service ==> Firewall

Name: type1 \*

Protocol: TCP

Port Range: 1000 -- 2000 \* [1~65535]

Description: test

Save Return

**Figure 3-47 Add or Modify Service Type Entry**

The following items are displayed on this screen:

- **Name:** Name of this entry, it will be list in Internet Access-Ctrl page.
- **Protocol:** Select the protocol for this entry. Four types are provided: TCP, UDP, ICMP and ALL.
- **Port Range:** Configure the port range for this entry.
- **Description:** Enter a description string for this entry

### 3.4.4.3 Internet Access-Ctrl

Each sub-page under this page is used to control Internet access.

#### 3.4.4.3.1 Access Control

This sub-page is used to control Internet access through IP, port, and time.

Choose the menu **Data Service→Firewall Config→Internet Access-Ctrl→Access Control** to load the following page.

DataService ==> Internet Access-Ctrl

**Access Control** | User Authentication | Page Push

Enable Access Control ☒

Policy **Allow**

**Save** **Refresh**

<input type="checkbox"/>	Index	Enable	Src IP Range	Dst IP Range	Service Name	Active Time	Description
<input type="checkbox"/>	1	Enable	10.0.1.1--...	192.168.100.1--...	type1	00:00--23:59 (...)	rule1

1 Total 1 Pages, 1 Rows

**Add** **Del**

**Figure 3-48 View Access Control Entry**

The following items are displayed on this screen:

- ▶ **Enable Access Control:** Enable or disable access control from WAN.
- ▶ **Policy:** Default policy of access control: **Allow** or **Deny**. If Allow is selected, all packets will be allowed except the entries list on this page. If Deny is selected, all packets will be denied except the entries list on this page.

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

DataService ==> Access Control

Action Deny

Enable Rule ☒

Description rule1

Source IP Range 10.0.1.1 to 10.0.1.200

Destination IP Range 192.168.100.1 to 192.168.100.200

Service Name type1

Active Time 00:00 --23:59 (hh:mm)

Active Day ☒ All ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

**Save** **Return**

**Figure 3-49 Add or Modify Access Control Entry**

The following items are displayed on this screen:

- ▶ **Action:** The policy of this entry, Allow or Deny. It is the inverse of **Policy**. Read only.
- ▶ **Enable Rule:** Enable or disable this rule.
- ▶ **Description:** Enter a description string for this rule
- ▶ **Source IP Range:** Enter the source IP range in dotted-decimal format (e.g. 192.168.1.23).
- ▶ **Destination IP Range:** Enter the destination IP range in dotted-decimal format (e.g. 192.168.1.23).
- ▶ **Service Name:** Choose a service type that defined in **Service Type** page.
- ▶ **Active Time:** Specify the time range for the entry to take effect.
- ▶ **Active Day:** Specify the day range for the entry to take effect.

### 3.4.4.3.2 User Authentication

This sub-page is used to control Internet access through username and password.

Choose the menu **Data Service**→**Firewall Config**→**Internet Access-Ctrl**→**User Authentication** to load the following page.

Index	Username	Password
1	gaoke	gktel

**Figure 3-50 View User Authentication Entry**

The following items are displayed on this screen:

- **Enable User Authentication:** Enable or disable user authentication globally. If enabled, only the following list of users and passwords can access the Internet. Press **Save** button if you have modified this parameter.

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

**Figure 3-51 Add or Modify User Authentication Entry**

The following items are displayed on this screen:

- **Username:** Enter the username of this entry.
- **Password:** Enter the password of this entry.
- **Auth Mode:** Choose the authentication mode of this entry. Provides four modes:
  - Allow Multi-PC Access:** Allows multiple computers to access the Internet using this account.
  - Allow One PC Access:** Only allows one computer to access the Internet using this account.
  - Allow Special IP Access:** Allowing only specified IP computer uses this account to access the Internet.
  - Allow Special MAC Access:** Allowing only specified MAC computer uses this account to access the Internet

### 3.4.4.3.3 Page Push

HTTP Page push is a mechanism for sending unsolicited (asynchronous) data from web server to a web browser. When accessing the Internet for the first time, the specified HTTP page will be pushed to the browser when enabled.

Choose the menu **Data Service**→**Firewall Config**→**Internet Access-Ctrl**→**Page Push** to load the following page.

**Figure 3-52 Configure Page Push**

The following items are displayed on this screen:

- **Enable Page Push:** If enabled, push specified HTTP page to the browser when accessing the Internet for the first time.
- **Push Http Url:** Specifies the HTTP URL of the page you want to push.

### 3.4.4.4 Network Access-Ctrl

#### 3.4.4.4.1 WEB

Choose the menu **Data Service**→**Firewall Config**→**Network Access-Ctrl**→**WEB** to load the following page.

**Figure 3-53 Configure WEB Access-Ctrl**

The following items are displayed on this screen:

- **HTTP Port:** Port used with HTTP access device.  
**HTTP:** Hypertext Transfer Protocol.

- ▶ **HTTPS Port:** Port used with HTTPS access device.  
**HTTPS:** it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol.

#### Internet Web Access:

- ▶ **Allow Access:** If enabled, allow user to access the device from the Internet via WEB.
- ▶ **IP Limit:** If enabled, allow only specific IP range to access the device from the Internet via WEB.
- ▶ **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that is only allowed to access to the device from the Internet via WEB.
- ▶ **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that is only allowed to access to the device from the Internet via WEB.

#### Intranet Web Access:

- ▶ **Allow Access:** If enabled, allow user to access the device from the Intranet via WEB.
- ▶ **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via WEB.
- ▶ **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that is only allowed to access the device from the Intranet via WEB.
- ▶ **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that is only allowed to access the device from the Intranet via WEB.

#### 3.4.4.4.2 TELNET

Choose the menu **Data Service**→**Firewall Config**→**Network Access-Ctrl**→**TELNET** to load the following page.

The screenshot shows the 'Data Service ==> Network Access-Ctrl' configuration page for TELNET. It has tabs for WEB, TELNET, and SSH. The TELNET tab is active. At the top, there is a 'Port' field set to 23 with a range of [1~65535]. Below this, there are two sections: 'Internet Telnet Access' and 'Intranet Telnet Access'. Each section has a table of settings:

Section	Allow Access	IP Limit	IP Range	IPv6 Range
Internet Telnet Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	138.0.60.1 -- 138.0.255.255	2001::60 -- 2001::ffff
Intranet Telnet Access	<input checked="" type="checkbox"/>	<input type="checkbox"/>	192.168.1.2 -- 192.168.1.255	2001::60 -- 2001::ffff

At the bottom of the page, there are 'Save' and 'Refresh' buttons.

**Figure 3-54 Configure Telnet Access-Ctrl**

The following items are displayed on this screen:

- ▶ **Port:** Port when using telnet tools access device.

#### Internet Web Access:

- ▶ **Allow Access:** If enabled, allow access to the device from the Internet via telnet.
- ▶ **IP Limit:** If enabled, allow only specific IP range to access the device from the Internet via telnet
- ▶ **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the

device from the Internet via telnet.

- ▶ **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that only allow access to the device from the Internet via telnet.

#### Intranet Web Access:

- ▶ **Allow Access:** If enabled, allow access to the device from the Intranet via telnet.
- ▶ **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via telnet
- ▶ **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Intranet via telnet.
- ▶ **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that only allow access to the device from the Intranet via telnet.

#### 3.4.4.4.3 SSH

Choose the menu **Data Service**→**Firewall Config**→**Network Access-Ctrl**→**SSH** to load the following page.

The screenshot shows the 'Data Service ==> Network Access-Ctrl' interface. The 'SSH' tab is selected. The 'Port' is set to 22. The 'Internet SSH Access' section has 'Allow Access' and 'IP Limit' disabled. The 'IP Range' is set to 138.0.60.1 -- 138.0.255.255, and the 'IPv6 Range' is set to 2001::60 -- 2001::ffff. The 'Intranet SSH Access' section has 'Allow Access' enabled (checked), 'IP Limit' disabled, 'IP Range' set to 192.168.1.255 -- 192.168.1.255, and 'IPv6 Range' set to 2001::60 -- 2001::ffff. 'Save' and 'Refresh' buttons are at the bottom.

**Figure 3-55 Configure SSH Access-Ctrl**

The following items are displayed on this screen:

- ▶ **Port:** Port when using SSH tools access device.

#### Internet Web Access:

- ▶ **Allow Access:** If enabled, allow access to the device from the Internet via SSH.
- ▶ **IP Limit:** If enabled, allow only specific IP range to access the device from the Internet via SSH
- ▶ **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Internet via SSH.
- ▶ **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that only allow access to the device from the Internet via SSH.

#### Intranet Web Access:

- ▶ **Allow Access:** If enabled, allow access to the device from the Intranet via SSH.
- ▶ **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via SSH



- **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Intranet via SSH.
- **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that only allow access to the device from the Intranet via SSH.

### 3.4.4.5 Filter Strategy

Each sub-page under this page is used to filter Internet access.

#### 3.4.4.5.1 Keyword Filter

Choose the menu **Data Service**→**Firewall Config**→**Filter Strategy**→**Keyword Filter** to load the following page.

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del.**

Click the **Add** button to add a new entry.

Data Service ==> Filter Strategy

Keyword Filter IP Filter MAC Filter

Keyword Filter ☒ Policy: Deny

Save Refresh

Index	Keyword
1	terrorist

1 Total 1 Pages, 1 Rows

Add Del

Import File Browse... Import Export

**Figure 3-56 Configure Keyword Filter**

The following items are displayed on this screen:

- **Keyword Filter:** If enabled, packet filtering is enabled by keyword.
  - **Policy:** The policy for filtering web page, Deny and Allow.
- You can export all the keywords as a file. Of course, you can also import a file.

#### 3.4.4.5.2 IP Filter

On this page, you can control the Internet access of local hosts by specifying their IP addresses.

Choose the menu **Data Service**→**Firewall Config**→**Filter Strategy**→**IP Filter** to load the following page.

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del.**

Click the **Add** button to add a new entry.

Data Service ==> Filter Strategy

**Keyword Filter** **IP Filter** **MAC Filter**

IP Filter ☒

Policy **Deny**

**Save** **Refresh**

<input type="checkbox"/>	Index	IPv4	IPv6
<input type="checkbox"/>	1	192.168.1.222	

1 Total 1 Pages, 1 Rows

**Add** **Del**

Import File **浏览...** 未选择文件。 **Import** **Export**

**Figure 3-57 Configure IP Filter**

The following items are displayed on this screen:

- **IP Filter:** If enabled, packet filtering is enabled by IP address.
- **Policy:** The policy for IP address list. Deny and Allow.

You can export all the IP addresses as a file. Of course, you can also import a file.

#### 3.4.4.5.3 MAC Filter

On this page, you can control the Internet access of local hosts by specifying their MAC addresses.

Choose the menu **Data Service**→**Firewall Config**→**Filter Strategy**→**MAC Filter** to load the following page.

Data Service ==> Filter Strategy

**Keyword Filter** **IP Filter** **MAC Filter**

MAC Filter ☒

Policy **Deny**

**Save** **Refresh**

<input type="checkbox"/>	Index	MAC
<input type="checkbox"/>	1	00:11:22:33:44:55

1 Total 1 Pages, 1 Rows

**Add** **Del**

Import File **浏览...** 未选择文件。 **Import** **Export**

**Figure 3-58 Configure MAC Filter**

The following items are displayed on this screen:

- **IP Filter:** If enabled, packet filtering is enabled by MAC.
- **Policy:** The policy for MAC list. Deny and Allow.

You can export all the MAC addresses as a file. Of course, you can also import a file.

If you want to delete an entry, select it and click the **Del**. Click the **Add** button to add a new entry.

There are two ways to add MAC:

**Artificial designated MAC:** You can manually enter a MAC.

**Using Studying MAC:** You can choose one or more MAC devices learned.

DataService ==> Filter Strategy ==> MAC Filter

☒ Artificial designated MAC  
MAC:  \*

☐ Using Studing MAC

Studed MAC

Selected List

>  
>>  
<  
<<

**Figure 3-59 Add a MAC Filter Entry**

#### 3.4.4.6 IP&MAC Binding

Choose the menu **Data Service**→**Firewall Config**→**IP&MAC Binding** to load the following page.

There are two ways to add a binding entry: You can manually enter a pair of IP and MAC, and then press **Add Item**. Alternatively you can select a pair of IP and MAC in **Scan List** that device learned.

Data Service ==> IP&MAC Binding

IP  MAC

Scan List

192.168.1.121	00:0d:88:48:b4:1f
192.168.1.65	00:00:00:00:00:00
192.168.111.221	00:22:33:44:55:02
192.168.1.66	00:00:00:00:00:00

Binding List

>  
>>  
<  
<<

**Figure 3-60 Configure IP&MAC Binding**

### 3.4.5 QoS

#### 3.4.5.1 Basic Settings

QOS feature is enabled by default, based on 802.1P, strict priority scheduling mode. The device supports four priority queues, when QoS feature enabled.

Choose the menu **Data Service**→**QoS**→**Basic Settings** to load the following page.

**Figure 3-61 Configure QoS Basic Settings**

The following items are displayed on this screen:

#### Global Parameters

► **QoS Enable:**

Enable or disable QoS functionality.

► **Scheduling Mode:**

**PQ:** PQ means strict priority, that is, when congestion occurs, first sending packets of high priority queue.

**WRR:** All queues use weighted fair queuing scheme which is defined in **Weight Ratio**

**PQ+WRR:** Only highest queue use strict priority; others use weighted fair queuing scheme.

► **QoS Priority:**

**DSCP:** When you select DSCP value, corresponding to the following relationship.

DSCP priority value	Priority queue (queue 3 highest priority)
0-15	Queue 0
16 ~ 31	Queue 1
32 to 47	Queue 2
48 ~ 63	Queue 3

**802.1P:** Select the queue classification mode, when selecting 802.1P mode, depending on the value of 802.1p priority classification into different queues, corresponding to the following relationship.

801.1p priority value	Priority queue (queue 3 highest priority)
0 to 1	Queue 0
2.3	Queue 1
4.5	Queue 2
6-7	Queue 3

### Bandwidth Setting

- ▶ **Upstream Bandwidth:** Configure the bandwidth of upstream.
- ▶ **Downstream Bandwidth:** Configure the bandwidth of downstream.

### Advanced Parameters

- ▶ **Enable Voice Reservation:** Enable voice reservation and give the value to reserved for voice
- ▶ **Enable Video Reservation:** Enable video reservation and give the value to reserved for video
- ▶ **Remap Tos/DSCP to CoS:** Check the box that the system will remark 802.1P value with TOS/DSCP of upstream packets, the mapping relationship is as follows:

DSCP priority value	802.1p priority
0-7	0
8-15	1
16 ~ 23	2
24 ~ 31	3
32 to 39	4
40 ~ 47	5
48 ~ 55	6
56 to 63	7

#### 3.4.5.2 Port Rate Limit

Rate limit for physical LAN ports, you can select the package type restrictions limiting the entrance. All multiples of 32kbps speed requirements

Choose the menu **Data Service**→**QoS**→**Port Rate Limit** to load the following page.

Data Service ==> QoS ==> Port Rate Limit

Port	Enable	Incoming Rate Limit(Kbps)	Limit Packet Type	Outgoing Rate Limit(Kbps)
LAN1	<input type="checkbox"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/> AP <input checked="" type="checkbox"/> UP <input checked="" type="checkbox"/> MP <input checked="" type="checkbox"/> BP <input checked="" type="checkbox"/> UUP <input checked="" type="checkbox"/> UMP	<input type="text" value="0"/>
LAN2	<input type="checkbox"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/> AP <input checked="" type="checkbox"/> UP <input checked="" type="checkbox"/> MP <input checked="" type="checkbox"/> BP <input checked="" type="checkbox"/> UUP <input checked="" type="checkbox"/> UMP	<input type="text" value="0"/>
LAN3	<input type="checkbox"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/> AP <input checked="" type="checkbox"/> UP <input checked="" type="checkbox"/> MP <input checked="" type="checkbox"/> BP <input checked="" type="checkbox"/> UUP <input checked="" type="checkbox"/> UMP	<input type="text" value="0"/>
LAN4	<input type="checkbox"/>	<input type="text" value="0"/>	<input checked="" type="checkbox"/> AP <input checked="" type="checkbox"/> UP <input checked="" type="checkbox"/> MP <input checked="" type="checkbox"/> BP <input checked="" type="checkbox"/> UUP <input checked="" type="checkbox"/> UMP	<input type="text" value="0"/>

**Tips:** AP:All; UP:Unicast; MP:Multicast; BP:Broadcast; UUP:Unknown Unicast; UMP:Unknown Multicast;

**Figure 3-62 Configure Qos Port Rate Limit**

The following items are displayed on this screen:

- ▶ **Port:** Physical LAN port
- ▶ **Enable:** Enable or disable rate limit function.
- ▶ **Incoming Rate Limit:** Enter incoming maximum rate, which must be times of 32Kbps.
- ▶ **Limit Packet Type:** Select the packet type which is limited rate.
- ▶ **Outgoing Rate Limit:** Enter Outgoing maximum rate, which must be times of 32Kbps.

#### 3.4.5.3 Flow Rate Limit

Choose the menu **Data Service**→**QoS**→**Flow Rate Limit** to load the following page.

DataService ==> QoS ==> Flow Rate Limit										
<input type="checkbox"/>	Index	Protocol	IP Range	Start Time	End Time	Direction	Protocol Type	Port Range	CIR	PIR
<input type="checkbox"/>	1	ANY	192.168.1.10~192.168.1.20	00:00	00:00	UP	--	--	0	0
1 Total 1 Pages, 1 Rows										
<input type="button" value="Add"/> <input type="button" value="Del"/>										

**Figure 3-63 View QoS Flow Rate Limit Entry**

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

DataService ==> QoS ==> Flow Rate Limit	
IP Range	192.168.1.10 ~ 192.168.1.20
Active Time	00:00 -- 00:00 (hh:mm)
Active Day	<input checked="" type="checkbox"/> All <input checked="" type="checkbox"/> Monday <input checked="" type="checkbox"/> Tuesday <input checked="" type="checkbox"/> Wednesday <input checked="" type="checkbox"/> Thursday <input checked="" type="checkbox"/> Friday <input checked="" type="checkbox"/> Saturday <input checked="" type="checkbox"/> Sunday
Direction	Up
Application Protocol	<input checked="" type="radio"/> Application <input type="radio"/> Custom <input type="radio"/> HTTP <input type="radio"/> HTTPS <input type="radio"/> FTP <input type="radio"/> TFTP <input type="radio"/> SMTP <input type="radio"/> POP3 <input type="radio"/> TELNET <input checked="" type="radio"/> ANY
Limited Bandwidth(CIR)	0 (0~1024000)Kbps
Maximal Bandwidth(PIR)	0 (0~1024000)Kbps
<input type="button" value="Save"/> <input type="button" value="Return"/>	

**Figure 3-64 Configure Qos Flow Rate Limit**

The following items are displayed on this screen:

- ▶ **IP Range:** The IP range of LAN's PC.
- ▶ **Active Time:** If not configured, which means that all time are in active
- ▶ **Active Day:** If not configured, which means that all time in active
- ▶ **Direction:**
  - Up:** Check the frame from the direction of the LAN port to the WAN port, and match the source IP and destination port;
  - Down:** Check the frame from the direction of the WAN port to the LAN port, and match the destination IP and source port;
  - Bidirectional:** Limit both upstream and downstream speed.
- ▶ **Limited Bandwidth(CIR):** The limited bandwidth.
- ▶ **Maximal Bandwidth(PIR):** The maximum bandwidth.

If **Application** is selected:

- ▶ **Application Protocol:** Such as HTTP, HTTPS, FTP, TFTP, SMTP, POP3, TELNET, etc.

If **Custom** is selected, the following page will be loaded:

Protocol Type	<input type="radio"/> Application <input checked="" type="radio"/> Custom
Port Range	<input checked="" type="radio"/> UDP <input type="radio"/> TCP
	0 ~ 0 (0~65535)

**Figure 3-65 Configure Custom of Qos Flow Rate Limit**

The following items are displayed on this screen:

- **Protocol Type:** Custom protocol type, UDP or TCP.
- **Port Range:** Set port range.

#### 3.4.5.4 Service

The device supports to remap scheduling priority and remark the value of DSCP or 802.1P according to the service type.

Choose the menu **Data Service**→**QoS**→**Service** to load the following page.

Data Service ==> QoS ==> Service

Name	Remap Queue Priority	Priority	Remark 802.1p	802.1p Value	Remark DSCP	DSCP Value
VOICE	<input type="checkbox"/>	3	<input type="checkbox"/>	0	<input type="checkbox"/>	0
MGMT	<input type="checkbox"/>	2	<input type="checkbox"/>	0	<input type="checkbox"/>	0
VIDEO	<input type="checkbox"/>	1	<input type="checkbox"/>	0	<input type="checkbox"/>	0

**Figure 3-66 View Qos Service**

The following items are displayed on this screen:

- **Name:** Service name. Read only.
- **Remap Queue Priority:** Check the box to remap scheduling queue.
- **Priority:** There are four levels of priority. Priority 3 is highest, and priority 0 is the lowest
- **Remark 802.1p:** Check the box to enable 802.1p priority remarking.
- **802.1p Value:** The value of remarking 802.1P.
- **Remark DSCP:** Check the box to enable DSCP remarking.
- **DSCP Value:** The value of remarking DSCP.

#### 3.4.5.5 ACL

Choose the menu **Data Service**→**QoS**→**ACL** to load the following page.

Data Service ==> QoS ==> ACL

Index	Rule Name	Rule Type	Rule	DEL
1	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
2	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
3	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
4	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
5	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
6	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
7	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
8	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
9	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
10	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
11	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
12	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
13	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
14	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
15	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
16	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
17	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
18	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
19	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
20	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
21	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
22	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
23	--	--	<a href="#">Detail</a>	<a href="#">Del</a>
24	--	--	<a href="#">Detail</a>	<a href="#">Del</a>

**Figure 3-67 View Qos ACL**

Click the **Del** in the entry you want to delete.

Click the **Index** or **Detail** in the entry you want to modify, and then the following page will be loaded:

Data Service ==> QoS ==> ACL Rule

Condition

Rule Name	<input type="text"/> *
Physical Port	<input type="checkbox"/> LAN1 <input type="checkbox"/> LAN2 <input type="checkbox"/> LAN3 <input type="checkbox"/> LAN4 <input type="checkbox"/> WAN
Rule Type	<input checked="" type="radio"/> L2 Data <input type="radio"/> L3 Data
SRC MAC	<input type="text"/>
DEST MAC	<input type="text"/>
Ether Type	0x <input type="text"/> (0x00~0xFFFF)
VLAN ID	<input type="text"/> (1~4094)
802.1p	<input type="text"/> (0~7)

Action

Drop	<input type="checkbox"/>
Remark VID	<input type="checkbox"/> <input type="text"/> (1~4094)
Remark 802.1P	<input type="checkbox"/> <input type="text"/> (0~7)
Remark DSCP	<input type="checkbox"/> <input type="text"/> (0~63)
Priority	<input type="checkbox"/> <input type="text"/> (0~3, 3: highest)
Maximal Bandwidth	<input type="text"/> (32,1024000)kbps;0: Full Rate

**Figure 3-68 Modify Qos ACL**

The following items are display on this page:

**Condition:**

- ▶ **Rule Name:** The custom name.
- ▶ **Physical Port:** Rule's source port
- ▶ **Rule Type:** Type of rule: **L2 data** or **L3 data**.

If **L3 Data** is selected:

Rule Type	<input type="radio"/> L2 Data <input checked="" type="radio"/> L3 Data
Src IP/Netmask	<input type="text"/> / <input type="text"/>
Dest IP/Netmask	<input type="text"/> / <input type="text"/>
Protocol	<input checked="" type="radio"/> Ignore <input type="radio"/> ICMP <input type="radio"/> UDP <input type="radio"/> TCP <input type="radio"/> Other <input type="text"/> (0~255)
L4 Src Port	<input type="text"/> ~ <input type="text"/> (0~65535)
L4 Dest Port	<input type="text"/> ~ <input type="text"/> (0~65535)

**Figure 3-69 L3 Data Rule Type**

The following items are display on this page:

- ▶ **Src IP/Netmask:** The source IP address and netmask of packets, such is 192.168.100.1/255.255.255.0.
- ▶ **Dest IP/Netmask:** The destination IP address and netmask of packets.
- ▶ **Protocol:** E.g. ICMP, UDP, TCP, or custom IP protocol types.
- ▶ **L4 Src Port:** Source port range.
- ▶ **L4 Dest Port:** Destination port range.



If **L2 Data** is selected:

Rule Type	<input checked="" type="radio"/> L2 Data <input type="radio"/> L3 Data
SRC MAC	<input type="text"/>
DEST MAC	<input type="text"/>
Ether Type	0x <input type="text"/> (0x00~0xFFFF)
VLAN ID	<input type="text"/> (1~4094)
802.1p	<input type="text"/> (0~7)

**Figure 3-70 L2 Data Rule Type**

The following items are display on this page:

- ▶ **SRC MAC:** Source MAC address of packets.
- ▶ **DEST MAC:** Destination MAC address of packets.
- ▶ **Ether Type:** The ether type of packets.
- ▶ **VLAN ID:** The VLAN id of packets.
- ▶ **802.1p:** The VLAN priority of packets.

#### Action

- ▶ **Drop:** Drop the packets matched with the rule.
- ▶ **Remark VID:** Change the VID of packets matched with the rule.
- ▶ **Remark 802.1p:** Change the 802.1P priority of packets matched with the rule.
- ▶ **Remark DSCP:** Change the DSCP of packets matched with the rule.
- ▶ **Priority:** Change the scheduling queue of packets matched with the rule.
- ▶ **Maximal Bandwidth:** Limit the bandwidth of packet matched with the rule.

### 3.4.6 DDNS

**DDNS(Dynamic DNS)** service allows you to assign a fixed domain name to a dynamic WAN ip address, which enables the Internet hosts to access the Router or the hosts in LAN using the domain names.

Choose the menu **Data Service**→**DDNS** to load the following page.

DDNS Enable	<input checked="" type="checkbox"/>	
Username	dydns	*
Password	•••••	*
First Url	dydns1.com	*
Second Url	dydns2.com	
Update Interval	600	*[0,65535]s
Server Type	DYNDNS	
Server Name	dydns.com	
Server Url	dydns.com	
Dyn DNS Server Name	dydns.com	
Dyn DNS Server Url	dydns.com	
System Item	dydns.com	
DDNS Status	DDNS_TASK_NOT_INIT	

Save Refresh

**Figure 3-71 Configure DDNS**

The following items are display on this page:

- ▶ **DDNS Enable:** Active or inactive dynamic DNS service.
- ▶ **Username:** Enter account name of your DDNS account.
- ▶ **Password:** Enter password of your DDNS account.
- ▶ **First Url:** First domain name that you registered your DDNS service provider.
- ▶ **Second Url:** First domain name that you registered your DDNS service provider.
- ▶ **Update Interval:** How often, in seconds, the IP is updated.
- ▶ **Server Type:** optional DDNS server type, can select from pull-dwon list:
  - DYNDNS:** For dyndns.org
  - FREEDNS:** For freedns.afraid.org
  - ZONE:** For zoneedit.com
  - NOIP:** For no-ip.com
  - 3322:** For 3322.org
  - CUSTOM:** For custom self-defined DDNS server type.
- ▶ **Server Name:** If CUSTOM is selected, specify server name of the device.
- ▶ **Server Url:** If CUSTOM is selected, specify server URL of the device.
- ▶ **Dyn DNS Server Name:** If CUSTOM is selected, specify dyndns DNS server name of custom self-defined.
- ▶ **Dyn DNS Server Url:** If CUSTOM is selected, specify dyndns DNS server URL of custom self-defined.
- ▶ **System Item:** If CUSTOM is selected, specify system item of custom self-defined.
- ▶ **DDNS Status:** Display the status of DDNS service. Read only.

Click the **Save** button when finished.

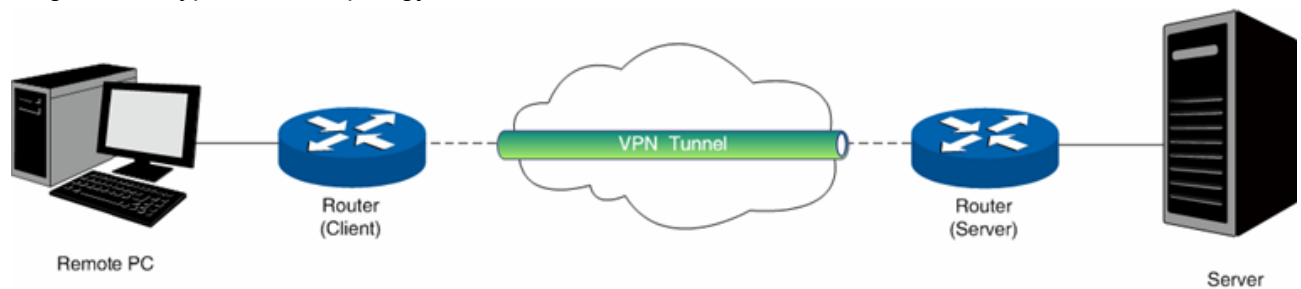
Click **Refresh** button to refresh the web page.

### 3.4.7 VPN

**VPN (Virtual Private Network)** is a private network established via the public network, generally via the Internet. However, the private network is a logical network without any physical network lines, so it is called Virtual Private Network.

With the wide application of the Internet, more and more data are needed to be shared through the Internet. Connecting the local network to the Internet directly, though can allow the data exchange, will cause the private data to be exposed to all the users on the Internet. The VPN (Virtual Private Network) technology is developed and used to establish the private network through the public network, which can guarantee a secured data exchange.

VPN adopts the tunneling technology to establish a private connection between two endpoints. It is a connection secured by encrypting the data and using point-to-point authentication. The following diagram is a typical VPN topology.



**Figure 3-72 VPN – Network Topology**

As the packets are encapsulated and de-encapsulated in the Router, the tunneling topology implemented by encapsulating packets is transparent to users. The tunneling protocols supported contain Layer 3 IPSEC and Layer 2 L2TP/PPTP.

#### 3.4.7.2 PPTP Server

Layer 2 VPN tunneling protocol consists of L2TP (Layer 2 Tunneling Protocol) and PPTP (Point to Point Tunneling Protocol). Both L2TP and PPTP encapsulate packet and add extra header to the packet by using PPP (Point to Point Protocol).

Table depicts the difference between L2TP and PPTP.

Protocol	Media	Tunnel	Length of Header	Authentication
PPTP	IP network	Single tunnel	6 bytes at least	Not supported
L2TP	IP network of UDP	Multiple tunnels	4 bytes at least	Supported

**Figure 3-73 Difference between L2TP and PPTP**

Choose the menu **Data Service**→**VPN**→**PPTP Server** to load the following page.

Data Service ==> PPTP Server

Enable PPTP Server ☒

IP Address Pool Range  to

Enable Authentication ☒

Enable Encryption ☒

<input type="checkbox"/>	Index	Username	IP	Description
<input type="checkbox"/>	1	pptp_user1	192.168.1.206	test

**Figure 3-74 Configure PPTP Server**

The following items are displayed on this screen:

- ▶ **Enable PPTP Server:** Enable or disable the PPTP server function globally.
- ▶ **IP Address Pool Range:** Specify the start and the end IP address for IP Pool. The start IP address should not exceed the end address and the IP ranges must not overlap.
- ▶ **Enable Authentication:** Specify whether to enable authentication for the tunnel.
- ▶ **Enable Encryption:** Specify whether to enable the encryption for the tunnel. If enabled, the PPTP tunnel will be encrypted by MPPE.

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

Data Service ==> VPN ==> PPTP Server

Username  \*

Password  \*

Binding IP  \*

Description

**Figure 3-75 Add or Modify PPTP Client Entry**

The following items are displayed on this screen:

- ▶ **Username:** Enter the account name of PPTP tunnel. It should be configured identically on server and client.
- ▶ **Password:** Enter the password of PPTP tunnel. It should be configured identically on server and client.
- ▶ **Binding IP:** Enter the IP address of the client which is allowed to connect to this PPTP server.
- ▶ **Description:** Enter the humane readable description for this account.

### 3.4.7.3 L2TP Server

Choose the menu **Data Service**→**VPN**→**L2TP Server** to load the following page.

Data Service ==> L2TP Server

Enable L2TP Server ☒

Local IP

IP Address Pool Range  to

Enable Authentication ☒ Auth Secret  (1-127 Characters)

Enable Debug ☐

<input type="checkbox"/>	Index	Username	IP	Description
<input type="checkbox"/>	1	l2tp_user1	192.168.1.206	test

Total 1 Pages, 1 Rows

Index	Username	IP	State
Total 0 Pages, 0 Rows			

**Figure 3-76 Configure L2TP Server**

The following items are displayed on this screen:

- ▶ **Enable L2TP Server:** Enable or disable the L2TP server function globally.
- ▶ **Local IP:** Enter the local IP address of L2TP server.
- ▶ **IP Address Pool Range:** Specify the start and the end IP address for IP Pool. The start IP address should not exceed the end address and the IP ranges must not overlap.
- ▶ **Enable Authentication:** Specify whether to enable authentication for the tunnel. If enabled, enter the authentication secret.
- ▶ **Enable Debug:** Specify whether to enable the debug for L2TP.

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

Data Service ==> VPN ==> L2TP Server

Username  \*

Password  \*

Binding IP  \*

Description

**Figure 3-77 Add or Modify L2TP Client Entry**

The following items are displayed on this screen:

- ▶ **Username:** Enter the account name of L2TP tunnel. It should be configured identically on server and client.
- ▶ **Password:** Enter the password of L2TP tunnel. It should be configured identically on server and client.
- ▶ **Binding IP:** Enter the IP address of the client which is allowed to connect to this L2TP server.
- ▶ **Description:** Enter the humane readable description for this account.

### 3.4.7.4 IPSEC

**IPSEC (IP Security)** is a set of services and protocols defined by IETF (Internet Engineering Task Force) to provide high security for IP packets and prevent attacks. To ensure a secured communication, the two IPSEC peers use IPSEC protocol to negotiate the data encryption algorithm and the security protocols for checking the integrity of the transmission data, and exchange the key to data de-encryption. IPSEC has two important security protocols, AH (Authentication Header) and ESP (Encapsulating Security Payload). AH is used to guarantee the data integrity. If the packet has been tampered during transmission, the receiver will drop this packet when validating the data integrity. ESP is used to check the data integrity and encrypt the packets. Even if the encrypted packet is intercepted, the third party still cannot get the actual information.

**IKE:** In the IPSEC VPN, to ensure a secure communication, the two peers should encapsulate and de-encapsulate the packets using the information both known. Therefore the two peers need to negotiate a security key for communication with IKE (Internet Key Exchange) protocols. Actually IKE is a hybrid protocol based on three underlying security protocols, ISAKMP (Internet Security Association and Key Management Protocol), Oakley Key Determination Protocol, and SKEME Security Key Exchange Protocol. ISAKMP provides a framework for Key Exchange and SA (Security Association) negotiation. Oakley describes a series of key exchange modes. SKEME describes another key exchange mode different from those described by Oakley. IKE consists of two phases. Phase 1 is used to negotiate the parameters, key exchange algorithm and encryption to establish an ISAKMP SA for securely exchanging more information in Phase 2. During phase 2, the IKE peers use the ISAKMP SA established in Phase 1 to negotiate the parameters for security protocols in IPSEC and create IPSEC SA to secure the transmission data.

#### 3.4.7.4.1 IKE Safety Proposal

In this table, you can view the information of IKE Proposals.

Choose the menu **Data Service**→**VPN**→**IPSec**→**IKE Safety Proposal** to load the following page.

Data Service ==>VPN ==>IPSec

<input type="checkbox"/>	Index	Proposal Name	Encryption Algorithm	Auth Algorithm	DH Group
<input type="checkbox"/>	<a href="#">1</a>	test1	3DES	SHA1	DH 1536 modp

1 Total 1 Pages, 1 Rows

Add Del

**Figure 3-78 View IKE Safety Proposal Configuration**

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del.** Click the **Add** button to add a new entry.

Data Service ==> VPN==>IPSec ==> IKE Proposal

Proposal Name	<input type="text" value="test1"/> * (Maximum 128 Characters )
Encryption Algorithm	<input type="text" value="3DES"/>
Auth Algorithm	<input type="text" value="SHA1"/>
DH Group	<input type="text" value="DH 1536 modp"/>

Save Return

**Figure 3-79 Add or Modify IKE Safety Proposal Entry**

The following items are displayed on this screen:

- ▶ **Proposal Name:** Specify a unique name to the IKE proposal for identification and management purposes. The IKE proposal can be applied to IPSEC proposal.
- ▶ **Encryption Algorithm:** Specify the encryption algorithm for IKE negotiation. Options include:
  - DES:** DES (Data Encryption Standard) encrypts a 64-bit block of plain text with a 56-bit key.
  - 3DES:** Triple DES, encrypts a plain text with 168-bit key.
  - AES:** Uses the AES algorithm for encryption.
- ▶ **Auth Algorithm:** Select the authentication algorithm for IKE negotiation. Options include:
  - MD5:** MD5 (Message Digest Algorithm) takes a message of arbitrary length and generates a 128-bit message digest.
  - SHA1:** SHA1 (Secure Hash Algorithm) takes a message less than  $2^{64}$  (the 64th power of 2) in bits and generates a 160-bit message digest.
- ▶ **DH Group:** Select the DH (Diffie-Hellman) group to be used in key negotiation phase 1. The DH Group sets the strength of the algorithm in bits. Options include **DH 768 modp**, **DH 1024 modp** and **DH 1536 modp**.

#### 3.4.7.4.2 IKE Safety Policy

In this table, you can view the information of IKE Policy.

Choose the menu Data Service→VPN→IPSec→IKE Safety Policy to load the following page.

Data Service ==>VPN ==>IPSec

<a href="#">IKE Safety Proposal</a>	<a href="#">IKE Safety Policy</a>	<a href="#">IPSEC Safety Proposal</a>	<a href="#">IPSEC Safety Policy</a>
-------------------------------------	-----------------------------------	---------------------------------------	-------------------------------------

<input type="checkbox"/>	Index	Policy Name	Operation Mode	Enable Local ID	Local ID	Enable Remote ID	Remote ID	Auth Mode	Pre Share Key
<input type="checkbox"/>	<a href="#">1</a>	test2	Main Mode	Disable		Disable		PSK	123

1 Total 1 Pages, 1 Rows

Add Del

**Figure 3-80 View IKE Safety Policy Configuration**

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

Data Service ==> VPN==>IPSec ==> IKE Policy

Policy Name	<input type="text" value="test2"/> * (Maximum 128 Characters)
Operation Mode	<input type="radio"/> Challenge Mode <input checked="" type="radio"/> Main Mode
Enable Local ID	<input type="checkbox"/> <input type="text"/> (Maximum 256 Characters)
Enable Remote ID	<input type="checkbox"/> <input type="text"/> (Maximum 256 Characters)
Auth Mode	<input type="text" value="PSK"/> ▼
Pre Share Key	<input type="text" value="123"/> * (Maximum 256 characters)
Enable Safety Proposal1	<input checked="" type="checkbox"/> <input type="text" value="test1"/> ▼
Enable Safety Proposal2	<input type="checkbox"/> <input type="text" value="test1"/> ▼
Enable Safety Proposal3	<input type="checkbox"/> <input type="text" value="test1"/> ▼
Enable Safety Proposal4	<input type="checkbox"/> <input type="text" value="test1"/> ▼

**Figure 3-81 Add or Modify IKE Safety Policy Entry**

The following items are displayed on this screen:

- ▶ **Policy Name:** Specify a unique name to the IKE policy for identification and management purposes. The IKE policy can be applied to IPSEC policy.
- ▶ **Operation Mode:** Select the IKE Exchange Mode in phase 1, and ensure the remote VPN peer uses the same mode.
  - Main:** Main mode provides identity protection and exchanges more information, which applies to the scenarios with higher requirement for identity protection.
  - Challenge:** Challenge Mode establishes a faster connection but with lower security, which applies to scenarios with lower requirement for identity protection.
- ▶ **Enable Local ID:** If enabled, enter a name for the local device as the ID in IKE negotiation.
- ▶ **Enable Remote ID:** If enabled, enter the name of the remote peer as the ID in IKE negotiation.
- ▶ **Auth Mode:** Select the authentication mode for this IKE policy entry.
  - PSK:**
  - Certificate:**
- ▶ **Pre Share Key:** Enter the Pre-shared Key for IKE authentication, and ensure both the two peers use the same key. The key should consist of visible characters without blank space.
- ▶ **Enable Safety Proposal:** Select the Proposal for IKE negotiation phase 1. Up to four proposals can be selected.

#### 3.4.7.4.3 IPSEC Safety Proposal

In this table, you can view the information of IPSEC proposal.

Choose the menu **Data Service**→**VPN**→**IPSec**→**IPSEC Safety Proposal** to load the following page.



Data Service ==> VPN ==> IPsec					
IKE Safety Proposal   IKE Safety Policy <b>IPSEC Safety Proposal</b> IPSEC Safety Policy					
<input type="checkbox"/>	Index	Proposal Name	Protocol Type	Encryption Algorithm	Auth Algorithm
<input type="checkbox"/>	<a href="#">1</a>	test3	ESP	3DES	SHA1
1 Total 1 Pages, 1 Rows					
Add Del					

**Figure 3-82 View IPSEC Safety Proposal Configuration**

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

Data Service ==> VPN ==> IPsec	
Proposal Name	test3 * (Maximum 128 Characters)
IPsec Protocol	ESP
Encryption Algorithm	3DES
Auth Algorithm	SHA1
Save Return	

**Figure 3-83 Add or Modify IPSEC Safety Proposal Entry**

The following items are displayed on this screen:

- **Proposal Name:** Specify a unique name to the IPSEC Proposal for identification and management purposes. The IPSEC proposal can be applied to IPSEC policy.
- **IPsec Protocol:** Select the security protocol to be used. Options include:
  - AH:** AH (Authentication Header) provides data origin authentication, data integrity and anti-replay services.
  - ESP:** ESP (Encapsulating Security Payload) provides data encryption in addition to origin authentication, data integrity, and anti-replay services.
  - ESP+AH:** Both ESP and AH security protocol.
- **Encryption Algorithm:** Select the algorithm used to encrypt the data for ESP encryption. Options include:
  - DES:** DES (Data Encryption Standard) encrypts a 64-bit block of plain text with a 56-bit key. The key should be 8 characters.
  - 3DES:** Triple DES, encrypts a plain text with 168-bit key. The key should be 24 characters.
  - AES:** Uses the AES algorithm for encryption. The key should be 16 characters.
- **Auth Algorithm:** Select the algorithm used to verify the integrity of the data. Options include:
  - MD5:** MD5 (Message Digest Algorithm) takes a message of arbitrary length and generates a 128-bit message digest.
  - SHA:** SHA (Secure Hash Algorithm) takes a message less than the 64th power of 2 in bits and generates a 160-bit message digest.

#### 3.4.7.4.4 IPSEC Safety Policy

In this table, you can view the information of IPSEC policy.

Choose the menu **Data Service**→**VPN**→**IPSec**→**IPSEC Safety Policy** to load the following page.

Data Service ==>VPN ==>IPSec								
IKE Safety Proposal IKE Safety Policy IPSEC Safety Proposal IPSEC Safety Policy								
<input type="checkbox"/>	Index	Policy Name	Enable IPSEC	Interface	VPN Mode	Local Subnet	Remote Address	Remote Subnet
<input type="checkbox"/>	1	test4	Enable	DATA	Site2Site	192.168.1.1/255.255.255.0	10.0.2.3	10.0.1.1/255.255.0.0
1 Total 1 Pages, 1 Rows								
Add Del								

**Figure 3-84 View IPSEC Safety Policy Configuration**

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

Data Service ==> VPN ==> IPSec ==> IPSec Policy	
Enable Isec	<input checked="" type="checkbox"/>
IPSEC Policy Name	test4 * (Maximum 128 Characters)
Select Interface	DATA_WAN *
VPN Mode	<input checked="" type="radio"/> Site To Site <input type="radio"/> PC To Site
Local Subnet IP	192.168.1.1
Local Subnet Netmask	255.255.255.0
Remote Address	10.0.2.3 * (IP Address or Domain Name)
Remote Subnet IP	10.0.1.1
Remote Subnet Netmask	255.255.0.0
IKE Safety Policy	test2
Enable Safety Proposal1	<input checked="" type="checkbox"/> test3
Enable Safety Proposal2	<input type="checkbox"/> test3
Enable Safety Proposal3	<input type="checkbox"/> test3
Enable Safety Proposal4	<input type="checkbox"/> test3
Save Return	

**Figure 3-85 Add or Modify IPSEC Safety Policy Entry**

The following items are displayed on this screen:

- ▶ **Enable Isec:** Enable or disable this IPSEC entry.
- ▶ **IPSEC Policy Name:** Specify a unique name to the IPSEC policy.
- ▶ **Select Interface:** Specify the local WAN port for this Policy.
- ▶ **VPN Mode:** Select the network mode for IPSEC policy. Options include:
  - Site To Site:** Select this option when the client is a network.
  - PC to Site:** Select this option when the client is a host.
- ▶ **Local Subnet IP & Local Subnet Netmask:** Specify IP address range on your local LAN to identify which PCs on your LAN are covered by this policy.
- ▶ **Remote Address:** If **PC to Site** is selected, specify IP address on your remote network to identify which PCs on the remote network are covered by this policy.
- ▶ **Remote Subnet IP & Remote Subnet Netmask:** Specify IP address range on your remote network to identify which PCs on the remote network are covered by this policy.
- ▶ **IKE Safety Policy:** Specify the IKE policy. If there is no policy selection, add new policy on **VPN→IPSec→IKE Safety Policy** page.
- ▶ **Enable Safety Prososal:** If enabled, Select IPSEC Proposal. If there is no policy selection, add new IPSEC proposal on **VPN→IPSec→IPSEC Safety Proposal** page. Up to

four IPSEC Proposals can be selected.

### 3.4.8 Routing

#### 3.4.8.1 Static Route

##### 3.4.8.1.1 IPv4

Choose the menu **Data Service**→**Routing**→**Static Route**→**IPv4** to load the following page.

	Enable	Destination IP	Netmask	Next Hop Type	Next Hop Interface	Next Hop Address	Valid
1	<input checked="" type="checkbox"/>	10.0.1.1	255.255.255.0	Interface	DATA		
2	<input type="checkbox"/>			Interface	DATA		
3	<input type="checkbox"/>			Interface	DATA		
4	<input type="checkbox"/>			Interface	DATA		
5	<input type="checkbox"/>			Interface	DATA		
6	<input type="checkbox"/>			Interface	DATA		
7	<input type="checkbox"/>			Interface	DATA		
8	<input type="checkbox"/>			Interface	DATA		
9	<input type="checkbox"/>			Interface	DATA		
10	<input type="checkbox"/>			Interface	DATA		

Save

**Figure 3-86 Configure IPv4 Static Route**

The following items are displayed on this screen:

- **Enable:** Select it to add and modify the current route. Conversely, disable the current route.
- **Destination IP:** Enter the destination host the route leads to.
- **Netmask:** Enter the Subnet mask of the destination network.
- **Next Hop Type:** Include **Next Hop Interface** and **Next Hop Address**(see following option)
- **Next Hop Interface:** Specify the interface of next hop for current route
- **Next Hop Address:** Specify the address of next hop for current route
- **Valid:** Show the status of current route.

##### 3.4.8.1.2 IPv6

The menu IPV6 is hidden if you don't enable Ipv6 stack, please refer to configuration index **Network**→**IPv6** for detail setting.

Choose the menu **Data Service**→**Route**→**Static Route**→**IPv6** to load the following page.

IPv4
IPv6

Enable	Destination IPv6/Prefix Length	Next Hop Type	Next Hop Interface	Next Hop Address	Valid
1 <input checked="" type="checkbox"/>	2010::20c:29ff:fe85:a330 / 64	Interface	WAN		Invalid
2 <input type="checkbox"/>		Interface	WAN		
3 <input type="checkbox"/>		Interface	WAN		
4 <input type="checkbox"/>		Interface	WAN		
5 <input type="checkbox"/>		Interface	WAN		
6 <input type="checkbox"/>		Interface	WAN		
7 <input type="checkbox"/>		Interface	WAN		
8 <input type="checkbox"/>		Interface	WAN		
9 <input type="checkbox"/>		Interface	WAN		
10 <input type="checkbox"/>		Interface	WAN		

Save

**Figure 3-87 Configure IPv6 Static Route**

The configuration options of Ipv6 is similar to Ipv4, the prefix length is equal to mask of Ipv4 address.

### 3.4.8.2 Policy Route

Choose the menu **Data Service**→**Route**→**Policy Route** to load the following page.

Data Service ==> Policy Route

<input type="checkbox"/>	Index	Enable	Src IP Range	Dst IP Range	Dst Port Range	Next Hop	Active Time
<input type="checkbox"/>	<a href="#">1</a>	YES	192.168.1.100-192.168.1.200	210.10.10.3-210.10.10.50	1000-2000	DATA	<a href="#">TimeInfo</a>

1 Total 1 Pages, 1 Rows

Add
Del

**Figure 3-88 View Policy Route**

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

DataService ==> Policy Route

Enable PolicyRoute ☒

Next Hop Type Interface

Interface DATA

Description policy1

Protocol ALL

Source IP 192.168.1.100 to 192.168.1.200

Destination IP 210.10.10.3 to 210.10.10.50

Destination Port 1000 to 2000 [0~65535]

Active Time 00:00 -- 23:59 (hh:mm)

Active Day All ☒ Monday ☒ Tuesday ☒ Wednesday ☒ Thursday ☒ Friday ☒ Saturday ☒ Sunday

Save
Return

**Figure 3-89 Add or Modify Policy Route**

The following items are displayed on this page:

- ▶ **Enable PoliceRoute:** Enable or disable the entry
- ▶ **Next Hop Type:** Select from pull-down list: **Interface**, **Address**.
- ▶ **Interface:** Specify the interface of next hop for the entry.
- ▶ **Address:** Specify the address of next hop for the entry.
- ▶ **Description:** Give description for the entry.
- ▶ **Protocol:** Specify the protocol, **TCP**, **UDP** or **ALL**.
- ▶ **Source IP:** Enter IP address or IP range of source in the rule entry.
- ▶ **Destination IP:** Enter IP address or IP range of destination in the rule entry.
- ▶ **Destination Port:** Specify port or port range of destination in the rule entry.
- ▶ **Active Time:** Specify the active time range for the rule entry.
- ▶ **Active Day:** Specify the active days for the rule entry.

### 3.4.8.3 RIP

The **Routing Information Protocol (RIP)** is one of the oldest distance-vector routing protocols, which employs the hop count as a routing metric.

#### 3.4.8.3.1 RIP Service

Choose the menu **Data Service**→**RIP**→**RIP Service** to load the following page.

**Figure 3-90 RIP Service Configuration**

The following items are displayed on this page:

- ▶ **Enable RIP Service:** Enable or disable RIP service function globally.

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

**Figure 3-91 Add or Modify RIP Service Entry**

The following items are displayed on this page:

- ▶ **Interface:** Specify the interface for the entry.

- **Receive RIP Version:** Specify receiving RIP version for the entry.
- **Send RIP Version:** Specify sending RIP version for the entry.
- **Authorization Enable:** Check the box to enable authorization.
- **Key Mode:** Specify the encryption mode of key, **TEXT**(plaintext),**MD5**(cipertext).
- **Key Type:** Specify the key from **Simple String** or **Key Chain**.
- **Simple String:** If select Simple String in item of Key Type, enter simple string as key.

#### 3.4.8.3.2 Key Chain

Key Chain is a chain of keys used as RIP authorization key.

Choose the menu **Data Service**→**RIP**→**Key Chain** to load the following page.

Data Service ==> RIP

**RIP Service** **Key Chain**

Key Chain Name | test\_1 (max 19 char)

Save

<input type="checkbox"/>	Index	Key ID	Key String
Add Del			

**Figure 3-92 View RIP Key Chain Configuration**

The following items are displayed on this page:

- **Key Chain Name:** Enter the name of key chain.

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

Data Service ==> RIP

Key ID | [1,255]

Key String | (max 15 char)

Save Return

**Figure 3-93 Add or Modify RIP Key Chain Entry**

The following items are displayed on this page:

- **Key ID:** Enter the ID of the entry.
- **Key String:** Enter the Key of the entry.

### 3.4.9 Advanced Parameters

#### 3.4.9.1 UPnP Parameter

**The Universal Plug and Play (UPnP)** technology is enabling a world in which music and other digital entertainment content is accessible from various devices in the home without regard for where the media is stored. Using UPnP devices the whole family can share in the fun together whether it's:

- Viewing your best family photos via the TV
- Watching home videos

- Listening to favorite tunes throughout the house

The **Digital Living Network Alliance (DLNA)** is a non-profit collaborative trade organization established by Sony in June 2003, which is responsible for defining interoperability guidelines to enable sharing of digital media between multimedia devices. DLNA uses UPnP for media management, discovery and control.

Here, UPNP mainly for DLNA, DLNA server can be automatically discovered by sending NOTIFY via Multicast, and DLNA clients can search DLNA servers by sending M-SEARCH via Multicast.

Choose the menu **Data Service**→**Advanced Parameters**→**UPnp Parameter** to load the following page.

**Figure 3-94 Configure UPnp**

The following items are displayed on this screen:

- **Enable UPnP:** Enable or disable the UPnP function globally.
- **Upstream Interface:** The network interface connected to the DLNA server.
- **Downstream Interface:** The network interface connected to the DLNA client.

### 3.4.10 Multicast

Choose the menu **Data Service**→**Multicast** to load the following page.

**Figure 3-95 Configure Multicast**

The following items are displayed on this screen:

- **Enable IGMP Proxy:** Enable or disable the IGMP proxy function globally. Currently, IGMP proxy is mainly used for IPTV.

### 3.4.11 USB Storage

USB Storage function let Windows OS share files of USB storage mounted on embedded device by Samba and ftp.

#### 1) User Management

Manage the list of users which access USB storage.

Choose menu **Data Service**→**USB Storage** to load the following page.

Index	Username	Access Right
1	gaoke	Read

**Figure 3-96 View User Management Configuration**

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

**Figure 3-97 Add or Modify User Management Entry**

The following items are displayed on this screen:

- ▶ **Username:** Enter user name of this entry.
- ▶ **Password:** Enter password of this entry.
- ▶ **Access Right:** Select access right from pull-down list, **Read** or **Read/Write**.

## 2) USB Storage

Scan the partitions of USB Storage by click **Rescan** button and umount specified partition by clicking **Umount** button. Click **start** to start service, click **stop** to stop service.

Disk	Share Name	File System	Storage(GB)	Used Storage(GB)	Free Storage(GB)	Utilization Rate	Property
/media/sda1	share0	vfat	3.80	0.00	3.79	1%	<a href="#">Modify</a>

**Figure 3-98 View USB Storage**

Click **Modify** to load the following page:

**Figure 3-99 Modify USB Storage**

The following items are displayed on this screen:



- **Share Name:** Enter the share name.
- **Allowed User:** Select the users need to access the partition of the entry.

## 3.5 VOIP Service

The **Session Initiation Protocol (SIP)** is a signaling protocol used for establishing sessions in an IP network. The protocol can be used for creating, modifying and terminating two-party (unicast) or multiparty (multicast) sessions. Sessions may consist of one or several media streams.

### 3.5.1 SIP Service

Choose the menu **VOIP Service**→**SIP Service** to load the following page.

VoIP Service ==> SIP Service

General Parameters

Primary Server Address	<input type="text" value="192.168.1.65"/>	*
Primary Server Port	<input type="text" value="5060"/>	[0 or 1024~65535]
Enable Backup Server	<input type="checkbox"/>	
Backup Server Address	<input type="text"/>	
Backup Server Port	<input type="text" value="5060"/>	[0 or 1024~65535]
Enable Proxy Server	<input type="checkbox"/>	
Proxy Address	<input type="text"/>	
Proxy Port	<input type="text" value="5060"/>	[0 or 1024~65535]
Enable Secondary Proxy	<input type="checkbox"/>	
Secondary Proxy Address	<input type="text"/>	
Secondary Proxy Port	<input type="text" value="0"/>	[0 or 1024~65535]
Register Interval	<input type="text" value="1200"/>	* [60~3600]s
RTP Port	<input type="text" value="9000"/> - <input type="text" value="20000"/>	* [1024 - 65535]
Local SIP Port	<input type="text" value="5060"/>	* Default:5060

[+Advanced Parameters](#)

Save Refresh

**Figure 3-100 Configure General Parameters of SIP Service**

The following items are displayed on this screen:

- **Primary Server Address:** Domain or IP of SIP server.
- **Primary Server Port:** Listening port of SIP server.
- **Enable Backup Server:** Enable or disable backup SIP server.
- **Backup Server Address:** Domain or IP of backup SIP server.
- **Backup Server Port:** Listening port of backup SIP server.
- **Enable Proxy Server:** Enable or disable Proxy server.
- **Proxy Address:** Domain or IP of proxy server.
- **Proxy Port:** Listening port of proxy server.
- **Enable Secondary Proxy:** Enable or disable backup proxy server.
- **Secondary Proxy Address:** Domain or IP of backup proxy server.
- **Secondary Proxy Port:** Listening port of backup proxy server.
- **Register Interval:** Enter the desired time interval at which the sip UA will send register

message.

- ▶ **RTP Port:** Local RTP port range.
- ▶ **Local SIP Port:** Local listening port.

Click **+Advanced Parameters** to load the following page.

The screenshot shows the 'Advanced Parameters' configuration page for SIP Service. The page is divided into two columns. The left column lists the parameters, and the right column contains the configuration options. The parameters and their current values are as follows:

Parameter	Value / Option
Enable Alive	<input type="checkbox"/> 600 [20~3600]s
Keep Alive Mode	<input checked="" type="radio"/> CLRF <input type="radio"/> OPTIONS <input type="radio"/> PING
Enable Realm	<input type="checkbox"/> [Empty]
Enable Session Timer	<input type="checkbox"/> 90 [90~3800]s
Timer Preference	<input checked="" type="radio"/> UAC <input type="radio"/> UAS
Enable SIP Retrans Timer	<input type="checkbox"/>
Register Failed Retrans Interval	30 [1~360]s
Retrans Times	0
User Agent	[Empty]
Hold Mode	<input checked="" type="radio"/> 0.0.0.0 <input type="radio"/> Send-Only
Enable NextNonce	<input type="checkbox"/> 0 (Nonce Count)
ToS/DiffServ Settings	<input checked="" type="radio"/> ToS IP Precedence <input type="radio"/> DiffServ(DSCP)
Signalling Precedence	0 (0~7)
Voice Data Precedence	0 (0~7)
Support PRACK	<input type="checkbox"/>
Support User=Phone	<input type="checkbox"/>
Update Register Cycle	<input checked="" type="checkbox"/>
Support Full Register	<input type="checkbox"/>
First Package With Auth Info	<input type="checkbox"/>
SDP With Audio When T38 Faxing	<input type="checkbox"/>

At the bottom of the page, there are two buttons: 'Save' and 'Refresh'.

**Figure 3-101 Configure Advanced Parameters of SIP Service**

The following items are displayed on this screen:

- ▶ **Enable Alive:** After successful registration, whether to send keep-alive packets.
- ▶ **Keep Alive Mode:** Keep alive mode: **CLRF**, **OPTIONS** or **PING**.
- ▶ **Enable Realm:** Check the box to enable SIP signaling packets with realm field information.
- ▶ **Enable Session Timer:** Enable or disable UAC / UAS session refresh mode.
- ▶ **Enable SIP Retrans Timer:** When registration fails, whether to initiate retransmission, retransmission cycle and time with configuration.
- ▶ **User Agent:** Check the box to enable signaling packets with **User Agent** field.
- ▶ **Hold Mode:** Select the SIP signal format of call hold.
- ▶ **Enable Next Nonce:** Enable SIP packets with nonce count field information, incremented each one and with a maximum value.
- ▶ **Support PRACK:** Enable or disable provisional response. If enabled, 1xx (except 100rel) messages are required to respond with ACK.
- ▶ **Support User=Phone:** Whether SIP signaling packets with User = Phone field information.
- ▶ **Update Register Cycle:** Based on server response to update registration period.

- **Support Full Register:** Each registration packets are generated, rather than re-issued.
- **First Package With Auth Info:** The first registration packet with authentication information.
- **SDP With Audio When T38 Faxing:** T38 fax signaling packet with audio information.

### 3.5.2 User

#### 3.5.2.1 User

Choose the menu **VOIP Service**→**User**→**User** to load the following page.

VoIP Service ==> User

User Wildcard Group

<input type="checkbox"/>	User	Account	Phone Number	Enable	Primary Reg-Status	Secondary Reg-Status
<input type="checkbox"/>	FXS1	bgiad_test1	6001	Yes	Disabled	Disabled
<input type="checkbox"/>	FXS2	--	--	No	Disabled	Disabled

1 Total 1 Pages, 2 Rows

Register Unregister

**Figure 3-102 User Configuration**

Click the **Register** button to start the registering to the SIP server.

Click the **Unregister** button to start the un-registering to the SIP server.

Click the **User** in the entry you want to modify to load the following page.

VoIP Service ==> User

Account

User FXS1

Account bgiad\_test1 \*

Auth Username bgiad\_test1

Password ●●●●

Phone Number 6001 \*

Enable Register ☒

Ring Group Identity ☐

Save Return

**Figure 3-103 Configure User**

The following items are displayed on this screen:

- **Account:** Account name registered to SIP server.
- **Auth Username:** Username of the account.
- **Password:** Password of the account.
- **Phone number:** Caller and called number of subscriber line.
- **Enable Register:** Enable registering.
- **Ring Group Identity:** Phone number configured as one hunt group, after saving, the configuration can be seen in the Centrex page.

#### 3.5.2.2 Wildcard Group

Choose the menu **VOIP Service**→**User**→**Wildcard Group** to load the following page.

VoIP Service ==> User

User **Wildcard Group**

<input type="checkbox"/>	Wildcard Group	Account	Register Status
<input type="checkbox"/>	1	bgiad_test1	Not Register

Add Del

**Figure 3-104 Wildcard Group Configuration**

Click the **Wildcard Group** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

VoIP Service ==> Wildcard Group

☒ Enable Group Register

Wildcard Group:

(Free Account List)

bgiad\_test1  
test2

>  
>>  
<  
<<

(Register Group Account List)

>  
<

(Register Account)

**Figure 3-105 Add or Modify Wildcard Group Configuration**

The following items are displayed on this screen:

- **Enable Group Register:** Enable or disable the group register function globally.

### 3.5.3 Supplementary

Choose the menu **VOIP Service**→**Supplementary** to load the following page.

VoIP Service ==> Supplementary

<input type="checkbox"/>	User	Phone Number	Hotline	CID Restriction	DND	Call Waiting	CID	Abbr Dialing	Black&White List
<input type="checkbox"/>	FXS1	6001	Disable	Disable	Disable	Disable	Enable	<a href="#">Abbr Dialing</a>	<a href="#">Black&amp;White List</a>
<input type="checkbox"/>	FXS2	1002	Disable	Disable	Disable	Disable	Enable	<a href="#">Abbr Dialing</a>	<a href="#">Black&amp;White List</a>

1 Total 1 Pages, 2 Rows

**Figure 3-106 User Supplementary**

- 1) Click the **User** in the entry you want to modify to load the following page. You can also select multiple, then click **Batch Edit** to batch configuration.

VoIP Service == > Supplementary ==> FXS1

Call Forward

Call Forwarding Unconditional	<input checked="" type="checkbox"/>
Call Number	<input type="text"/> (1-32 digits,*,#,null for disable)

Call Forwarding No Reply	<input checked="" type="checkbox"/>
Call Number	<input type="text"/> (1-32 digits,*,#,null for disable)
Wait Time Long	<input type="text"/> [1,120]s

Call Forwarding On Busy	<input checked="" type="checkbox"/>
Call Number	<input type="text"/>

Hotline

Hotline Number	<input type="text"/> (max 32 digits,*,#)
Delay Time	<input type="text"/> 0 (0~10 s)

Other

CID Restriction	<input type="checkbox"/>
Anonymous As UserName	<input type="checkbox"/>
Enable No Disturb	<input type="checkbox"/>
Enable Call Waiting	<input type="checkbox"/>
Enable MWI	<input type="checkbox"/>
Enable CID	<input checked="" type="checkbox"/>
CID Mode	<input type="text"/> FSK

Save Return

**Figure 3-107 Modify Supplementary Configuration**

The following items are displayed on this screen:

- ▶ **Call Forwarding Unconditional:** Enable or disable CFU function, if enabled, enter **Call Number**.
  - 1) Set by keypad service system: **\*57\*TN#**, TN is the phone number to be redirected to.
  - 2) Cancel by keypad service system: **#57#**.
- ▶ **Call Forwarding No Reply:** Enable or disable CFNR, if enabled, enter **Call Number** and **Wait Time Long**.
  - 1) Set by keypad service system: **\*41\*TN#**, TN is the phone number to be redirected to.
  - 2) Cancel by keypad service system: **#41#**.
- ▶ **Call Forwarding On Busy:** Enable or disable CFB function, if enabled, enter **Call Number**.
  - 1) Set by keypad service system: **\*40\*TN#**, TN is the phone number to be redirected to.
  - 2) Cancel by keypad service system: **#40#**.
- ▶ **Hotline Number:** Enter number to hotline function, empty expressed disable.
  - 1) Set **delay hotline** number by Keypad service system: **\*52\*TN#**, TN is the hotline number.
  - 2) Cancel **delay hotline** number by Keypad service system: **#52#**.
  - 3) Set **instant hotline** number by Keypad service system: **\*42\*TN#**, TN is the hotline number.
  - 4) Cancel **instant hotline** number by Keypad service system: **#42\*EN#**, instant hotline can only be deactivated with other extension; EN is the extension number which needs to deactivate

- instant hotline.
- **Delay Time:** Time 0 indicates immediate Hotline, Otherwise, indicates delay Hotline. The Delay Time must be configured on the WEB.
  - **CID Restriction:** Enable or disable CID Restriction. If **Anonymous As UserName** is chosen, user name content is Anonymous also.
  - **Enable No Disturb:** Allows block incoming calls at any time.
  - **Enable Call Waiting:** When you talking, a third party phone comes in, you can hear the beep tone.
  - **Enable MWI:** Enable or disable MWI (Message-waiting indicator) function.
  - **Enable CID:** Enable or disable to send CID to phone.
  - **CID Mode:** There are two methods used for sending caller ID information depending on the application and country specific requirements:  
**FSK:** caller ID generation using Frequency Shift Keying (FSK)  
**DTMF:** caller ID generation using DTMF signaling.

- 2) Abbreviated Dialing allows you to store selected phone numbers for quick and easy dialing. Each telephone number can be dialed by using a one to two-digit code with a simple prefix. Stored numbers may be up to 32 digits in length.
- If you want to add or remove abbreviated dialing numbers, click the **Abbr Dialing** to load the following page.

ABBR. Number	Phone Number
1	1001

Total 1 Pages, 1 Rows

Add Del Return

**Figure 3-108 View Abbreviated Dialing Configuration**

Click the **Del** button to delete the entries you select.

Click the **Add** button to add a new entry.

Abbreviated Number: 1 (1-2 digits)

Phone Number: 1001 \*(1-31 digits,\*,#)

Save Return

**Figure 3-109 Add Abbreviated Dialing Entry**

The following items are displayed on this screen:

- **Abbreviated Number:** Enter the abbreviated number.
- **Phone Number:** Enter the Actual phone number.

- 3) If you want to add or remove black&white list, click the **Black&White List** to load the following page.

Information	List Type
5123	Incoming Blacklist

<< 1 >>

Add Del Return

**Figure 3-110 Black&White List Configuration**

Click the **Information** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**.

Click the **Add** button to add a new entry.

**Figure 3-111 Add or Modify Black&White List Entry**

The following items are displayed on this screen:

- **List Type:** Choose type of Black&White List, four types are provided:  
**Incoming Blacklist, Incoming Whitelist, Outgoing Blacklist, Outgoing Whitelist.**
- **Information:** Enter the phone number or sip account.

### 3.5.4 Codec Parameters

- 1) Packet Period defines how long the device sends a RTP packet to the other side. The smaller the value, the more bandwidth usage. The larger the value, the more voice delay. Choose the menu **VOIP Service→Codec Parameters** to load the following page.

**Figure 3-112 Configure Packet Period**

- **G.711A Packet Period:** RTP packetization period of G.711A codec.
- **G.711u Packet Period:** RTP packetization period of G.711U codec.
- **G.723 Packet Period:** RTP packetization period of G.723 codec.
- **G.729 Packet Period:** RTP packetization period of G.729 codec.

- 2) Choose the menu **VOIP Service→Codec Parameters** to load the following page.

<input type="checkbox"/>	User	Fax Mode	Codec First Priority	Codec Second Priority	Codec Third Priority	Codec Fourth Priority
<input type="checkbox"/>	FXS1	Transparent	G.729	G.711U	G.723	G.711A
<input type="checkbox"/>	FXS2	Transparent	G.711A	G.711U	G.723	G.729
1 Total 1 Pages, 2 Rows						
Batch Edit						

**Figure 3-113 View Fax Mode&Codec Priority Configuration**

To modify fax mode or codec priority of users, click the **User** in the entry you want to modify to load the following page. You can also select multiple, then click **Batch Edit** to batch configuration.

**Figure 3-114 Add or Modify Fax Mode&Codec Priority**

The following items are displayed on this screen:

- ▶ **Fax Mode:** Choose fax mode, three types are provided: **Transparent, T38, VBD.**
- ▶ **Codec Answer Strategy:** Two modes are provided:
  - Use Answerer Priority:** Codec selection decisions based on the priority level configuration
  - Use Offerer Priority:** Codec selection decision based on caller's priority.
- ▶ **Codec Priority:** If **Use Answerer Priority** is selected, set the priority of codec.

### 3.5.5 DSP Parameters

Choose the menu **VOIP Service**→**DSP Parameters** to load the following page.

**Figure 3-115 Configure DSP Parameters**

The following items are displayed on this screen:

- ▶ **Echo Cancellation:** Enable or disable echo cancellation.
- ▶ **Silence Detection/Suppression:** Enable or disable silence detection and silence suppression.
- ▶ **Input Gain:** Configure the input gain value.
- ▶ **Output Gain:** Configure the input gain value



- **Delay Level:** Choose the delay level, five levels are provided: **Minimum, Smaller, Moderate, Larger, Maximum.**
- **DTMF Transfer Model:** Select DTMF transmission mode: **In-Band, INFO, RFC2833.**
- **RFC2833 Load Type:** If RFC2833 is selected, specify payload type of RFC2833.
- **T38 Max FAX Rate:** Select the maximum rate, when using T38 fax mode: **Unlimited, 2400bps, 4800bps, 7200bps, 9600bps, 12000bps, 14400bps.**
- **T38 Signaling Redundancy:** Configure the redundancy of T38 signal.
- **T38 Data Redundancy:** Configure the redundancy of T38 data.
- **Ring Frequency:** Choose the ring frequency: **20Hz, 25Hz.**
- **Impedance Type:** Choose the impedance type: **600Ω, China Standard, Switzerland Standard.**

### 3.5.6 Digitmap

The destination number will be sent all in one time for SIP application, digitmap is used to determine exactly when there are enough digits entered from the user to place a call. If the number length of suited route item is fixed, the number will be sent when specified number of digits is received; the call will be disconnected when inter-digit timeout expires. If the number length of suited route item is indefinite, there are 3 ways to determine whether the digits is enough, press pound(#) key, timeout expires or digitmap comparing. If digits dialed partly matching with digitmap patterns, continue waiting of number receiving. If they match, send the number immediately. If not, send the number immediately too, in order to play the prompts.

Table 3-1 Digitmap Characters

Character	Description
0~9	Indicates specific digits in a telephone number expression.
X	Wildcard, matches any digit, excluding “#” and “*”.
*	Digit star
#	Digit pound
-	Connects the start and the end of a range
[]	Indicates the a range of numbers(not letters).
.	Matches an arbitrary number of occurrences of the preceding digit, including 0.
	Indicates a choice of matching expressions (OR).
T	Inter-digit timeout expires
S	Short timer expires, usually place at the middle of an expression

Digitmap Example: 8XXXXXXX|1[0-24]0|2[18].3|3XXSXX|[0-9\*#][0-9\*#][0-9\*#].#[0-9\*#].T

- “8XXXXXXX” denotes numbers start with 8, the length is 8.
- “1[0-24]0” denotes numbers include 100, 110, 120 and 140.
- “2[18].3” denotes numbers that start with 2 and end with 3, there can be arbitrary length of 1 or 8 after the first digit 2. 23, 213, 2183 is matched.
- “3XXSXX” denotes numbers start with 3, the length can be 3 or 5. If the short timer configured expires between the third digit and the fourth digit, the number will be sent.
- “[0-9\*#][0-9\*#][0-9\*#].#” denotes numbers end with #, and the length is no less than 2.

- “[0-9\*#].T” denotes any number that dialing time out.

Choose the menu **VOIP Service**→**Digitmap** to load the following page.

**Figure 3-116 Configure Digitmap**

The following items are displayed on this screen:

- ▶ **Enable:** Enable or disable digit map function.
- ▶ **Short Timer:** Enter the time of Short Timer in second.
- ▶ **Digit Map:** Enter the digit map rules.

### 3.5.7 Signal Tone

Choose the menu **VOIP Service**→**Signal Tone** to load the following page.

Distinction Ring		
Internal Ring On Time1	<input type="text" value="10"/>	[1,100]* 100ms
Internal Ring Off Time1	<input type="text" value="40"/>	[1,100]* 100ms
Internal Ring On Time2	<input type="text" value="0"/>	[0,100]* 100ms
Internal Ring Off Time2	<input type="text" value="0"/>	[0,100]* 100ms
External Ring On Time1	<input type="text" value="10"/>	[1,100]* 100ms
External Ring Off Time1	<input type="text" value="40"/>	[1,100]* 100ms
External Ring On Time2	<input type="text" value="0"/>	[0,100]* 100ms
External Ring Off Time2	<input type="text" value="0"/>	[0,100]* 100ms

**Figure 3-117 Configure Signal Tone**

The following items are displayed on this screen:

- ▶ **Tone Type:** Select the type of signal tone.

#### Dial Tone

- ▶ **User Define Enable:** Whether to use user-defined dial tone frequency.
- ▶ **Dial Tone Frequency 1:**
- ▶ **Dial Tone Frequency 2:**

#### Busy Tone

- ▶ **User Define Enable:** Whether to use user-defined busy tone frequency.
- ▶ **Busy Tone Frequency 1:**
- ▶ **Busy Tone Frequency 2:**
- ▶ **On Time:**
- ▶ **Off Time:**

#### Ring Back Tone

- ▶ **User Define Enable:** Whether to use user-defined ringback tone frequency.
- ▶ **Ring Back Tone Frequency 1:**
- ▶ **Ring Back Tone Frequency 2:**
- ▶ **On Time:**
- ▶ **Off Time:**

**Distinction Ring:** Specify the ring cadence for the FXS port. In these fields, you specify the on and off pulses for the ring. The ring cadence that should be configured differs between internal call and external call.

### 3.5.8 FXS Parameters

Choose the menu **VOIP Service**→**FXS Parameters** to load the following page.

VoIP Service ==> FXS Parameters

Min Flash Detect Time	<input type="text" value="80"/>	* [50,750]ms ; default:50
Max Flash Detect Time	<input type="text" value="500"/>	* [50,1200]ms ; default:500

Flash Key Enable	<input checked="" type="checkbox"/>	
Switch&Release Call	Flash+ <input type="text" value="1"/>	(0-9)
Three Party Call	Flash+ <input type="text" value="3"/>	(0-9)
Reject Key	Flash+ <input type="text" value="0"/>	(0-9)
Switch Call Key	Flash+ <input type="text" value="2"/>	(0-9)

Keep the hold call when onhook	<input type="checkbox"/>	
(#)Quick Dial Key	<input checked="" type="checkbox"/>	
Asterisk Func Key	<input type="checkbox"/>	
Tap Report	<input type="checkbox"/>	
Escape Seq	<input type="checkbox"/>	
CID Enable	<input checked="" type="checkbox"/>	
Callee Inverse Polarity	<input type="checkbox"/>	
Caller Inverse Polarity	<input type="checkbox"/>	

**Figure 3-118 Configure FXS Parameters**

The following items are displayed on this screen:

- ▶ **Min Flash Detect Time:** The minimum time to detect the flash.
- ▶ **Max Flash Detect Time:** The maximum time to detect the flash.
- ▶ **Flash Key Enable:** Whether to enable digit detect after flash.
- ▶ **Switch&Release Call:** If the digit specified is detected after flash, terminate the active call and recover the call on hold.
- ▶ **Three Party Call:** If the digit specified is detected after flash, enter the conference mode.
- ▶ **Reject Key:** If the digit specified is detected after flash, reject the call on hold.
- ▶ **Switch Call Key:** If the digit specified is detected after flash, hold the active call and recover the call on hold.
- ▶ **Keep the hold call when onhook:** If selected, when hanging up in this context, the telephone rings to notify the user there is still a call on hold.
- ▶ **(#)Quick Dial Key:** Whether to send telephone number immediately after receiving the # key.
- ▶ **Asterisk Func Key:** Whether to use the '\*' key as flash key.
- ▶ **Tap Report:** Whether to report an event to server when flash detected.
- ▶ **Escape Seq:** Whether to use an escape characters when sending special DTMF.
- ▶ **CID Enable:** Whether to enable caller id globally.
- ▶ **Callee Inverse Polarity:** Whether to activate the Polarity Reversal for FXS callee.
- ▶ **Caller Inverse Polarity:** Whether to activate the Polarity Reversal for FXS caller.

### 3.5.9 Centrex

To control call each other of internal number in the same device, choose the menu

**VOIP Service→Centrex** to load the following page.

VoIP Service ==> Centrex

Enable Centrex ☒

<input type="checkbox"/>	Group Number	Ring Policy	Ring Time	Phone Number
<input type="checkbox"/>	1111	Alternate	20	<a href="#">Telephone Number</a>

1 Total 1 Pages, 1 Rows

**Figure 3-119 Centrex&Ring Group Configuration**

The following items are displayed on this screen:

- **Enable Centrex:** Whether to enable centrex function globally.

A **hunt group** is a collection of extensions that ring in a particular order when the hunt group number is dialed. Hunt groups usually have a phone number associated with them, which are referred to as the group number. Ordinal hunt groups always start ringing the first extension in the list. Alternate hunt groups remember the last number that ringed first and begins ringing on the next number in the list. when the end of the list is reached, both wrap around to the first number in the list again. With a parallel hunt group, all extensions in the list will ring at the same time.

To delete an exist entry, select it and click the **Del**.

To modify ring policy or ring time configuration, please click the **Group Number** in the exist entry which you want to modify. You can also click the **Add** button to add a new entry.

VoIP Service ==> Ring Group

Group Number  \* (digital,\*,#)

Ringing Policy

Ring Time  \* (5,90)s; default 20

**Figure 3-120 Add or Modify RingGroup**

The following items are displayed on this screen:

- **Group Number:** The phone number of this ring group.
- **Ringing Policy:** Phone ringing policy: **Alternate**, **Ordinal**, **Parallel**.
- **Ring Time:** Ring time of each member.

Click **Submit** button when finished, then you can **Add** telephone numbers to this Ring Group, you can also click the **Phone Number** in the exist entry to Add or Del telephone numbers.

VoIP Service ==> Centrex ==> Telephone Number

<input type="checkbox"/>	Index	Telephone Number
<input type="checkbox"/>	1	1001
<input type="checkbox"/>	2	6001

1 Total 1 Pages, 2 Rows

**Figure 3-121 Add or Delete Number of RingGroup**

The following items are displayed on this screen:

- **Telephone Number:** The number will be added to the ring group.

### 3.5.10 Phone Book

Choose the menu **VOIP Service**→**Phone Book** to load the following page.

VoIP Service ==> Phone Book									
<input type="checkbox"/>	Index	Prefix	Total Length	Modify Type	Modify Length	Modify Prefix Number	IP/Domain	Port	Description
<input type="checkbox"/>	2	0	0	Unmodify	0		10.0.1.1	5050	book1
1 Total 1 Pages, 1 Rows									
<input type="button" value="Add"/> <input type="button" value="Del"/>									

**Figure 3-122 Configure Phone Book**

Click the **Index** in the entry you want to modify. If you want to delete the entry, select it and click the **Del**. Click the **Add** button to add a new entry.

VoIP Service ==> Phone Book	
Phone Prefix	<input type="text" value="0"/> * (digit,*,#)
Total Length	<input type="text" value="0"/> * (0,32); 0:is no limit
Prefix Mode	<input type="text" value="Unmodify"/> ▼
IP/Domain	<input type="text" value="10.0.1.1"/> *
Port	<input type="text" value="5050"/> [0 or 1024~65535]
Description	<input type="text" value="book1"/> *
<input type="button" value="Save"/> <input type="button" value="Return"/>	

The following items are displayed on this screen:

- **Phone Prefix:** The prefix of this phone book.
- **Total Length:** The total length of number to wait before sending.
- **Prefix Mode:** Mode of processing number prefix: **Unmodify**, **Remove**, **Add**, **Modify**.
- **IP/Domain:** The IP address or domain of destination.
- **Port:** The port of destination.
- **Description:** Description of this rule.

## 3.6 System

### 3.6.1 Time Management

Menu of time management is used to manage system time.

#### 1) Manual Configuration

Choose the menu **Data Service**→**Time Management** and select **Manual Configuration** to load the following page.

System ==> Time Management

Configuration mode	Auto Configuration <input type="radio"/> Manual Configuration <input checked="" type="radio"/>
System Time :	2000-01-01 00:12:22 [HH:MM:SS]
Daylight Saving Time :	<input type="checkbox"/>
Offset :	60 Min
Start Month :	March
Start Day of Week :	Sunday
Start Day of Week Last in Month :	Last in Month
Start Hour of Day :	2
Stop Month :	December
Stop Day of Week :	Sunday
Stop Day of Week Last in Month :	Last in Month
Stop Hour of Day :	2

Save Refresh

**Figure 3-123 Time Manual Configuration**

The following items are displayed on this screen:

- ▶ **Configuration mode:** Specify configuration mode of time, **Auto Configuration** or **Manual Configuration**, default is **Manual Configuration**.
- ▶ **System Time:** Enter the system time under **Manual Configuration**.
- ▶ **Daylight Saving Time:** Enable or disable the Daylight Saving Time(DST).
- ▶ **Offset:** Enter the offset of DST.
- ▶ **Start Month:** Specify the start month of DST, range from 1 to 12 in one year.
- ▶ **Start Day of Week:** Specify the start weekday of DST, range from Sunday to Saturday.
- ▶ **Start Day of Week Last in Month:** Specify the order of start weekday in the month from pull-down list as following:
  - **First in Month**
  - **Second in Month**
  - **Third in Month**
  - **Fourth in Month**
  - **Last in Month**
- ▶ **Start Hour of Day:** Specify the start hour of DST, range from 0 to 23 in one day.
- ▶ **End Month:** Specify the end month of DST, range from 1 to 12 in one year.
- ▶ **End Day of Week:** Specify the end weekday of DST, range from Sunday to Saturday.
- ▶ **End Day of Week Last in Month:** Specify the order of end weekday in the month, similar as **Start Day of Week Last in Month**.
- ▶ **End Hour of Day:** Specify the end hour of DST, range from 0 to 23 in one day.

## 2) Auto Configuration

Choose **Auto Configuration** to load the following page:

System ==> Time Management

Configuration mode	Auto Configuration <input checked="" type="radio"/> Manual Configuration <input type="radio"/>	
Enable NTP	<input checked="" type="checkbox"/>	
NTP Service Mode	Client <input type="button" value="v"/>	
Primary NTP Server	ntp.ucsd.edu (Maximus 128 Character)	
Secondary NTP Server	ntp.univ-lyon1.fr (Maximus 128 Character)	
Time Zone	(GMT+01:00)CET-Germany, Italy, Switzerland, Tunisia <input type="button" value="v"/>	
Update Interval	3600 [60~36000]s; default:3600	
Daylight Saving Time : <input type="checkbox"/>		
Offset :	0 Min	
Start Month :	January <input type="button" value="v"/>	
Start Day of Week :	Sunday <input type="button" value="v"/>	
Start Day of Week Last in Month :	First in Month <input type="button" value="v"/>	
Start Hour of Day :	0	
Stop Month :	January <input type="button" value="v"/>	
Stop Day of Week :	Sunday <input type="button" value="v"/>	
Stop Day of Week Last in Month :	First in Month <input type="button" value="v"/>	
Stop Hour of Day :	0	

**Figure 3-124 Time Auto Configuration**

The following items are displayed on this screen:

- ▶ **Enable NTP:** Enable or disable NTP service.
- ▶ **NTP Service Mode:** Specify CPE role as NTP Client or both Client and Server.
- ▶ **Primary NTP Server:** Specify the primary NTP server for role as NTP client.
- ▶ **Second NTP Server:** Specify the second NTP server for role as NTP client.
- ▶ **Time Zone:** Enter the local time zone.
- ▶ **Update Interval:** Specify update interval for role as NTP client.

## 3.6.2 Upgrade

### 3.6.2.1 Application

Firmware upgrade via WEB interface is available. There are 2 steps to complete firmware updating.

- 1) Choose menu "**System→Upgrade**", then select the right firmware file, click **Upgrade**, wait a few minutes for firmware downloading and programming.
- 2) Choose menu "**System →Reboot**", then click **Reboot** button to reset the device.

### 3.6.2.2 Configuration

#### 3.6.2.2.1 Update Configuration

Configuration updating via WEB interface is available. There are 2 steps to complete configuration updating.

- 1) Choose menu "**System→Upgrade**", then select the right configuration file, click **Upgrade**, wait a few seconds for downloading and programming.
- 2) Choose menu "**System →Reboot**", then click **Reboot** button to reset the device.

#### 3.6.2.2.2 Export Configuration

Configuration exporting via WEB interface is available. Click the "**Export Configuration File**" to export the configuration file.



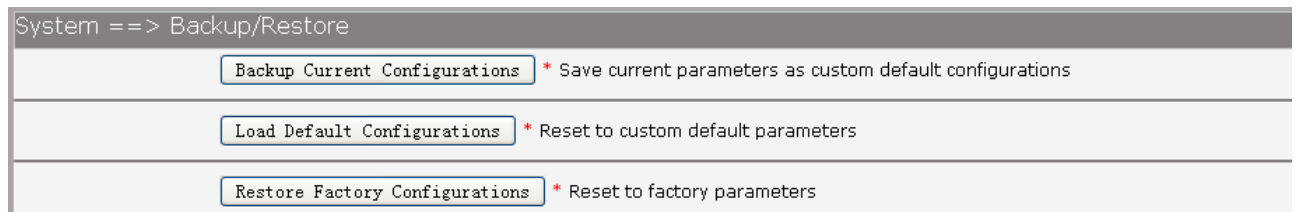
Web interface configuration index: **System→Upgrade→( Configuration)**.

### 3.6.3 Reboot System

Choose menu "**System → Reboot**", then click **Reboot** button to reset the device.

### 3.6.4 Backup/Restore

Choose the menu **System→Backup/Restore** to load the following page.



**Figure 3-125 Backup/Restore Configurations**

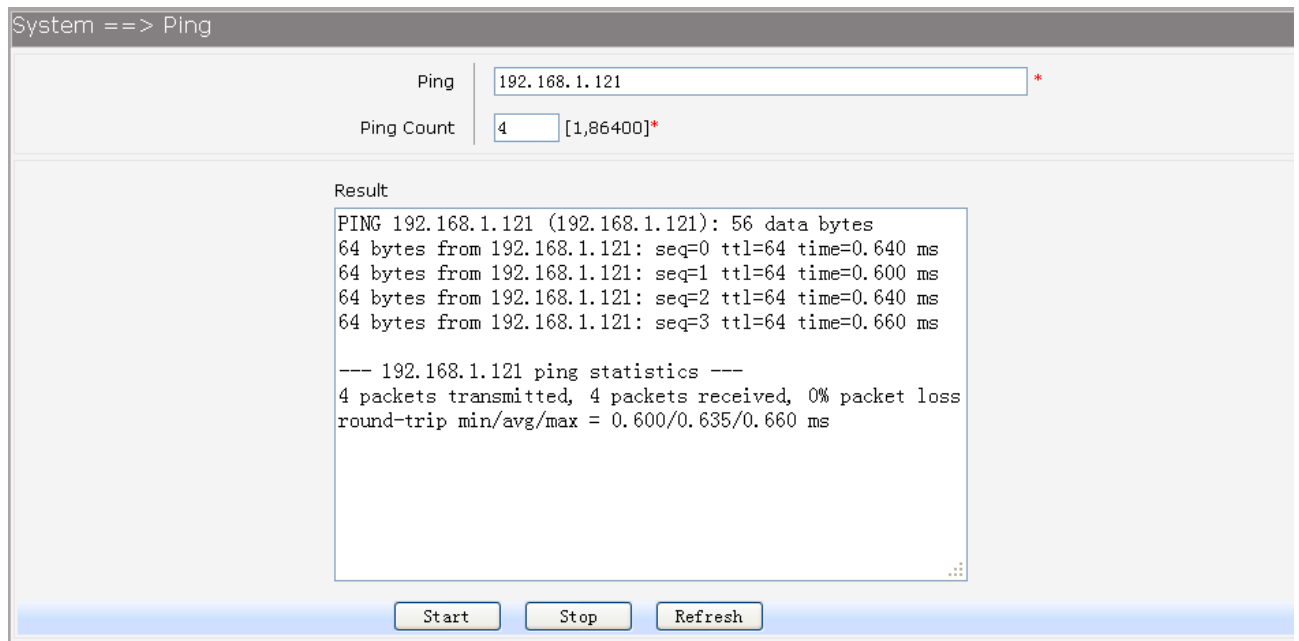
The following items are displayed on this screen:

- ▶ **Backup Current Configurations:** Save current parameters as customer default parameters.
- ▶ **Load Default Configurations:** To reset to customer default parameters.
- ▶ **Restore Factory Configurations:** To reset to factory parameters.

### 3.6.5 Diagnostic

#### 3.6.5.1 Ping

Choose menu "**System→Diagnostic→Ping**", and then you can use **Ping** function to check connectivity of your network in the following screen.



**Figure 3-126 Ping Diagnostic**

The following items are displayed on this screen:

- ▶ **Ping:** Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.

- **Ping Count:** Specifies the number of Echo Request messages sent.
  - **Result:** This page displays the result of diagnosis.
- Click **Start** button to check the connectivity of the Internet.
- Click **Stop** button to stop sending the Echo Request messages.
- Click **Refresh** button to refresh the web page.

### 3.6.5.2 Tcpcdump

You can use tcpcdump tool to capture the packets, and show the result of capture packets.

Choose the menu **System**→**Diagnostic**→**Tcpcdump** to load the following page.

**Figure 3-127 Tcpcdump Diagnostic**

The following items are displayed on this screen:

- **Interface:** By selecting the interface, only packets through this interface will be captured.
  - **Protocol:** By selecting the protocol, only packets of this protocol will be captured.
  - **Tcpcdump:** Enter some options of tcpcdump(e.g. -n -s0 -c 100)
  - **Result:** This page displays the result of capture packets.
- Click **Start** button to capture the packets which correspond to the configuration requirement.
- Click **Stop** button to stop capturing the packets.
- Click **"\*.pcap"** to open or download the capture packets file.
- Click **"clean"** to delete all the packets file.
- Click **Refresh** button to refresh the web page.

### 3.6.5.3 WAN Speed Test

Test the download speed and upload speed of WAN interface, and show the result on the web page.

Choose the menu **System**→**Diagnostic**→**WAN Speed Test** to load the following page.

**Figure 3-128 WAN Speed Test**

The following items are displayed on this screen:

- **Download URL:** Enter the URL to test the download speed of WAN. For example <http://speedtest1.szunicom.com/speedtest/random1000x1000.jpg>
  - **Upload URL:** Enter the URL to test the upload speed of WAN. For example <http://speedtest1.szunicom.com/speedtest/random2000x2000.jpg>
- Click the **Start** button to starting test.

### 3.6.6 User Management

You can change the factory default user password of the device.

Choose the menu **System**→**User Management** to load the following page.

**Figure 3-129 User Management**

The following items are displayed on this screen:

- **Username:** You can select the user with different permissions. However, you can not select the user whose permission is higher than your permission.
- **New Password:** Enter the new password for specified user, not more than 32 characters, and the space is not supported.
- **Confirm Password:** Enter the new password again to confirm for specified user, not more than 32 characters, and the space is not supported.

Click the **Save** button when finished.

### 3.6.7 System Log

#### 3.6.7.1 Log Config

Choose the menu **System**→**System Log**→**Log Config** to load the following page.

**Figure 3-130 Configure System Log**

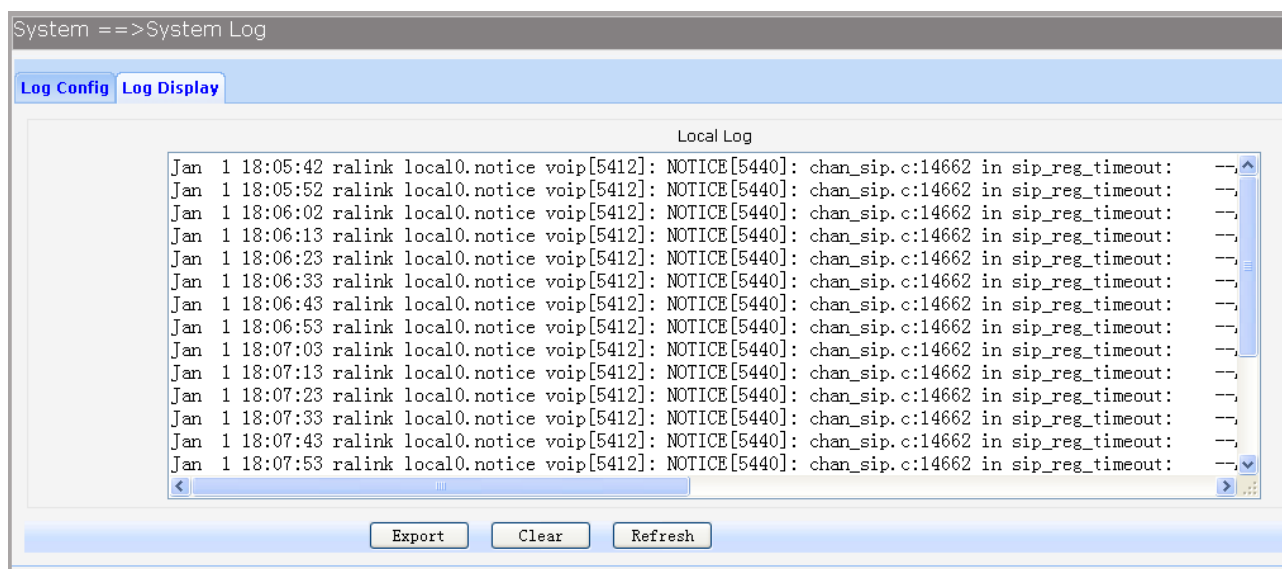
The following items are displayed on this screen:

- **Log Level:** By selecting the log level, only logs of this level will be shown.
- **Log Content:** By selecting the log content, only logs of selected content will be shown.
- **Local Log Enable:** Check this box to enable local log function.
- **Remote Log Enable:** Check this box to enable remote log function, the logs will be send to the Log Server.
- **Log Server IP:** Enter the IP address of the Log Server.
- **Log Server Port:** Enter the port that Log service used.

Click the **Save** button when finished.

### 3.6.7.2 Log Display

Choose the menu **System**→**System Log**→**Log Display** to load the following page.



**Figure 3-131 Display System Log**

Click the **Export** button to export all the local logs as a file.

Click the **Clear** button to clear all the local logs from the device permanently, not just from the page.

Click **Refresh** button to refresh the web page.

### 3.6.8 TR069

**TR-069** (Technical Report 069) is a Broadband Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. As a bi-directional SOAP/HTTP-based protocol, it provides the communication between customer-premises equipment (CPE) and Auto Configuration Servers (ACS). It includes both a safe auto configuration and the control of other CPE management functions within an integrated framework.

Choose the menu **System**→**TR069** to load the following page.

System ==> TR069 (WARNING:new settings are only valid after [Restarting](#))

Serial Number	000EB48G9000000eb409ad20		
Enable	<input checked="" type="checkbox"/>		
ACS Address	<input type="text" value="192.168.1.121"/>	*	
ACS Port	<input type="text" value="8080"/>	*(0,65535)	
ACS Server Name	<input type="text" value="ACS-server/ACS"/>	*	
SSL Enable	<input type="checkbox"/>		
Scheduler Send Inform	<input checked="" type="checkbox"/> <input type="text" value="3600"/>	(1,4294967295)s	

Single Account Enable	<input checked="" type="checkbox"/>		
TR069 Account	<input type="text" value="acs"/>	*	
TR069 password	<input type="password" value="●●●"/>	*	

Connection Request Auth	<input type="checkbox"/>		
Connection Request Username	<input type="text" value="cpe"/>		
Connection Request Password	<input type="password" value="●●●"/>		
CPE Server Name	<input type="text" value="cpe"/>		
CPE Port	<input type="text" value="8099"/>		
Status	Connect Success		
Fail Reason	Connected Success		

**Figure 3-132 Configure TR069**

The following items are displayed on this screen:

- ▶ **Serial Number:** The serial number of device. Read only.
- ▶ **Enable:** Enable or disable the TR069 function globally.
- ▶ **ACS Address:** Enter the IP address or domain name of ACS.
- ▶ **ACS Port:** Enter the port of ACS.
- ▶ **ACS Server Name:** Enter the TR069 server name of ACS.
- ▶ **SSL Enable:** Enable or disable the SSL(Secure Sockets Layer) for TR069.
- ▶ **Scheduler Send Inform:** Whether or not the CPE must periodically send CPE information to Server using the Inform method call. Enter the duration in seconds of the interval if enabled.
- ▶ **Single Account Enable:** Whether or not the TR069 Account is enabled.
- ▶ **TR069 Account:** Username used to authenticate the CPE when making a connection to the ACS.
- ▶ **TR069 password:** Password used to authenticate the CPE when making a connection to the ACS.
- ▶ **Connection Request Auth:** Whether to authenticate an ACS making a Connection Request to the CPE.
- ▶ **Connection Request Username:** Username used to authenticate an ACS making a Connection Request to the CPE.
- ▶ **Connection Request Password:** Password used to authenticate an ACS making a Connection Request to the CPE.

- **CPE Server Name:** A part of the HTTP URL for an ACS to make a Connection Request notification to the CPE. In the form: `http://host:port/path`
- **CPE Port:** A part of the HTTP URL for an ACS to make a Connection Request notification to the CPE. In the form: `http://host:port/path`
- **Status:** Connection Status when CPE making a connection to the ACS. Read only.
- **Fail Reason:** Show reason for the failure when CPE making a connection to the ACS. Read only.

Click the **Save** button when finished.

Click **Refresh** button to refresh the web page.

### 3.6.9 SNMP

You can configure the SNMP parameters and view the registration status of SNMP. Choose the menu **System**→**SNMP** to load the following page.

**Figure 3-133 Configure SNMP**

The following items are displayed on this screen:

- **Register Enable:** Check this box to enable SNMP register.
- **Server Address or Domain:** Enter the IP address or domain name of register server.
- **Server Port:** Enter the port of Register Server.
- **TRAP Message Interval:** Set the sending interval between TRAP messages.
- **Regional Identity:** Set the identity of regional.
- **Device Identifier:** Set the identifier of device.
- **Enable Double Register Server:** Check this box to enable backup Register Server.
- **Backup Server Address or Domain:** Enter the IP Address or Domain Name of Backup Register Server.
- **Backup Server Port:** Enter the port of Backup Register Server.
- **Registration Status:** The status of registration. Read only.

Click the **Save** button when finished.

Click **Refresh** button to refresh the web page.

### 3.6.10 User Access Right

If the permission level of login user is super, you can see this web page. On this page, you can change the access right of the user to access the web pages.

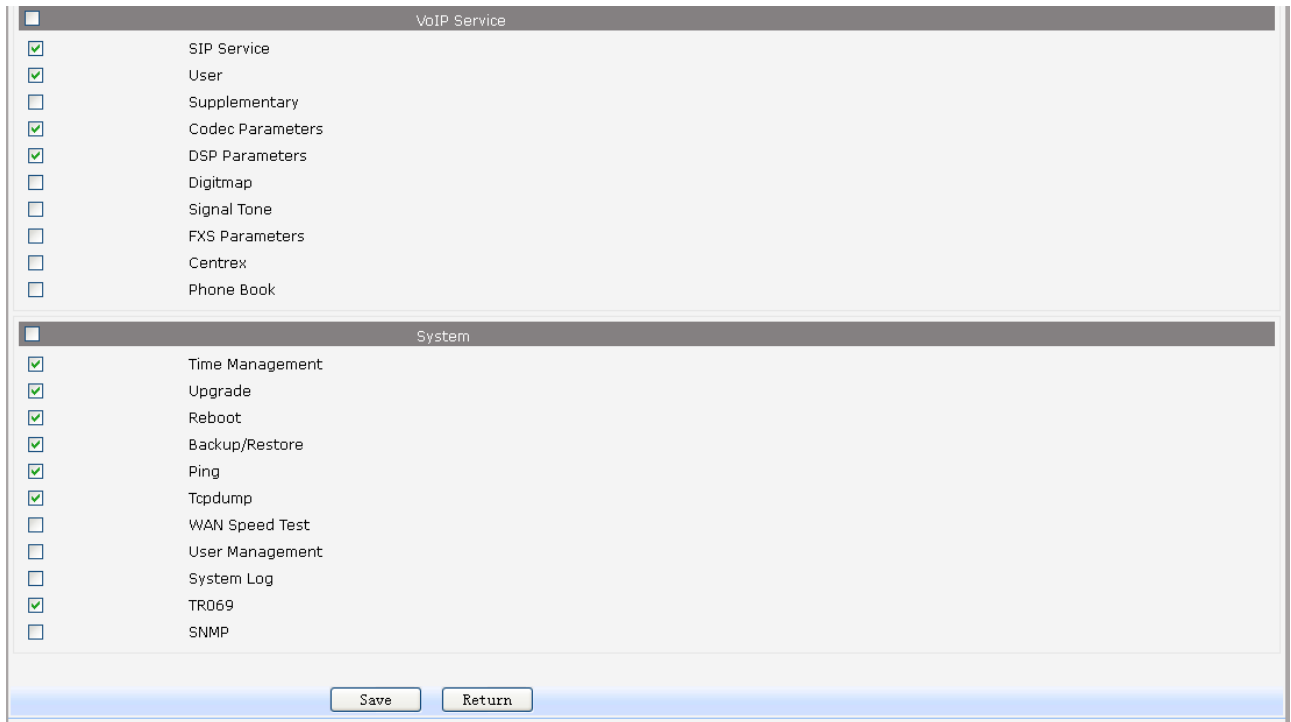
Choose the menu **System**→**User Access Right** to load the following page.

System ==> User Access Right		
Index	Username	Access Detail
1	admin	<a href="#">detail</a>
2	guest	<a href="#">detail</a>

**Figure 3-134 View users**

If you want to change the user access right, click **detail** in the entry to load the following page.

System ==> WebAccessSetting	
<b>Network</b>	
<input checked="" type="checkbox"/>	Status
<input checked="" type="checkbox"/>	WAN
<input checked="" type="checkbox"/>	LAN
<input checked="" type="checkbox"/>	WLAN
<input checked="" type="checkbox"/>	3G Modem
<input type="checkbox"/>	VLAN
<input type="checkbox"/>	PortMirror
<input type="checkbox"/>	IPv6
<b>Data Service</b>	
<input checked="" type="checkbox"/>	Status
<input checked="" type="checkbox"/>	DHCP Server
<input checked="" type="checkbox"/>	NAT Basic-Settings
<input checked="" type="checkbox"/>	PAT Settings
<input checked="" type="checkbox"/>	DMZ Settings
<input type="checkbox"/>	ALG Settings
<input checked="" type="checkbox"/>	Attack Defense
<input checked="" type="checkbox"/>	Service Type
<input checked="" type="checkbox"/>	Internet Access-Ctrl
<input checked="" type="checkbox"/>	Management Access-Ctrl
<input checked="" type="checkbox"/>	Filter Strategy
<input type="checkbox"/>	IP&MAC Binding
<input type="checkbox"/>	Basic Settings
<input type="checkbox"/>	ACL
<input type="checkbox"/>	Port Rate Limit
<input type="checkbox"/>	Flow Rate Limit
<input type="checkbox"/>	Service
<input type="checkbox"/>	DDNS
<input type="checkbox"/>	GRE VPN
<input type="checkbox"/>	PPTP VPN
<input type="checkbox"/>	L2TP VPN
<input type="checkbox"/>	IPSec
<input checked="" type="checkbox"/>	Static Route
<input type="checkbox"/>	Policy Route
<input type="checkbox"/>	RIP
<input type="checkbox"/>	UPnP Parameter
<input type="checkbox"/>	Apply Filter Control
<input type="checkbox"/>	Multicast
<input checked="" type="checkbox"/>	Share File



VoIP Service	
<input checked="" type="checkbox"/>	SIP Service
<input checked="" type="checkbox"/>	User
<input type="checkbox"/>	Supplementary
<input checked="" type="checkbox"/>	Codec Parameters
<input checked="" type="checkbox"/>	DSP Parameters
<input type="checkbox"/>	Digitmap
<input type="checkbox"/>	Signal Tone
<input type="checkbox"/>	FXS Parameters
<input type="checkbox"/>	Centrex
<input type="checkbox"/>	Phone Book

System	
<input checked="" type="checkbox"/>	Time Management
<input checked="" type="checkbox"/>	Upgrade
<input checked="" type="checkbox"/>	Reboot
<input checked="" type="checkbox"/>	Backup/Restore
<input checked="" type="checkbox"/>	Ping
<input checked="" type="checkbox"/>	Tcpcdump
<input type="checkbox"/>	WAN Speed Test
<input type="checkbox"/>	User Management
<input type="checkbox"/>	System Log
<input checked="" type="checkbox"/>	TR069
<input type="checkbox"/>	SNMP

Save Return

Figure 3-135 Modify User Access Right

## 3.7 Apply

Follow the prompts, Some parameters will take effect after click the button of “**Apply**”.



Home | Network | Data Service | VoIP Service | System | **Apply** | Logout |

System ==> Time Management (WARNING: new settings are only valid after clicked [Apply])

Figure 3-136 Apply

## 3.8 Print Function

The device supports to link printer port and provides share printing capabilities to other computers. To use print function, you need do the following steps.

### 1. Add Printer

Open the windows of the Control Panel, select Printers and Faxes, and add the printer



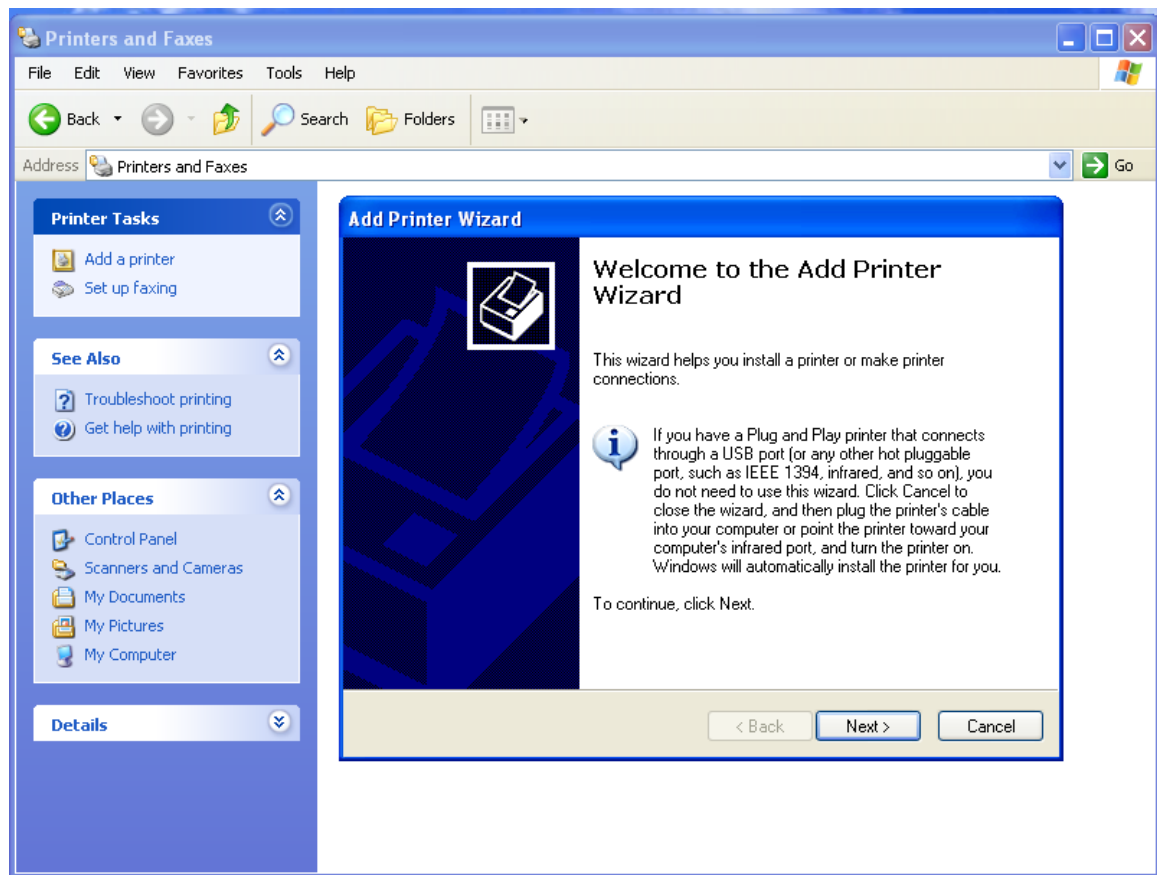
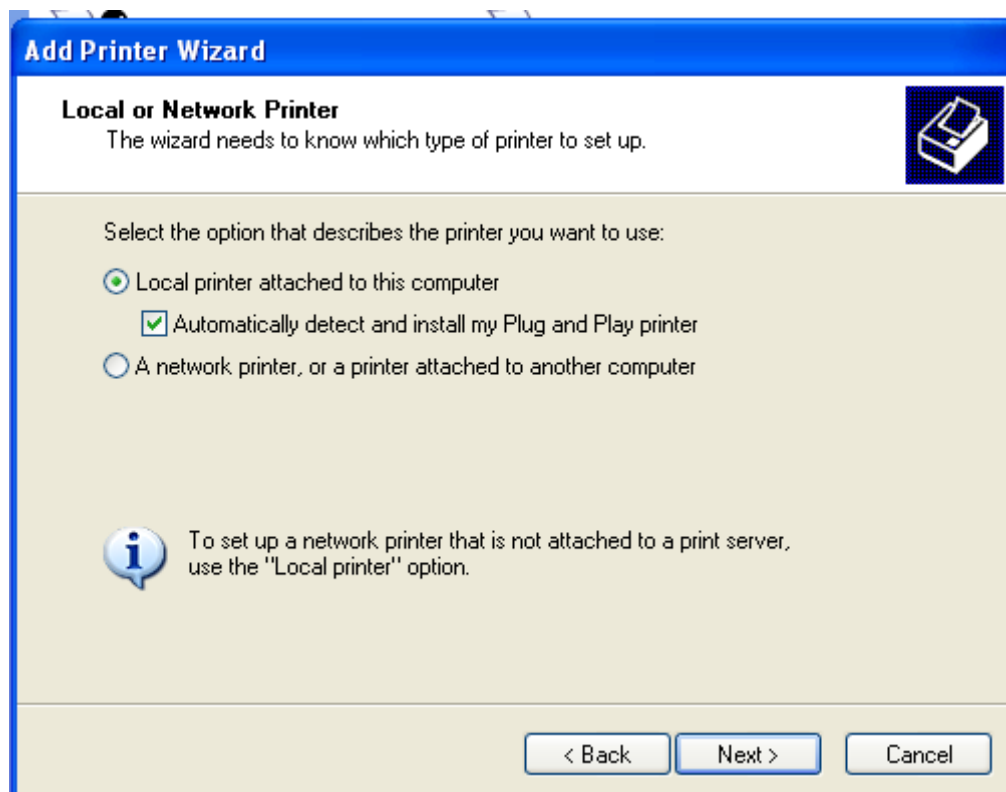


Figure 3-137 Add Printer

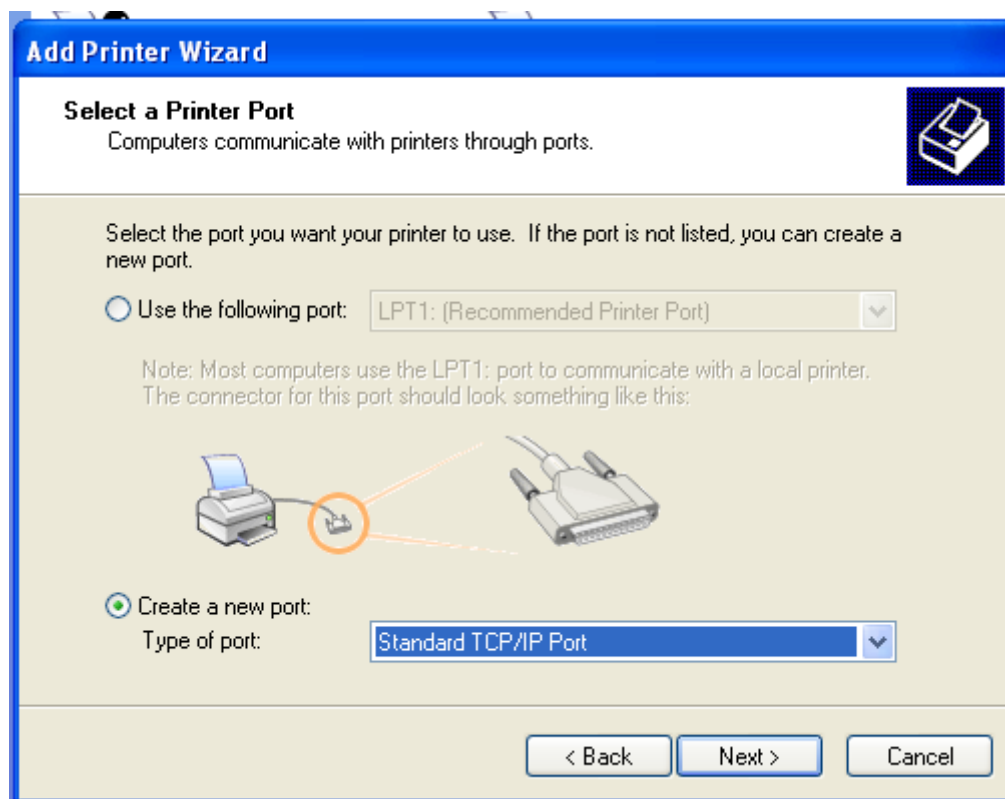
## 2. Connecting local printer

Select "Local printer attached to this computer."

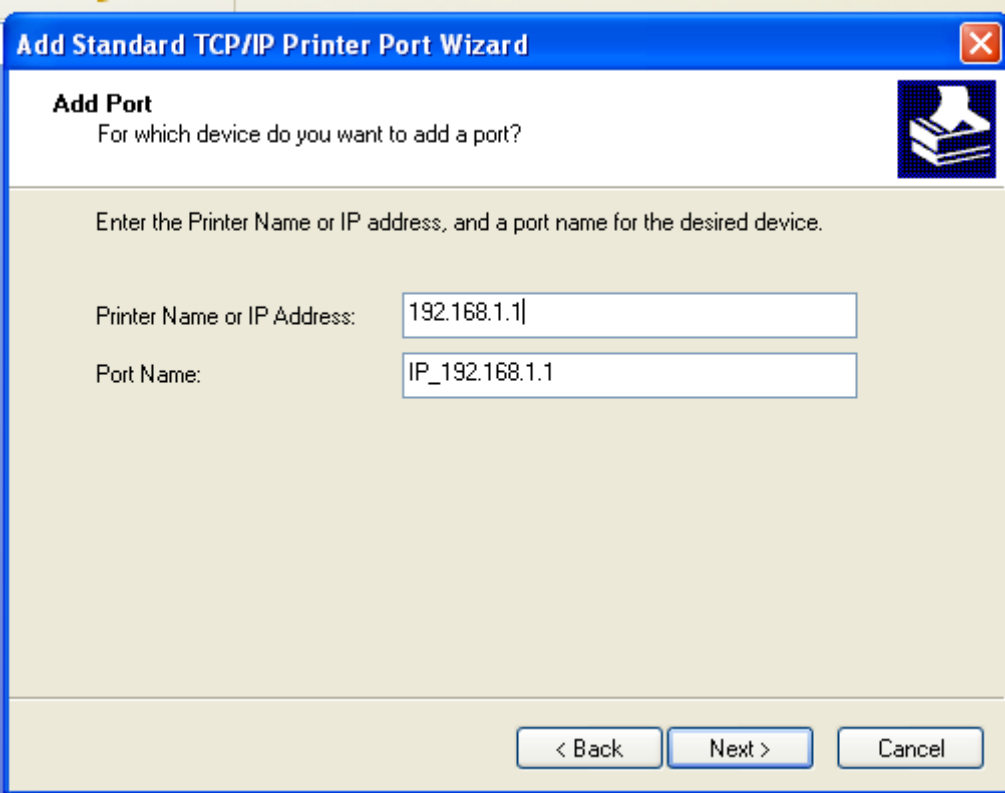


**Figure 3-138 Connecting local printer****3. Create a new port**

Select "Create a new port" and select "Standard TCP / IP Port"

**Figure 3-139 Create a new port****4. Add print device**

Click Next, and add IP devices, assuming the device IP is 192.168.1.1.



**Add Standard TCP/IP Printer Port Wizard**

**Add Port**  
For which device do you want to add a port?

Enter the Printer Name or IP address, and a port name for the desired device.

Printer Name or IP Address: 192.168.1.1

Port Name: IP\_192.168.1.1

< Back   Next >   Cancel

**Figure 3-140 Add IP LAN devices**

## **5. Configure printer port**

Select "Custom", click "Settings" to confirm the agreement as "RAW (R)"

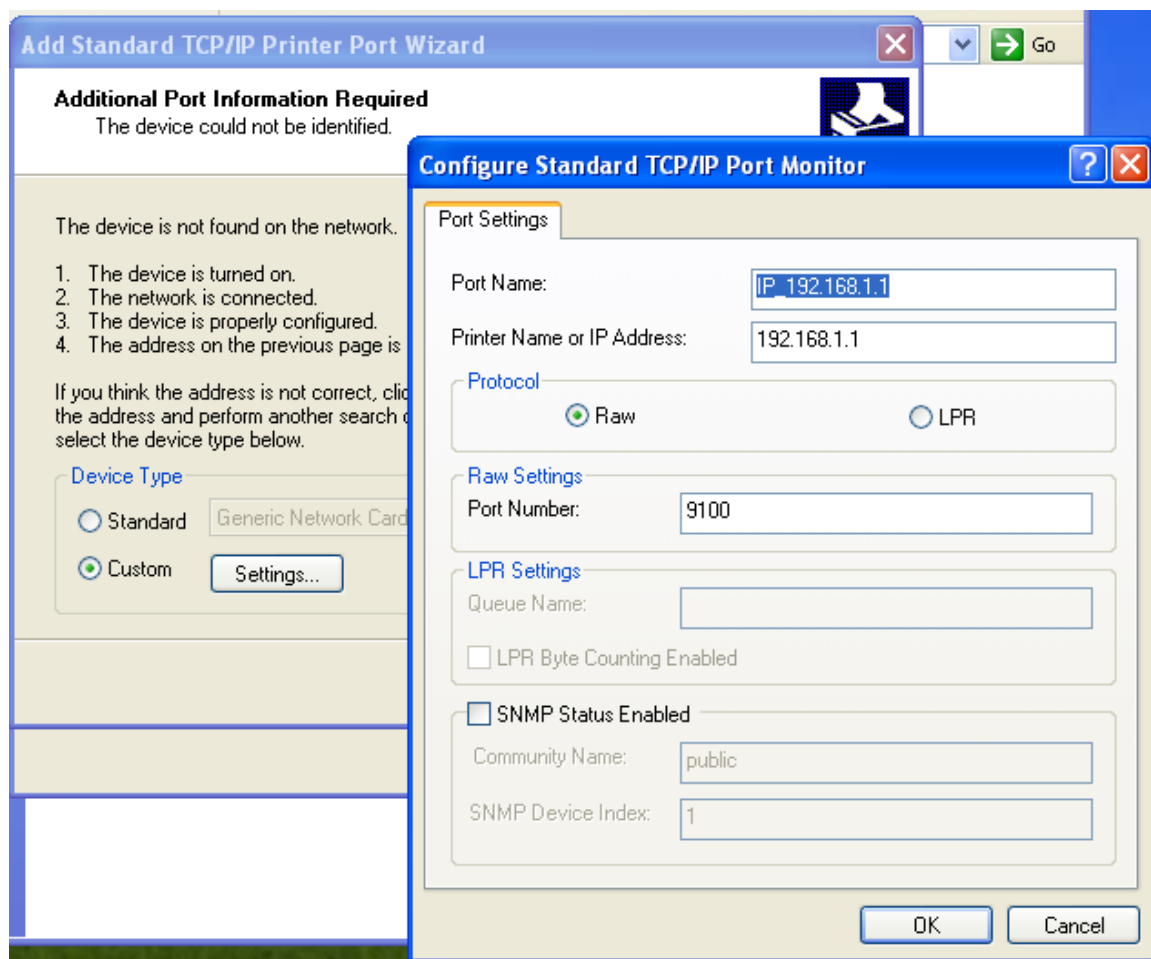


Figure 3-141 Configurer printer port

## 6. Add Printer Driver

According to the printer manufacturer and printer type, select the appropriate driver. If the computer has not printer driver, you need to install the printer driver.

After adding the printer, you can print through the USB printer.

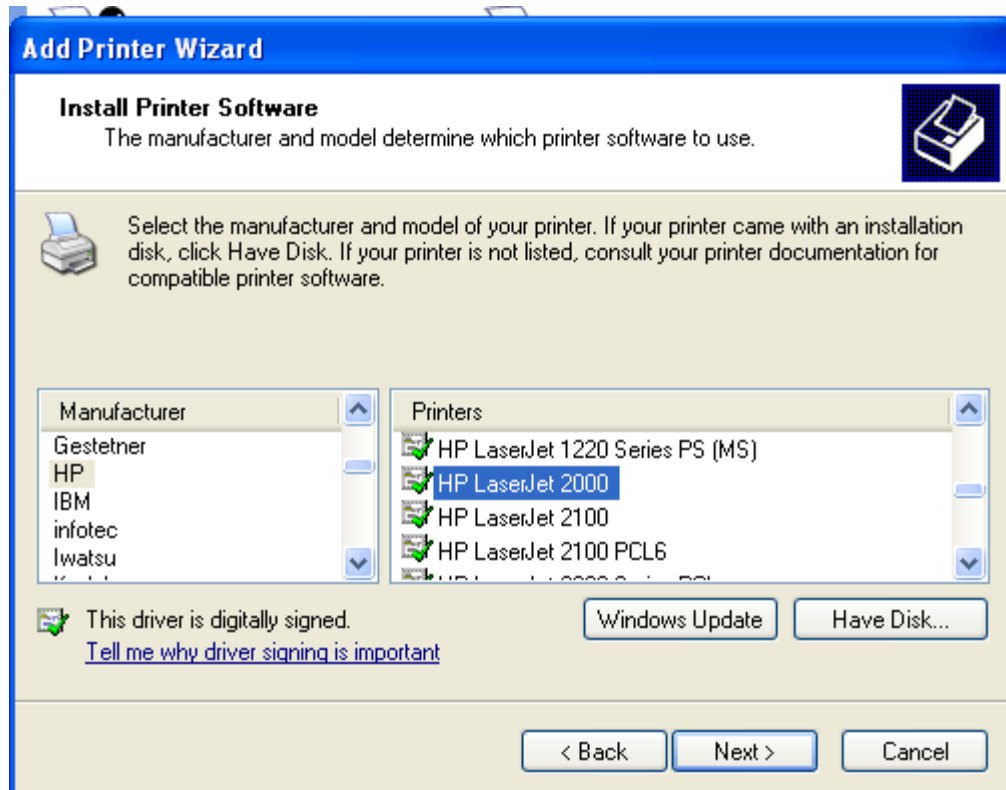


Figure 3-142 Add Printer Driver

## 4 CLI Introduction

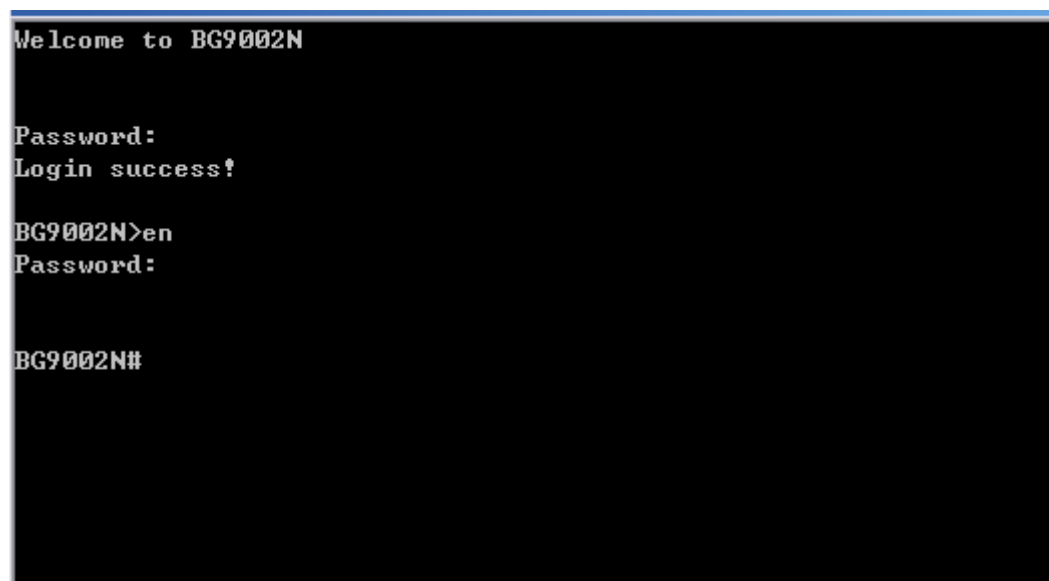
### 4.1 Login

The CLI interface is ready for accessing about one minute after the device powers on. The default LAN IP address is 192.168.100.1, you can access the CLI interface via either WAN port or LAN port. Enter telnet with IP address and then press ENTER, you can get access to the Login interface. Such as IP address is 192.168.100.17, you can input “telnet 192.168.100.17”, and then press ENTER, it will show as below:



**Figure 4-1 Telnet Login**

And input the “password” and “en” and the privileged password, you will enter the CLI command interface:



**Figure 4-2 Telnet Command Interface**

Input the command “set language” to set the CLI language:

```
Welcome to BG9002N

Password:
Login success!

BG9002N>en
Password:

BG9002N#set lang

BG9002N#set language
CLI语言(CLI language):
0 -- 中文(Chinese)
1 -- 英文(English)
->[1]:1

BG9002N#
```

Figure 4-3 Set CLI Language

## 4.2 Network

### 4.2.1 3G Modem

The command “show 3gmodem” show the 3G modem information as below:

```
BG9002N#show 3gmodem

SP Network.....: Swisscom
Connect Mode.....: Manual
Online Mode.....:
  Disconnect After Idle Interval
Idle Interval.....: 60
Authentication.....: Auto
DNS.....: 192.168.5.6
TCP MSS.....: 1460
MTU.....: 1500
Data Link Backup.....: Enable
Heartbeat Address.....: 192.168.6.3
```

Figure 4-4 Show 3G Modem Information

The command “set 3gmodem” configure the 3G modem parameters as below.

```

BG9002N#set 3gmodem
->SP Network<0-Other,1-Swisscom>[1]:
->Connect Mode<0-Manual,1-Auto>[0]:
->Online Mode<0-Always Online,1-Disconnect After Idle Interval>[1]:
->Idle Interval<1~65535>[60]:
->Advanced Parameters? 'yes' or 'no'[no]:y
->Authentication <0-Auto,1-CHAP,2-PAP>[0]:
->DNS[192.168.5.6]:
->TCP MSS<128~2048>[1460]:
->MTU<128~1500>[1460]:
->Data Link Backup? 'yes' or 'no'[no]:y
->Heartbeat Address[0.0.0.0]:192.168.6.3
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
BG9002N#

```

**Figure 4-5 Configure 3G Modem Parameters**

The following items are displayed on this screen:

- ▶ **SP Network:** **Other** or **Swisscom**. If it is not the target user, you need to select the other.
- ▶ **Connect Mode:** **Manual** or **Auto**. The default is Auto.
- ▶ **Online Mode:** **always online** and **disconnect after idle interval**. The default is “always online”.  
The default idle interval is 60 seconds.

If **Other** is selected, the following parameters appear:

- ▶ **Username:** 3G network dial-up username.
- ▶ **Password:** 3G network dial-up password.
- ▶ **Dial Number:** 3G network dial numbers.
- ▶ **APN:** 3G network access APN.
- ▶ **PIN:** 3G networks need to use dial-up PIN code, if not, can be set to empty.

**Advanced Parameters:**

- ▶ **Authentication:** 3G dial-up authentication, **CHAP**, **PAP**, **Auto** are provided. Default is **Auto**.
- ▶ **DNS:** The default is obtained from the dial-up network devices automatically. You can also configure DNS manually.
- ▶ **TCP MSS:** Configure TCP maximum segment, we recommend using the default value.
- ▶ **MTU:** Configure 3G link MTU, the default value is recommended
- ▶ **Data Link Backup:** When enabled, if WAN uplink port is disconnected, the routing switches to the 3G link.
- ▶ **Heartbeat Address:** Set the heartbeat detecting address of the link, the default configuration is not required.

The command “show 3gmodem-status” show the 3G modem status as below:

```

BG9002N#show 3gmodem-status

Device Status.....: Unready
SIM Card Status.....: Unready
Product Name.....:
Manufacturer Name.....:
SP Name.....:
Signal Quality.....: 0
Connection Status.....: Disconnected

BG9002N#

```



**Figure 4-6 Show 3G Modem Status**

The following items are displayed on this screen:

- ▶ **Device Status:** Indicates whether to insert 3G module.
- ▶ **SIM Card Status:** Indicates whether to insert 3G modem in the SIM card, the ready state means the SIM card is detected.
- ▶ **Product Name:** 3G modem Product Type.
- ▶ **Manufacturer Name:** 3G modem vendor name.
- ▶ **SP Name:** 3G modem service provider name.
- ▶ **Signal Quality:** Signal quality of 3G Modem, up to 31.
- ▶ **Connection Status:** Connected or disconnected.

## 4.2.2 Port Management

### 4.2.2.1 Port Mirror

The command “show port-mirror” show the port mirror information as below:

```

BG9002N#show port-mirror
Destination Mirror Port.....: LAN1

LAN2.....: Not enable
LAN3.....: Ingress & Egress
LAN4.....: Ingress & Egress
WAN.....: Ingress & Egress

BG9002N#_

```

**Figure 4-7 Show Port Mirror Information**

The command “set port-mirror” configure the port mirror parameters as below.

```

BG9002N#set port-mirror
->Enable Port Mirror 'yes' or 'no' [yes]:
->Destination Port<0-WAN,1~LAN1,2-LAN2,3-LAN3,4-LAN4>[1]:
->Source Port<Bit:0-WAN,1~LAN1,2-LAN2,3-LAN3,4-LAN4>[0x19]: 0x18
->Mirror Type<0-ingress, 1-egress, 2-both>[2]:
Really want to modify? 'yes' or 'no' [yes]:
The configuration will take effect after saved and reloaded!

BG9002N#

```

**Figure 4-8 Configure Port Mirror Parameters**

The following items are displayed on this screen:

- ▶ **Enable Port Mirror:** Enable or disable port mirror.
- ▶ **Destination Port:** The duplicate of packets from **Source Port** will send to this destination port.
- ▶ **Source Port:** All packets received from **Source Port** will be duplicated and the duplicate will be send to **Destination Port**.

### 4.2.2.2 Media Type

The command “show port-status” show the port status information as below:

```

BG9002N#show port-status
Switch port:
  LAN1.....: Link down!
  LAN2.....: 10Mbps, Half Duplex, Auto-neg: Enable
  LAN3.....: Link down!
  LAN4.....: Link down!
  WAN .....: Link down!
BG9002N#

```

Figure 4-9 Show Port Status Information

The command “show port media-type” show the port media type information as below:

```

BG9002N#set port media-type
Switch port:
  WAN <-> port5, LAN1~4 <-> port1~4
  But if WAN is fiber interface: LAN1~4 <-> port1~4

->Input port index(1~5)[1]:
->Connection type:
  0 - 10Mbps, Half Duplex
  1 - 10Mbps, Full Duplex
  2 - 100Mbps, Half Duplex
  3 - 100Mbps, Full Duplex
  4 - 1000Mbps, Full Duplex
  5 - Auto-Negotiation
->Input connection type[4]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
BG9002N#

```

Figure 4-10 Show Port Media Type Information

The command “set port media-type” configure the port media type parameters as below.

```

BG9002N#show port media-type
WAN.....:1000Mbps, Full Duplex
LAN1.....:Auto-Negotiation
LAN2.....:Auto-Negotiation
LAN3.....:Auto-Negotiation
LAN4.....:Auto-Negotiation
BG9002N#

```

Figure 4-11 Configure Port Media Type Parameters

The following items are displayed on this screen:

- ▶ **Media Type:** provides the following six modes to all physical ports: 10M Half Duplex, 10M Full Duplex, 100M Half Duplex, 100M Full Duplex, 1000M Full Duplex, Auto-Negotiation.
- ▶ **Current Status:** Current link status of all physical ports. Read only.

### 4.2.3 Wan Parameter

#### 4.2.3.1 Show Wan Parameter

The command “show wan” show the WAN interface configuration as below:

```
BG9002N#show wan
->Please select one interface name to show<
1----DATA
2----VOICE
3----MGMT
4----OTHER1
5----OTHER2>[1]:
```

**Figure 4-12 Show Wan Parameter**

The wan interfaces include DATA、VOICE、MGMT、OTHER1 and OTHER2.

Input “1” to show DATA parameter as below:

```
BG9002N#show wan
->Please select one interface name to show<
1----DATA
2----VOICE
3----MGMT
4----OTHER1
5----OTHER2>[1]:

Interface Name.....:DATA
Enable or not.....:yes
LINK TYPE.....:PPPOE
Vlan Enable.....:yes
VLAN ID.....:2
Priority Level.....:3
Primary DNS.....:10.0.0.1
MTU.....:1500
Username.....:pppoeuser
Password.....:*****
AC Name.....:dsfsdf
Service Name.....:fdgfdg
LCP Interval.....:10
LCP Max Fails.....:5
```

**Figure 4-13 Show DATA Interface Parameter**

Input “2” to show VOICE parameter as below:

```

BG9002N#show wan
->Please select one interface name to show<
1----DATA
2----VOICE
3----MGMT
4----OTHER1
5----OTHER2>[1]:2

Interface Name.....:VOICE
Enable or not.....:yes
LINK TYPE.....:DHCP
Ulan Enable.....:yes
VLAN ID.....:1
Priority Level.....:0
Primary DNS.....:192.168.100.9
Secondary DNS.....:138.1.60.1
MTU.....:1500
Specify Server Ip or not.....:yes
Server IP address.....:138.0.60.2
Vendor Class Identifier or not.....:yes
Enterprise Code.....:3
Manufacture name.....:company
Device Class.....:device1
Device Type.....:type1
Device version.....:version1

```

Figure 4-14 Show VOICE Interface Parameter

Input "3" to show MGMT parameter as below:

```

BG9002N#show wan
->Please select one interface name to show<
1----DATA
2----VOICE
3----MGMT
4----OTHER1
5----OTHER2>[1]:3

Interface Name.....:MGMT
Enable or not.....:yes
LINK TYPE.....:DHCP
Ulan Enable.....:yes
VLAN ID.....:3
Priority Level.....:1
Primary DNS.....:138.0.60.2
Secondary DNS.....:138.1.60.1
MTU.....:1500
Specify Server Ip or not.....:yes
Server IP address.....:138.0.60.2
Vendor Class Identifier or not.....:no
Enterprise Code.....:0
Manufacture name.....:company1
Device Class.....:device2
Device Type.....:type3
Device version.....:version2

```

Figure 4-15 Show MGMT Interface Parameter

Input "4" to show OTHER1 parameter as below:

```
BG9002N#show wan
->Please select one interface name to show<
1----DATA
2----VOICE
3----MGMT
4----OTHER1
5----OTHER2>[1]:4

Interface Name.....:OTHER1
Enable or not.....:yes
LINK TYPE.....:PPTP
Vlan Enable.....:yes
VLAN ID.....:4
Priority Level.....:0
Primary DNS.....:138.0.60.2
Secondary DNS.....:138.1.60.1
MTU.....:1500
Specify Server Ip or not.....:no
Vendor Class Identifier or not.....:no
Enterprise Code.....:0
Manufacture name.....:
Device Class.....:
Device Type.....:
Device version.....:
Server IP.....:138.0.60.2
PPTP Username.....:gkser
PPTP Password.....:*****
Enable Encryption or not.....:no
```

Figure 4-16 Show OTHER1 Interface Parameter

Input "5" to show OTHER2 parameter as below:

```

BG9002N#show wan
->Please select one interface name to show<
1----DATA
2----VOICE
3----MGMT
4----OTHER1
5----OTHER2>[1]:5

Interface Name.....:OTHER2
Enable or not.....:yes
LINK TYPE.....:L2TP
Vlan Enable.....:yes
VLAN ID.....:5
Priority Level.....:0
Primary DNS.....:138.0.60.2
Secondary DNS.....:138.1.60.1
MTU.....:1500
Specify Server Ip or not.....:yes
Server IP address.....:138.0.60.2
Vendor Class Identifier or not.....:yes
Enterprise Code.....:3
Manufacture name.....:comany5
Device Class.....:class5
Device Type.....:type5
Device version.....:version5
Server IP.....:138.0.60.1
L2TP username.....:gkser
L2TP password.....:*****

```

Figure 4-17 Show OTHER2 Interface Parameter

#### 4.2.3.2 Configure Wan Parameter

The command "set wan" configure the wan interface parameter as below:

```

BG9002N#set wan
->Please select one interface name to show<
1----DATA
2----VOICE
3----MGMT
4----OTHER1
5----OTHER2>[1]:

```

Figure 4-18 Configure WAN Parameter

The wan interfaces include DATA、VOICE、MGMT、OTHER1 and OTHER2.

Input "1" to configure DATA parameter as below:

```

BG9002N#set wan
->Please select one interface name to show<
1----DATA
2----VOICE
3----MGMT
4----OTHER1
5----OTHER2>[1]:
->LINK TYPE<0-STATIC IP,1-PPPOE,2-DHCP,3-PPTP,4-L2TP>[1]:
->Vlan Enable[yes]:
->VLAN ID<1-4095>[2]:
->Priority Level<0-7>[3]:
->Primary DNS[10.0.0.1]:
->Secondary DNS[0.0.0.0]:
->MTU<512-1500>[1500]:
->Username[pppoeuser]:
->Password[*****]:
->AC Name[dsfsdf]:
->Service Name[fdgfdg]:
->LCP Interval<1-3000>[10]:
->LCP Max Fails[5]:
->Really want to modify? 'yes' or 'no'[yes]:

The configuration will take effect after saved and reset!

```

**Figure 4-19 Configure DATA Interface Parameter**

The following items are displayed on this screen:

- ▶ **Enable:** Enable this WAN interface (DATA can't be disabled).
- ▶ **Type:** Select PPPoE if your ISP provides xDSL Virtual Dial-up connection.
- ▶ **VLAN Enable:** Optional. Enable VLAN to configure VLAN ID and VLAN Priority Level.
- ▶ **VLAN ID:** Optional. VLAN ID of this WAN interface.
- ▶ **Priority Level:** Optional. VLAN Priority Level of this WAN interface.
- ▶ **Primary DNS:** Enter the IP address of your ISP's Primary DNS (Domain Name Server) manually. If you are not clear, please consult your ISP. It's not allowed to access the Internet via domain name if the Primary DNS field is blank.
- ▶ **Secondary DNS:** Optional. If a Secondary DNS Server address is available, enter it.
- ▶ **Username:** Enter the Account Name provided by your ISP. If you are not clear, please consult your ISP.
- ▶ **Password:** Enter the Password provided by your ISP.
- ▶ **Service Name /AC Name:** Optional. The service name and AC (Access Concentrator) name, which should not be configured unless you are sure it is necessary for your ISP. In most cases, leaving these fields blank will work.
- ▶ **LCP Interval:** PPPoE will send an LCP echo-request frame to the peer every **LCP interval** seconds.
- ▶ **LCP Max Fails:** PPPoE will presume the peer to be dead if **LCP Max Fails** LCP echo-requests are send without receiving a valid LCP echo-reply.

Input "2" to configure VOICE parameter as below:

```

BG9002N#set wan
->Please select one interface name to show<
 1----DATA
 2----VOICE
 3----MGMT
 4----OTHER1
 5----OTHER2>[1]:2
->Enable or not[yes]:
->LINK TYPE<0-STATIC IP,1-PPPOE,2-DHCP,3-PPTP,4-L2TP>[2]:0
->Vlan Enable[nol]:y
->VLAN ID<1-4095>[1]:
->Priority Level<0-7>[0]:
->Primary DNS[192.168.100.9]:
->Secondary DNS[138.1.60.1]:
->MTU<512-1508>[1500]:
->IP Address[138.0.60.1]:
->Netmask[0.0.0.0]:255.255.255.0
->Enable Gateway or not[nol]:
->Really want to modify? 'yes' or 'no'[yes]:

The configuration will take effect after saved and reset!

```

**Figure 4-20 Configure VOICE Interface Parameter**

The following items are displayed on this screen:

- ▶ **Enable:** Enable this WAN interface (DATA can't be disabled).
- ▶ **Type:** Select Static IP if your ISP has assigned a static IP address for your.
- ▶ **VLAN Enable:** Optional. Enable VLAN to configure VLAN ID and VLAN Priority Level.
- ▶ **VLAN ID:** Optional. VLAN ID of this WAN interface.
- ▶ **Priority Level:** Optional. VLAN Priority Level of this WAN interface.
- ▶ **Primary DNS:** Enter the IP address of your ISP's Primary DNS (Domain Name Server). If you are not clear, please consult your ISP. It's not allowed to access the Internet via domain name if the Primary DNS field is blank.
- ▶ **Secondary DNS:** Optional. If a Secondary DNS Server address is available, enter it.
- ▶ **IP Address:** Enter the IP address assigned by your ISP. If you are not clear, please consult your ISP.
- ▶ **Netmask:** Enter the Subnet Mask assigned by your ISP.
- ▶ **Gateway:** Optional. Enter the Gateway assigned by your ISP.

Input "3" to configure MGMT parameter as below:



```

BG9002N#set wan
->Please select one interface name to show<
1----DATA
2----VOICE
3----MGMT
4----OTHER1
5----OTHER2>[1]:3
->Enable or not[nol]:y
->LINK TYPE<0-STATIC IP,1-PPPOE,2-DHCP,3-PPTP,4-L2TP>[0]:2
->Vlan Enable[nol]:y
->VLAN ID<1-4095>[1]:3
->Priority Level<0-7>[0]:1
->Primary DNS[138.0.60.2]:
->Secondary DNS[138.1.60.1]:
->MTU<512-1508>[1500]:
->Specify Server Ip or not[nol]:y
->Server IP address[138.0.60.2]:
->Vendor Class Identifier or not[nol]:
->Manufacture name[:company1
->Device Class[:device2
->Device Type[:type3
->Device version[:version2
->Really want to modify? 'yes' or 'no'[yes]:

The configuration will take effect after saved and reset!

```

**Figure 4-21 Configure MGMT Interface Parameter**

The following items are displayed on this screen:

- ▶ **Enable:** Enable this WAN interface (DATA can't be disabled).
- ▶ **Type:** Select DHCP if your ISP assigns the IP address automatically.
- ▶ **VLAN Enable:** Optional. Enable VLAN to configure VLAN ID and VLAN Priority Level.
- ▶ **VLAN ID:** Optional. VLAN ID of this WAN interface.
- ▶ **Priority Level:** Optional. VLAN Priority Level of this WAN interface.
- ▶ **Primary DNS:** Enter the IP address of your ISP's Primary DNS (Domain Name Server) manually. If you are not clear, please consult your ISP. It's not allowed to access the Internet via domain name if the Primary DNS field is blank.
- ▶ **Secondary DNS:** Optional. If a Secondary DNS Server address is available, enter it.
- ▶ **Appoint Server IP:** Optional. If network has multiple DHCP servers, enter the IP address of your ISP'S DHCP server
- ▶ **Vendor Class Identifier:** Optional. This option (60) is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client.
- ▶ **Enterprise Code:** Optional.
- ▶ **Manufacture Name:** Optional.
- ▶ **Device Class:** Optional.
- ▶ **Device Type:** Optional.
- ▶ **Device Version:** Optional.

Input "4" to configure OTHER1 parameter as below:

```

BG9002N#set wan
->Please select one interface name to show<
1----DATA
2----VOICE
3----MGMT
4----OTHER1
5----OTHER2>[1]:4
->Enable or not[no]:y
->LINK TYPE<0-STATIC IP,1-PPPOE,2-DHCP,3-PPTP,4-L2TP>[0]:3
->The way of getting ip<0-STATIC IP,1-DHCP>[0]:1
->Vlan Enable[no]:y
->VLAN ID<1-4095>[1]:4
->Priority Level<0-7>[0]:
->Primary DNS[138.0.60.2]:
->Secondary DNS[138.1.60.1]:
->MTU<512-1508>[1500]:
->Specify Server Ip or not[no]:
->Vendor Class Identifier or not[no]:
->Manufacture name[]:
->Device Class[]:
->Device Type[]:
->Device version[]:
->Server IP[138.0.60.2]:
->PPTP Username[gkser]:
->PPTP Password[*****]:
->Enable Encryption or not[no]:
->Really want to modify? 'yes' or 'no'[yes]:

The configuration will take effect after saved and reset!

```

**Figure 4-22 Configure OTHER1 Interface Parameter**

The following items are displayed on this screen:

- ▶ **Enable:** Enable this WAN interface (DATA can't be disabled).
- ▶ **Type:** Select PPTP if your ISP provides a PPTP connection.
- ▶ **VLAN Enable:** Optional. Enable VLAN to configure VLAN ID and VLAN Priority Level.
- ▶ **VLAN ID:** Optional. VLAN ID of this WAN interface.
- ▶ **Priority Level:** Optional. VLAN Priority Level of this WAN interface.
- ▶ **Primary DNS:** Enter the IP address of your ISP's Primary DNS (Domain Name Server) manually. If you are not clear, please consult your ISP. It's not allowed to access the Internet via domain name if the Primary DNS field is blank.
- ▶ **Secondary DNS:** Optional. If a Secondary DNS Server address is available, enter it.
- ▶ **Server IP:** Enter the Server IP provided by your ISP.
- ▶ **Username:** Enter the Account Name provided by your ISP. If you are not clear, please consult your ISP.
- ▶ **Password:** Enter the Password provided by your ISP.
- ▶ **Enable Encryption:** Enable PPTP link encryption.

**Secondary Connection:** Here allow you to configure the secondary connection. DHCP and Static IP connection types are provided.

If **Static** is selected:

- ▶ **IP Address:** If Static IP is selected, configure the IP address of WAN port.
- ▶ **Netmask:** If Static IP is selected, configure the subnet mask of WAN port.

- **Gateway:** Optional. If Static IP is selected, configure the default gateway of WAN port.

If **DHCP** is selected:

- **Appoint Server IP:** Optional. If network has multiple DHCP servers, enter the IP address of your ISP's DHCP server.
- **Vendor Class Identifier:** Optional. This option (60) is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client.
- **Enterprise Code:** Optional.
- **Manufacture Name:** Optional.
- **Device Class:** Optional.
- **Device Type:** Optional.
- **Device Version:** Optional.

Input "5" to configure OTHER2 parameter as below:

```

BG9002N#set wan
->Please select one interface name to show<
1----DATA
2----VOICE
3----MGMT
4----OTHER1
5----OTHER2>[1]:5
->Enable or not[nol]:y
->LINK TYPE<0-STATIC IP,1-PPPOE,2-DHCP,3-PPTP,4-L2TP>[0]:4
->The way of getting ip<0-STATIC IP,1-DHCP,2-PPPOE>[0]:1
->Vlan Enable[nol]:y
->VLAN ID<1-4095>[1]:5
->Priority Level<0-7>[0]:
->Primary DNS[138.0.60.2]:
->Secondary DNS[138.1.60.1]:
->MTU<512-1500>[1500]:
->Specify Server Ip or not[nol]:y
->Server IP address[138.0.60.2]:
->Vendor Class Identifier or not[nol]:y
->Enterprise Code[0]:3
->Manufacture name[]:comany5
->Device Class[]:class5
->Device Type[]:type5
->Device version[]:version5
->Server IP[138.0.60.1]:
->L2TP username[gkser]:
->L2TP password[*****]:
->Really want to modify? 'yes' or 'no'[yes]:

The configuration will take effect after saved and reset!

```

**Figure 4-23 Configure OTHER2 Interface Parameter**

The following items are displayed on this screen:

- **Enable:** Enable this WAN interface (DATA can't be disabled).
- **Type:** Select L2TP if your ISP provides a L2TP connection.
- **VLAN Enable:** Optional. Enable VLAN to configure VLAN ID and VLAN Priority Level.
- **VLAN ID:** Optional. VLAN ID of this WAN interface.
- **Priority Level:** Optional. VLAN Priority Level of this WAN interface.
- **Primary DNS:** Enter the IP address of your ISP's Primary DNS (Domain Name Server). If

- you are not clear, please consult your ISP. It's not allowed to access the Internet via domain name if the Primary DNS field is blank.
- ▶ **Secondary DNS:** Optional. If a Secondary DNS Server address is available, enter it.
  - ▶ **Server IP:** Enter the Server IP provided by your ISP.
  - ▶ **Username:** Enter the Account Name provided by your ISP. If you are not clear, please consult your ISP.
  - ▶ **Password:** Enter the Password provided by your ISP.

**Secondary Connection:** Here allow you to configure the secondary connection. DHCP and Static IP connection types are provided.

If **Static** is selected:

- ▶ **IP Address:** If Static IP is selected, configure the IP address of WAN port.
- ▶ **Netmask:** If Static IP is selected, configure the subnet mask of WAN port.
- ▶ **Gateway:** Optional. If Static IP is selected, configure the default gateway of WAN port.

If **DHCP** is selected:

- ▶ **Appoint Server IP:** Optional. If network has multiple DHCP servers, enter the IP address of your ISP's DHCP server.
- ▶ **Vendor Class Identifier:** Optional. This option (60) is used by DHCP clients to optionally identify the vendor type and configuration of a DHCP client.
- ▶ **Enterprise Code:** Optional.
- ▶ **Manufacture Name:** Optional.
- ▶ **Device Class:** Optional.
- ▶ **Device Type:** Optional.
- ▶ **Device Version:** Optional.

#### 4.2.4 Lan Parameter

##### 4.2.4.1 Show Lan Parameter

The command "show lan" show the LAN configuration as below:

```
BG9002N#show lan

1----Static IP
2----Binding IP
3----Port Route/Bridge Mode
4----Advanced Parameters
Select the parameter to show[1]:
```

**Figure 4-24 Show LAN Parameter**

Input "1" to show LAN static IP configuration as below:

```

BG9002N#show lan

1----Static IP
2----Binding IP
3----Port Route/Bridge Mode
4----Advanced Parameters
Select the parameter to show[1]:

Interface Name.....:hello
IP Address.....:192.168.100.79
Netmask.....:255.255.255.0
Enable NAT or not.....:yes
Assign NAT IP or not.....:no
Enable DHCP Server or not.....:yes
Start IP.....:192.168.100.100
End IP.....:192.168.100.200
Netmask.....:255.255.255.0
Gateway.....:192.168.100.1
Primary DNS.....:192.168.100.1
Secondary DNS.....:192.168.100.1
Lease Time(Second).....:86400
Binding LAN Port.....:LAN2 LAN3 LAN4
Binding WAN Subinterface.....:DATA VOICE MGMT OTHER1 OTHER2

```

Figure 4-25 Show Static IP Parameter

Input "2" to show binding IP configuration as below:

```

BG9002N#show lan

1----Static IP
2----Binding IP
3----Port Route/Bridge Mode
4----Advanced Parameters
Select the parameter to show[1]:2
->Input the ID to show(0-0)[0]:

Interface Name.....:vlan2
IP Address.....:192.168.100.22
Netmask.....:255.255.255.0
Enable NAT or not.....:yes
Assign NAT IP or not.....:yes
NAT IP.....:192.168.100.111
Enable DHCP Server or not.....:yes
Start IP.....:192.168.100.23
End IP.....:192.168.100.30
Netmask.....:255.255.255.0
Gateway.....:192.168.100.26
Primary DNS.....:192.168.100.11
Secondary DNS.....:192.168.100.12
Lease Time(Second).....:36000
Binding LAN Port.....:LAN1 LAN2 LAN3 LAN4
Binding WAN Subinterface.....:DATA VOICE MGMT OTHER1 OTHER2
->Continue show or not[yes]:n

```

Figure 4-26 Show Binding IP Parameter

Input “3” to show port route/bridge mode as below:

```
BG9002N#show lan

1----Static IP
2----Binding IP
3----Port Route/Bridge Mode
4----Advanced Parameters
Select the parameter to show[1]:3
Lan Route/Bridge Mode:
LAN1.....:Route Mode
LAN2.....:Route Mode
LAN3.....:Route Mode
LAN4.....:Route Mode
```

Figure 4-27 Show Port Mode Parameter

Input “4” to show advanced parameters as below:

```
BG9002N#show lan

1----Static IP
2----Binding IP
3----Port Route/Bridge Mode
4----Advanced Parameters
Select the parameter to show[1]:4

LAN Isolate or not.....:no
Auto Bridge or not.....:yes
DHCP Vendor ID.....:albis sagem
STB Data Service IP Address.....:192.168.10.1
STB DATA Service Netmask.....:255.255.255.0
IPTV VLAN.....:8
IPTV PRI.....:4
STB Data VID Automatic or not.....:yes
```

Figure 4-28 Show Advanced Parameter

#### 4.2.4.2 Configure Lan Parameter

The command “set lan” configure the LAN parameter as below:

```
BG9002N#set lan

1----Static IP
2----Binding IP
3----Port Route/Bridge Mode
4----Advanced Parameters
Select the parameter to configure[1]:
```

Figure 4-29 Configure LAN Parameter

Input “1” to configure static IP as below:

```

BG9002N#set lan

1----Static IP
2----Binding IP
3----Port Route/Bridge Mode
4----Advanced Parameters
Select the parameter to configure[1]:
->Interface Name[hello]:
->IP Address[192.168.100.79]:
->Netmask[255.255.255.0]:
->Enable NAT or not[yes]:
->Assign NAT IP or not[no]:
->Enable DHCP Server or not[yes]:
->Start IP[192.168.100.100]:
->End IP[192.168.100.200]:
->Netmask[255.255.255.0]:
->Gateway[192.168.100.1]:
->Primary DNS[192.168.100.1]:
->Secondary DNS[192.168.100.1]:
->Lease Time(Second)[86400]:
Binding LAN Port:
->LAN1[no]:
->LAN2[yes]:
->LAN3[yes]:
->LAN4[yes]:
Binding WAN Subinterface:
->DATA[yes]:
->VOICE[yes]:
->MGMT[yes]:
->OTHER1[yes]:
->OTHER2[yes]:
->Really want to modify? 'yes' or 'no'[yes]:

Operate success!

```

**Figure 4-30 Configure Static IP Parameter**

The following items are displayed on this part.

- ▶ **Interface Name:** Name of this LAN interface.
- ▶ **IP Address:** Enter the IP address for this LAN interface.
- ▶ **Netmask:** Enter the subnet mask for this LAN interface.
- ▶ **NAT:** Optional Enable or disable NAT for this LAN interface
- ▶ **Assign NAT IP:** Optional If NAT is selected. NAT IP address can be assigned.
- ▶ **Enable DHCP Server:** Enable or disable DHCP server on this LAN interface.
- ▶ **Start IP:** If **Enable DHCP Server** is selected, enter the Start IP address to define a range for the DHCP server to assign dynamic IP addresses. This address should be in the same IP address subnet with the IP address of this LAN interface.
- ▶ **End IP:** If **Enable DHCP Server** is selected, enter the End IP address to define a range for the DHCP server to assign dynamic IP addresses. This address should be in the same IP address subnet with the IP address of this LAN interface.
- ▶ **Netmask:** If **Enable DHCP Server** is selected, enter the **Netmask** to define a range for the DHCP server to assign dynamic IP addresses.

- ▶ **Gateway:** Optional .If **Enable DHCP Server** is selected, enter the Gateway address to be assigned.
- ▶ **Primary DNS:** Optional. If **Enable DHCP Server** is selected, enter the Primary DNS server address to be assigned.
- ▶ **Secondary DNS:** Optional. If **Enable DHCP Server** is selected, enter the Secondary DNS server address to be assigned.
- ▶ **Lease Time(Second):** If **Enable DHCP Server** is selected, specify the length of time the DHCP server will reserve the IP address for each client. After the IP address expired, the client will be automatically assigned a new one.
- ▶ **Binding LAN Port:** Select the physical LAN port to bind the IP address of this LAN interface.
- ▶ **Binding WAN Subinterface:** Select the WAN subinterface which the packet from this LAN interface can be sending to.

Input “2” to configure binding IP as below:

```

BG9002N#set lan
1----Static IP
2----Binding IP
3----Port Route/Bridge Mode
4----Advanced Parameters
Select the parameter to configure[1]:
->Interface Name[hellol]:
->IP Address[192.168.100.79]:
->Netmask[255.255.255.0]:
->Enable NAT or not[yes]:
->Assign NAT IP or not[no]:
->Enable DHCP Server or not[yes]:
->Start IP[192.168.100.100]:
->End IP[192.168.100.200]:
->Netmask[255.255.255.0]:
->Gateway[192.168.100.1]:
->Primary DNS[192.168.100.1]:
->Secondary DNS[192.168.100.1]:
->Lease Time<Second>[86400]:
Binding LAN Port:
->LAN1[no]:
->LAN2[yes]:
->LAN3[yes]:
->LAN4[yes]:
Binding WAN Subinterface:
->DATA[yes]:
->VOICE[yes]:
->MGMT[yes]:
->OTHER1[yes]:
->OTHER2[yes]:
->Really want to modify? 'yes' or 'no'[yes]:

Operate success!

```

Figure 4-31 Configure Binding IP Parameter

Input “3” to configure port route/bridge mode as below:



```

BG9002N#set lan

1----Static IP
2----Binding IP
3----Port Route/Bridge Mode
4----Advanced Parameters
Select the parameter to configure[1]:3
Lan Route/Bridge Mode:

0----Route Mode
1----Transparent Bridge
2----Tagged Bridge
3----Promisc Bridge
->LAN1<0-3>[0]:
->LAN2<0-3>[0]:1
->LAN3<0-3>[0]:2
->VID<1-4095>[0]:7
->LAN4<0-3>[0]:3
->VID1[0]:8
->Continue Set Vid or not[yes]:
->VID2[0]:9
->Continue Set Vid or not[yes]:
->VID3[0]:10
->Continue Set Vid or not[yes]:
->VID4[0]:11
->Continue Set Vid or not[yes]:
->VID5[0]:12
->Continue Set Vid or not[yes]:n
->Really want to modify? 'yes' or 'no'[yes]:

Operate success!

```

**Figure 4-32 Configure Port Mode Parameter**

The following items are displayed on this part.

- ▶ **Port:** The physical LAN port name (LAN1~LAN4).
- ▶ **Route/Bridge:** Mode of this physical LAN port. The following four modes are provided:
  - Route:** route to WAN
  - Transparent bridge:** not modify the packets;
  - Tagged bridge:** LAN untagged, WAN tagged; only 1 VID supported
  - Promisc Mode:** Tagged packets in bridge mode, untagged packets in route mode; most 5 VIDs supported (e.g. 8, 10, 13).
- ▶ **VLAN ID List:** If Tagged bridge/Promisc Mode is selected, configure the VID/VIDs.

Input “4” to configure advanced parameters as below:

```

BG9002N#set lan

1----Static IP
2----Binding IP
3----Port Route/Bridge Mode
4----Advanced Parameters
Select the parameter to configure[1]:4
->LAN Isolate or not[no]:y
->Auto Bridge or not[yes]:
->DHCP Vendor ID1[albis]:
->DHCP Vendor ID2[albis]:
->STB Data Service IP Address[192.168.10.1]:
->STB DATA Service Netmask[255.255.255.0]:
->IPTV VLAN<1-4095>[8]:
->IPTV PRI<0-7>[4]:
->STB Data VID Automatic or not[yes]:
->Really want to modify? 'yes' or 'no'[yes]:

Operate success!

```

**Figure 4-33 Configure Advanced Parameter**

The following items are displayed on this part.

- ▶ **LAN Isolate:** Check the box to prohibit the access between LAN interfaces.
- ▶ **Auto Bridge:** Check the box to dynamically create IPTV bridge for STB.
- ▶ **DHCP Vendor ID:** Vendor class identifier List (DHCP 60 option), support at most two vendor IDs.
- ▶ **IPAddress:** IP address of interface for STB data service.
- ▶ **Netmask:** Subnet mask of interface for STB data service.
- ▶ **VID:** VID of IPTV VLAN.
- ▶ **PRI:** Priority level of IPTV VLAN.
- ▶ **Automatic:** Check the box to automatically detect the VID of STB data service.

## 4.2.5 WLAN

### 4.2.5.1 Show WLAN Parameter

The command “show wlan” show the WLAN configuration as below:

```

BG9002N#show wlan

1----Basic Settings
2----Security
3----Advanced Settings
4----Client Info
5----WPS
6----MAC Filtering
->Select the parameter to show[1]:

```

**Figure 4-34 Show WLAN Parameter**

Input “1” to show basic settings as below:

```

BG9002N#show wlan

1----Basic Settings
2----Security
3----Advanced Settings
4----Client Info
5----WPS
6----MAC Filtering
->Select the parameter to show[1]:1

Enable WiFi.....: Enable
Channel.....: 0
Wireless Mode.....: 11b/g/n

SSID1 Information:
Enable SSID.....: Enable
SSID Name.....: Gaoke-09AC88
Bind Interface.....: ULAN1
Enable Broadcast.....: Enable
Isolated.....: Disable
LAN Isolated.....: Disable
Max Client.....: 32

SSID2 Information:
Enable SSID.....: Disable

SSID3 Information:
Enable SSID.....: Disable

SSID4 Information:
Enable SSID.....: Disable
BG9002N#

```

Figure 4-35 Show Basic Settings

Input "2" to show security configuration as below:

```

BG9002N#show wlan

1----Basic Settings
2----Security
3----Advanced Settings
4----Client Info
5----WPS
6----MAC Filtering
->Select the parameter to show[1]:2
->Select the SSID to set<0-3>[0]:

Authentication.....: WPAPSKWPA2PSK
Algorithm.....: AES
Renew interval.....: 3600
WPA Pre-Shared Key.....: *****
->Continue or not?<yes/no>[yes]:y
->Select the SSID to set<0-3>[0]: 1

The SSID is not enable!!!
BG9002N#

```

Figure 4-36 Show Security Parameter

Input "3" to show advanced settings as below:

```
BG9002N#show wlan

1----Basic Settings
2----Security
3----Advanced Settings
4----Client Info
5----WPS
6----MAC Filtering
->Select the parameter to show[1]:3

Fragmentation Threshold.....: 2346
RTS Threshold.....: 2347
Transmit Power.....: 100
Enable WMM.....: Enable
BG9002N#
```

Figure 4-37 Show Advanced Settings

Input "4" to show client information as below:

```
BG9002N#show wl

BG9002N#show wlan

1----Basic Settings
2----Security
3----Advanced Settings
4----Client Info
5----WPS
6----MAC Filtering
->Select the parameter to show[1]:4
No client information!!!

BG9002N#
```

Figure 4-38 Show Client Information

Input "5" to show WPS configuration as below:

```
BG9002N#show wlan

1----Basic Settings
2----Security
3----Advanced Settings
4----Client Info
5----WPS
6----MAC Filtering
->Select the parameter to show[1]:5

Enable WPS.....:yes
BG9002N#
```

Figure 4-39 Show WPS Parameter

Input "6" to show MAC filtering configuration as below:

```
BG9002N#show wlan

1---Basic Settings
2---Security
3---Advanced Settings
4---Client Info
5---WPS
6---MAC Filtering
->Select the parameter to show[1]:6

Enable MAC Filter.....: Enable
Filtering Rules.....: Deny
+---+-----+
! No !      MAC      !
+---+-----+
!0  !12:45:90:87:90:34 !
+---+-----+

BG9002N#
```

Figure 4-40 Show MAC Filtering Parameter

#### 4.2.5.2 Configure WLAN Parameter

The command “set wlan” configure the WLAN parameter as below:

```
BG9002N#set wlan

1---Basic Settings
2---Security
3---Advanced Settings
4---WPS
5---MAC Filtering
->Select the parameter to configure[1]:
```

Figure 4-41 Configure WLAN Parameter

Input “1” to configure basic settings as below:

```

BG9002N#set wlan

1----Basic Settings
2----Security
3----Advanced Settings
4----WPS
5----MAC Filtering
->Select the parameter to configure[1]:
->Enable WiFi? 'yes' or 'no'[yes]:
->Channel<0-13,0-AutoSelect>[0]:
->Wireless Mode<0-11b/g,1-11b,2-11g,3-11b/g/n,4-11n>[3]:
->Channel Width<0-20MHz,1-20/40MHz>[1]:
Config SSID1:
->SSID Name[Gaoke-09AC88]:
->Bind Interface<[0]WAN [5]LAN1>[5]:
->Enable Broadcast? 'yes' or 'no'[no]:
->Isolated? 'yes' or 'no'[no]:
->LAN Isolated? 'yes' or 'no'[no]:
->Max Client<0~255>[32]:
Config SSID2:
->Enable SSID? 'yes' or 'no'[no]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

**Figure 4-42** Configure Basic Settings

The following items are displayed on this part.

- ▶ **Enable WiFi:** Enable or disable the WIFI AP function globally.
- ▶ **Channel:** This field determines which operating frequency will be used. The default channel is set to **AutoSelect**, so the AP will choose the best channel automatically. It is not necessary to change the wireless channel unless you notice interference problems with another nearby access point.
- ▶ **Wireless Mode:** Select the desired mode.
  - 11b:** Select if all of your wireless clients are 802.11b.
  - 11g:** Select if all of your wireless clients are 802.11g.
  - 11n:** Select only if all of your wireless clients are 802.11n.
  - 11b/g:** Select if you are using both 802.11b and 802.11g wireless clients.
  - 11b/g/n:** Select if you are using a mix of 802.11b, 11g and 11n wireless clients.
- ▶ **Channel Width:** Select any channel width from the drop-down list. The default setting is automatic, which can automatically adjust the channel width for your clients. If you choose to **11n** or **11b/g/n** Wireless mode, this configuration is required. Two values of width are provided: **20MHz** and **20/40MHz**.

The **Service Set Identifier (SSID)** is used to identify an 802.11 (Wi-Fi) network and it's discovered by network sniffing/scanning. GIGAROUTER UF72N provides up to four SSID.

- ▶ **Enable SSID:** Enable or disable this entry of SSID. SSID1 can't be disabled.
- ▶ **SSID Name:** Enter the name of SSID. The name of SSID must be unique in all wireless networks nearby.
- ▶ **Bind Interface:** Select a network interface to be bridged to the SSID.
- ▶ **Enable Broadcast:** When wireless clients survey the local area for wireless networks to associate with, they will detect the SSID broadcast by the device. If you select the **Enable Broadcast** checkbox, the device will broadcast its name (SSID) on

the air.

- ▶ **Isolated:** Enable or disable isolate different clients from the same wireless station.
- ▶ **LAN Isolated:** Enable or disable isolation between the LAN and SSID.
- ▶ **Max Client:** Enter the maximum number of clients allowed to connect to the SSID.
- ▶ **SSID AP Isolated:** This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

Input “2” to configure security parameter as below:

```

BG9002N#set wlan

1----Basic Settings
2----Security
3----Advanced Settings
4----WPS
5----MAC Filtering
->Select the parameter to configure[1]:2
->Select the SSID to set(0-3)[0]:

0----Disable
1----OPEN WEP
2----WPA2PSK
3----WPA2PSK
4----WPA2PSK
5----WPA
6----WPA2
7----WPA1WPA2
8----SHARE
9----WEPAUTO
->Authentication[4]:
->Algorithm(0-TKIP,1-AES,2-TKIP/AES)[1]:
->Renew interval(0-2592000)[3600]:
->WAP Pre-Shared Key(length:8-63)[*****]:
->Continue or not?(yes/no)[yes]:n
->Really want to modify? 'yes' or 'no'[yes]:y

Oprate success!

BG9002N#_

```

**Figure 4-43** Configure Security Parameter

The following items are displayed on this part.

- ▶ **SSID:** The SSID enabled in **WLAN**→**Basic Settings** page.Read only
- ▶ **Authentication:** The authentication type selected: WPA-PSK, WPA2-PSK, WPAPSK/WPA2PSK.
- ▶ **Algorithm:** When WPA2-PSK or WPAPSK/WPA2PSK is set as the Authentication Type, you can select either **TKIP**, or **AES** or **TKIP/AES** as Encryption. When WPA-PSK is set as the Authentication Type, you can select either TKIP or AES as Encryption.
- ▶ **WPA Pre-Shared Key:** You can enter ASCII characters between 8 and 64 characters.
- ▶ **Renew Interval:** Specify the group key update interval in seconds. Enter 0 to disable the update.

Input “3” to configure advanced settings as below:

```

BG9002N#set wlan

1----Basic Settings
2----Security
3----Advanced Settings
4----WPS
5----MAC Filtering
->Select the parameter to configure[1]:3
->Fragmentation Threshold<256~2346>[2346]:
->RTS Threshold<256~2347>[2347]:
->Transmit Power<1~100>[100]:
->Enable WMM? 'yes' or 'no'[yes]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

**Figure 4-44** Configure Advanced Settings

The following items are displayed on this part.

- ▶ **Fragmentation Threshold:** This value is the maximum size determining whether packets will be fragmented. Setting the Fragmentation Threshold too low may result in poor network performance since excessive packets. 2346 is the default setting and is recommended.
- ▶ **RTS Threshold:** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the device will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2347.
- ▶ **Transmit Power:** Here you can specify the transmit power of device. 100 is the default setting and is recommended.
- ▶ **Enable WMM:** Enable or disable the WIFI WMM function globally. WMM function can guarantee the packets with high-priority messages, being transmitted preferentially. It is strongly recommended enabled.

Input "4" to configure WPS parameter as below:

```

BG9002N#set wlan

1----Basic Settings
2----Security
3----Advanced Settings
4----WPS
5----MAC Filtering
->Select the parameter to configure[1]:4
->Enable WPS<yes/no>[yes]
->WPS mode :< 0-quit; 1 - PIN ; 2 - PBC >[1]:
->Enter the PIN code: 123456
->Really want to modify? 'yes' or 'no'[yes]:

Oprate success!

BG9002N#

```

**Figure 4-45** Configure WPS Parameter

The following items are displayed on this part.

- ▶ **Enable WPS:** Enable or disable the WIFI WPS function globally.



Input "4" to configure MAC filtering parameter as below:

```

BG9002N#set wlan

1---Basic Settings
2---Security
3---Advanced Settings
4---WPS
5---MAC Filtering
->Select the parameter to configure[1]:5
WLAN MAC Filter Config:
->0-Rule,1-List[0]: 0
->Enable MAC Filter? 'yes' or 'no'[yes]:
->Filtering Rules(0-Allow,1-Deny)[0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

```

BG9002N#set wlan

1---Basic Settings
2---Security
3---Advanced Settings
4---WPS
5---MAC Filtering
->Select the parameter to configure[1]:5
WLAN MAC Filter Config:
->0-Rule,1-List[0]: 1
WLAN MAC Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->MAC[1]:15:41:66:88:ac:f8
The configuration will take effect after saved and reset!
BG9002N#

```

```

BG9002N#set wlan

1---Basic Settings
2---Security
3---Advanced Settings
4---WPS
5---MAC Filtering
->Select the parameter to configure[1]:5
WLAN MAC Filter Config:
->0-Rule,1-List[0]: 1
WLAN MAC Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+-----+-----+
| No |          MAC          |
+-----+-----+
| 0  | af:16:80:41:43:99    |
+-----+-----+
| 1  | 15:41:66:88:ac:f8    |
+-----+-----+
->Please input number which you will modify[0-1]:1
->MAC[15:41:66:88:ac:f8]:a2:35:68:41:12:43
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

```

BG9002N#set wlan

1----Basic Settings
2----Security
3----Advanced Settings
4----WPS
5----MAC Filtering
->Select the parameter to configure[1]:5
WLAN MAC Filter Config:
->0-Rule,1-List[0]: 1
WLAN MAC Filter List Config:
->Select config type<0-add,1-del,2-modify>[0]: 1
+-----+-----+
| No |      MAC      |
+-----+-----+
| 0 | af:16:80:41:43:99 |
+-----+-----+
| 1 | a2:35:68:41:12:43 |
+-----+-----+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

**Figure 4-46** Configure MAC Filtering Parameter

The following items are displayed on this part.

- **Enable MAC Filter:** Enable or disable the Wifi MAC filtering function globally.
- **Filtering Rules:** Two MAC filtering rules are provided:
  - Allow:** allow the stations specified by entries in the list to access.
  - Deny:** deny the stations specified by entries in the list to access.

## 4.3 Data Service

### 4.3.1 DHCP Server

#### 4.3.1.1 Static Address Assign

The command “show dhcp-server static-ip-assign” shows the static IP assign information as bellow:

```

BG9002N#show dhcp-server static-ip-assign
+-----+-----+-----+-----+-----+
|No|IP|Netmask|MAC|Description|
+-----+-----+-----+-----+-----+
|0|192.168.0.30|255.255.255.0|11:a2:3c:33:67:85|
+-----+-----+-----+-----+-----+

BG9002N#

```

**Figure 4-47** Show Static IP Assign Information

The command “set dhcp-server static-ip-assign” configures the static IP assign information as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```

BG9002N#set dhcp-server static-ip-assign
Static Ip Assign List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->IP[1]: 192.168.12.56
->Netmask[1]: 255.255.255.0
->MAC[00:00:00:00:00:00]: 14:34:86:99:a6:06
->Description[1]:static
The configuration will take effect after saved and reset!
BG9002N#

```

```

BG9002N#set dhcp-server static-ip-assign
Static Ip Assign List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2

+-----+-----+-----+-----+-----+
|No|IP|Netmask|MAC|Description|
+-----+-----+-----+-----+-----+
|0|192.168.0.30|255.255.255.0|11:a2:3c:33:67:85|
+-----+-----+-----+-----+-----+
|1|192.168.12.56|255.255.255.0|14:34:86:99:a6:06|static|
+-----+-----+-----+-----+-----+

->Please input number which you will modify[0-1]:1
->IP[192.168.12.56]:
->Netmask[255.255.255.0]:
->MAC[14:34:86:99:a6:06]:
->Description[static]:dhcp
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

```

BG9002N#set dhcp-server static-ip-assign
Static Ip Assign List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1

+-----+-----+-----+-----+-----+
|No|IP|Netmask|MAC|Description|
+-----+-----+-----+-----+-----+
|0|192.168.0.30|255.255.255.0|11:a2:3c:33:67:85|
+-----+-----+-----+-----+-----+
|1|192.168.12.56|255.255.255.0|14:34:86:99:a6:06|dhcp|
+-----+-----+-----+-----+-----+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

**Figure 4-48 Configure Static IP Assign**

The command will configure static ip assign.

The following items are displayed on this screen:

- ▶ **IP :** The IP address reserved.
- ▶ **Mask:** The subnet mask of IP address reserved.
- ▶ **MAC:** The MAC address you want to reserve IP address.

### 4.3.1.2 DHCP Relay

The command “show dhcp-relay” shows the DHCP relay information as below:

```
BG9002N#show dhcp-relay
->Enable DHCP Relay.....: Enable
->Client Interface 1.....: none
->Client Interface 2.....: ULAN1
->Client Interface 3.....: none
->Client Interface 4.....: VOICE
->Server Interface.....: DATA
->Server IP.....: 138.0.60.2
BG9002N#
```

Figure 4-49 Show DHCP Relay Information

The command “set dhcp-relay” configures the DHCP relay information as below:

```
BG9002N#set dhcp-relay
->Enable DHCP Relay? 'yes' or 'no' [yes]:
->Client Interface 1<[0]DATA [1]VOICE [5]ULAN1 [255]none>[255]:
->Client Interface 2<[0]DATA [1]VOICE [5]ULAN1 [255]none>[5]:
->Client Interface 3<[0]DATA [1]VOICE [5]ULAN1 [255]none>[255]:
->Client Interface 4<[0]DATA [1]VOICE [5]ULAN1 [255]none>[1]:
->Server Interface<[0]DATA [1]VOICE [5]ULAN1 [255]none>[0]:
->Server IP[138.0.60.2]:
Really want to modify? 'yes' or 'no' [yes]:
The configuration will take effect after saved and reset!
BG9002N#
```

Figure 4-50 Set DHCP Relay Information

The following items are displayed on this screen:

- ▶ **Enable DHCP Relay:** Enable or disable DHCP Relay.
- ▶ **Client Interface:** The interface to listen for DHCP client requests. Up to four interfaces can be selected.
- ▶ **Server Interface:** Choose the interface which connects DHCP server.
- ▶ **Server IP:** Configure the DHCP server IP address.

## 4.3.2 NAT Config

### 4.3.2.1 Basic Settings

The command “show nat” shows the NAT basic settings as below:

```
BG9002N#show nat
Max Nat Connections.....: 16000
Enable MSS Auto Adaptive.....: Disable
TCP MSS.....: 1260
BG9002N#
```

Figure 4-51 Show NAT Basic Settings

The command “set nat” configures the NAT basic settings as below:

```

BG9002N#set nat
->Max Nat Connections<512-16000>[16000]:
->Enable MSS Auto Adaptive 'yes' or 'no' [yes]:n
->TCP MSS<1260-1460>[1260]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

**Figure 4-52 Configure NAT Basic Settings**

The following items are displayed on this screen:

- ▶ **Max Nat Connections:** Specify the maximum number of NAT connections.
- ▶ **Enable MSS Auto Adaptive:** Enable or disable auto adaptive the value of MSS (Maximum Segment Size).
- ▶ **TCP MSS:** If **Enable MSS Auto Adaptive** is not selected, configure this to specify the maximum segment size of the TCP protocol.

#### 4.3.2.2 PAT Settings

The command “show pat” shows the PAT information as below:

```

BG9002N#show pat

  Enable PAT.....: Enable

+---+---+---+---+---+---+---+---+---+---+---+---+
| No | Enable | Inter_Iface | Inter_Port | Protocol | Intra_IP | Intra_Port |
+---+---+---+---+---+---+---+---+---+---+---+---+
| 0  | Enable | DATA      | 1000      | TCP      | 192.168.12.66 | 2000      |
+---+---+---+---+---+---+---+---+---+---+---+---+

BG9002N#

```

**Figure 4-53 Show PAT Information**

The command “set pat” configures the PAT parameters as below:

```

BG9002N#set pat
->Enable PAT? 'yes' or 'no'[yes]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#_

```

**Figure 4-54 Configure PAT Parameters**

The following items are displayed on this screen:

- ▶ **Enable PAT:** Enable or disable PAT globally.

The command “set pat rule” configures the PAT rule as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify .If you want to delete the entry, enter 1 and choose the corresponding entry.



```

BG9002N#set pat rule
Pat Regular List Config:
->Select config type<0-add,1-del,2-modify>[0]:
->Enable the PAT rule? 'yes' or 'no'[yes]:y
->Protocol Type<0-TCP, 1-UDP>[0]:1
->Internet Port<0-65535>[1000]:
->Intranet IP[1]:192.168.2.66
->Intranet Port<0-65535>[1000]:6000
->Internet Interface:'[0]DATA [1]VOICE'[0]:
The configuration will take effect after saved and reset!
BG9002N#

```

```

BG9002N#set pat rule
Pat Regular List Config:
->Select config type<0-add,1-del,2-modify>[0]: 2
+-----+-----+-----+-----+-----+-----+-----+
| No | Enable | Inter_Iface | Inter_Port | Protocol | Intra_IP | Intra_Port |
+-----+-----+-----+-----+-----+-----+-----+
| 0 | Enable | DATA      | 1000      | TCP      | 192.168.12.66 | 2000      |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | Enable | DATA      | 1000      | UDP      | 192.168.2.66  | 6000      |
+-----+-----+-----+-----+-----+-----+-----+
->Please input number which you will modify[0-1]:1
->Enable the PAT rule? 'yes' or 'no'[yes]:
->Protocol Type<0-TCP, 1-UDP>[1]:
->Internet Port<0-65535>[1000]:5000
->Intranet IP[192.168.2.66]:
->Intranet Port<0-65535>[6000]:
->Internet Interface:'[0]DATA [1]VOICE'[0]:
->Really want to modify? 'yes' or 'no'[yes]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#_

```

```

BG9002N#
BG9002N#set pat rule
Pat Regular List Config:
->Select config type<0-add,1-del,2-modify>[0]: 1
+-----+-----+-----+-----+-----+-----+-----+
| No | Enable | Inter_Iface | Inter_Port | Protocol | Intra_IP | Intra_Port |
+-----+-----+-----+-----+-----+-----+-----+
| 0 | Enable | DATA      | 1000      | TCP      | 192.168.12.66 | 2000      |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | Enable | DATA      | 5000      | UDP      | 192.168.2.66  | 6000      |
+-----+-----+-----+-----+-----+-----+-----+
->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#_

```

**Figure 4-55 Configure PAT Rule**

The following items are displayed on this screen:

- ▶ **Enable:** Enable or disable this PAT entry.
- ▶ **Internet Port:** Enter the service port provided for accessing external network. All the requests from internet to this service port will be redirected to the specified server in local

- network.
- **Intranet Port:** Specify the service port of the LAN host as virtual server.
  - **Intranet IP:** Enter the IP address of the specified internal server for the entry. All the requests from the internet to the specified LAN port will be redirected to this host.
  - **Protocol:** Specify the protocol used for the entry.
  - **Internet Interface:** Specify the interface to receive requests from the internet for the entry.

#### 4.3.2.3 DMZ Settings

The command “show dmz” shows the DMZ information as below:

```

BG9002N#show dmz

Enable DMZ.....: Enable

+---+-----+-----+
| No | Public IP | Private IP |
+---+-----+-----+
| 0  | 138.1.61.2 | 192.168.12.54 |
+---+-----+-----+

BG9002N#

```

Figure 4-56 Show DMZ Information

The command “set dmz ” configures the DMZ Parameters as below:

```

BG9002N#set dmz
->Enable DMZ? 'yes' or 'no'[yes]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

Figure 4-57 Configure DMZ Parameters

The following items are displayed on this screen:

- **Enable DMZ:** Enable or disable DMZ globally.

The command “set dmz rule” configures the DMZ rule as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```

BG9002N#set dmz rule
DMZ Regular List Config:
->Select config type<0-add,1-del,2-modify>[0]:
->Public IP[1]:192.15.26.3
->Private IP[1]:172.56.5.69
The configuration will take effect after saved and reset!
BG9002N#

```

```

BG9002N#set dmz rule
DMZ Regular List Config:
->Select config type<0-add,1-del,2-modify>[0]: 2
+-----+-----+-----+
| No |   Public IP   |   Private IP   |
+-----+-----+-----+
| 0  | 138.1.61.2    | 192.168.12.54  |
+-----+-----+-----+
| 1  | 192.15.26.3   | 172.56.5.69    |
+-----+-----+-----+
->Please input number which you will modify[0-1]:1
->Public IP[192.15.26.3]:
->Private IP[172.56.5.69]:172.66.6.6
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

```

BG9002N#set dmz rule
DMZ Regular List Config:
->Select config type<0-add,1-del,2-modify>[0]: 1
+-----+-----+-----+
| No |   Public IP   |   Private IP   |
+-----+-----+-----+
| 0  | 138.1.61.2    | 192.168.12.54  |
+-----+-----+-----+
| 1  | 192.15.26.3   | 172.66.6.6     |
+-----+-----+-----+
->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

Figure 4-58 Configure DMZ Rule

The following items are displayed on this screen:

- **Public IP:** The public IP address for this DMZ entry.
- **Private IP:** The private IP address for this DMZ entry.

#### 4.3.2.4 ALG Settings

The command “show alg” shows the ALG information as below:

```

BG9002N#show alg
Enable SIP ALG.....: Disable
Enable H323 ALG.....: Enable
Enable FTP ALG.....: Enable
Enable RTSP ALG.....: Enable
RTSP Server Port.....: 554
Enable PPTP ALG.....: Enable
BG9002N#

```

Figure 4-59 Show ALG Information

The command “set alg” configures the ALG parameters as below:



```
BG9002N#set alg
->Enable SIP ALG? 'yes' or 'no' [no]:
->Enable H323 ALG? 'yes' or 'no' [yes]:
->Enable FTP ALG? 'yes' or 'no' [yes]:
->Enable RTSP ALG? 'yes' or 'no' [yes]:
->RTSP Server Port(1~65535)[554]:
->Enable PPTP ALG? 'yes' or 'no' [yes]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#
```

**Figure 4-60 Configure ALG Parameters**

The following items are displayed on this screen:

- ▶ **Enable SIP:** Enable or disable SIP ALG.
- ▶ **Enable H323:** Allow Microsoft NetMeeting clients to communicate across NAT if selected.
- ▶ **Enable FTP:** Allow FTP clients and servers to transfer data across NAT if selected.
- ▶ **Enable PPTP:** Enable or disable PPTP ALG.
- ▶ **Enable RTSP:** Enable or disable RTSP ALG.

### 4.3.3 Firewall Config

#### 4.3.3.1 Attack Defense

The command “show attack-defense” shows the attack defense information as below:

```
BG9002N#show attack-defense
Enable Broadcast Storm Defense.....: Disable
Enable Block Ping.....: Disable
Enable TCP SYN Flood Defense.....: Enable
Max Limit(packets/second).....: 20
Enable UDP Flood Defense.....: Disable
Enable ICMP Defense.....: Enable
Max Limit(packets/second).....: 10
Enable ARP Attack Defense.....: Disable
Enable Port Scan Defense.....: Disable
Enable Land Based Defense.....: Disable
Enable Ping Of Death Defense.....: Disable
Enable Teardrop Defense.....: Disable
Enable Fraggle Defense.....: Disable
Enable Smurf Defense.....: Disable
BG9002N#
```

**Figure 4-61 Show Attack Defense Information**

The command “set attack-defense” configures the attack defense parameters as below:

```

BG9002N#set attack-defense
->Enable Broadcast Storm Defense? 'yes' or 'no' [no]:
->Enable Block Ping? 'yes' or 'no' [no]:
->Enable TCP SYN Flood Defense? 'yes' or 'no' [yes]:
->Max Limit(packets/second)(1~1000)[10]:
->Enable UDP Flood Defense? 'yes' or 'no' [no]:
->Enable ICMP Defense? 'yes' or 'no' [yes]:
->Max Limit(packets/second)(1~1000)[10]:
->Enable ARP Attack Defense? 'yes' or 'no' [no]:
->Enable Port Scan Defense? 'yes' or 'no' [no]:
->Enable Land Based Defense? 'yes' or 'no' [no]:
->Enable Ping Of Death Defense? 'yes' or 'no' [no]:
->Enable Teardrop Defense? 'yes' or 'no' [no]:
->Enable Fraggle Defense? 'yes' or 'no' [no]:
->Enable Smurf Defense? 'yes' or 'no' [no]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

**Figure 4-62 Configure Attack Defense Parameters**

The following items are displayed on this screen:

- ▶ **Enable Broadcast Storm Defense:** Enable or disable **Broadcast Storm Defense**.
- ▶ **Enable Block Ping:** Enable or disable **Block Ping** function.
- ▶ **Enable TCP SYN Flood Defense:** Enable or disable **TCP SYN Flood Defense**.
- ▶ **Enable UDP Flood Defense:** Enable or disable **UDP Flood Defense**.
- ▶ **Enable ICMP Defense:** Enable or disable **ICMP Defense**.
- ▶ **Enable ARP Attack Defense:** Enable or disable **ARP Attack Defense**.
- ▶ **Enable Port Scan Defense:** A port scanner is a software application designed to probe a server or host for open ports. Check the box to prevent port scanning.
- ▶ **Enable Land Based Defense:** The Land Denial of Service attack works by sending a spoofed packet with the SYN flag - used in a "handshake" between a client and a host - set from a host to any port that is open and listening. If the packet is programmed to have the same destination and source IP address, when it is sent to a machine, via IP spoofing, the transmission can fool the machine into thinking it is sending itself a message, which, depending on the operating system, will crash the machine. Check the box to enable **Land Based Defense**.
- ▶ **Enable Ping Of Death Defense:** Ping of death is a denial of service (DoS) attack caused by an attacker deliberately sending an IP packet larger than the 65,536 bytes allowed by the IP protocol. Check the box to enable **Ping of Death Defense**.
- ▶ **Enable Teardrop Defense:** Teardrop is a program that sends IP fragments to a machine connected to the Internet or a network. Check the box to enable **Teardrop Defense**.
- ▶ **Enable Fraggle Defense:** A fraggle attack is a variation of a Smurf attack where an attacker sends a large amount of UDP traffic to ports 7 (echo) and 19 (chargen) to an IP Broadcast Address, with the intended victim's spoofed source IP address. Check the box to enable **Fraggle Defense**.

### ► Enable Smurf Defense:

The Smurf Attack is a denial-of-service attack in which large numbers of Internet Control Message Protocol (ICMP) packets with the intended victim's spoofed source IP are broadcast to a computer network using an IP Broadcast address. Check the box to enable **Smurf Defense**.

#### 4.3.3.2 Service Type

The command "show service-type" shows the service type information as below:

```
BG9002N#show service-type
+-----+-----+-----+-----+
| No | Name | Protocol | Port Range |
+-----+-----+-----+-----+
| 0 | 123 | UDP | 1-65535 |
+-----+-----+-----+-----+

BG9002N#
```

Figure 4-63 Show Service Type Information

The command "set service-type" configures the service type as below. Enter 0 add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set service-type
Service Type List Config:
->Select Config type<0-add,1-del,2-modify>[0]: 0
->Name[]:asdf
->Protocol<0-UDP,1-TCP,2-ICMP,3-ALL>[0]: 1
->Port<Start Port><0-65535>[0]: 1000
->Port<End Port><0-65535>[0]: 2000
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set service-type
Service Type List Config:
->Select Config type<0-add,1-del,2-modify>[0]: 2
+-----+-----+-----+-----+
| No | Name | Protocol | Port Range |
+-----+-----+-----+-----+
| 0 | 123 | UDP | 1-65535 |
+-----+-----+-----+-----+
| 1 | asdf | TCP | 1000-2000 |
+-----+-----+-----+-----+
->Please input number which you will modify[0-1]:0
->Name[123]:1234
->Protocol<0-UDP,1-TCP,2-ICMP,3-ALL>[0]:
->Port<Start Port><0-65535>[1]:
->Port<End Port><0-65535>[65535]:
Really want to modify? 'yes' or 'no'[yes]:y
The configuration will take effect after saved and reloaded!
```

```

BG9002N#set service-type
Service Type List Config:
->Select config type<0-add,1-del,2-modify>[0]: 1
+-----+-----+-----+-----+
| No |      Name      | Protocol | Port Range |
+-----+-----+-----+-----+
| 0  | 123            | UDP      | 1-65535    |
+-----+-----+-----+-----+
| 1  | asdf           | TCP      | 1000-2000   |
+-----+-----+-----+-----+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

**Figure 4-64 Configure Service Type**

The following items are displayed on this screen:

- ▶ **Name:** Name of this entry, it will be list in Internet Access-Ctrl page.
- ▶ **Protocol:** Select the protocol for this entry. Four types are provided: TCP, UDP, ICMP and ALL.
- ▶ **Port Range:** Configure the port range for this entry.

#### 4.3.3.3 Internet Access-Ctrl

##### 4.3.3.3.1 Access Control

The command “show access-control” shows the access control information as below:

```

BG9002N#show access-control

Enable Access Control.....: Enable
Policy.....: Allow

+---+-----+-----+-----+-----+
| No | Enable |      Src IP Range      | Service Name |
+---+-----+-----+-----+-----+
| 0  | Enable | 192.168.1.3-192.168.2.6 | 123          |
+---+-----+-----+-----+-----+

->Enter the index to show(0-0)[0]:
Enable Rule.....:Enable
Service Name.....:123
Source IP<Start IP>.....:192.168.1.3
Source IP<End IP>.....:192.168.2.6
Destination IP<Start IP>.....:210.66.31.61
Destination IP<End IP>.....:210.66.55.99
Active Time<Start Time>.....:00:00
Active Time<End Time>.....:23:59
Active Monday.....:Disable
Active Tuesday.....:Disable
Active Wednesday.....:Disable
Active Thursday.....:Disable
Active Friday.....:Disable
Active Saturday.....:Disable
Active Sunday.....:Disable

->Show access control rule detail para continue or not?[yes]:n
BG9002N#

```

Figure 4-65 Show Access Control Information

The command “set access-control” configures the access control policy as below:

```

BG9002N#set access-control
->Enable Access Control? 'yes' or 'no'[yes]:
->Policy(0-Allow,1-Deny)[0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded?

BG9002N#

```

Figure 4-66 Configure Access Control

The following items are displayed on this screen:

- ▶ **Enable Access Control:** Enable or disable access control from WAN.
- ▶ **Policy:** Default policy of access control: **Allow** or **Deny**. If Allow is selected, all packets will be allowed except the entries list on this page. If Deny is selected, all packets will be denied except the entries list on this page.

The command “set access-control rule” configures the access control rule as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.



```

BG9002N#set access-control rule
Access Control Rule List Config:
->Select config type<0-add,1-del,2-modify>[0]:
->Enable Rule? 'yes' or 'no'[no]:y
->Source IP<Start IP>[1:192.168.5.6
->Source IP<End IP>[1:192.168.5.90
->Destination IP<Start IP>[1:139.0.1.6
->Destination IP<End IP>[1:139.0.1.66
->Service Name<0-123,255-NULL>[0]:
->Active Time<Start Time>[00:00]:
->Active Time<End Time>[00:00]:23:00
->Active Monday? 'yes' or 'no'[no]:y
->Active Tuesday? 'yes' or 'no'[no]:y
->Active Wednesday? 'yes' or 'no'[no]:
->Active Thursday? 'yes' or 'no'[no]:
->Active Friday? 'yes' or 'no'[no]:
->Active Saturday? 'yes' or 'no'[no]:
->Active Sunday? 'yes' or 'no'[no]:
The configuration will take effect after saved and reloaded!

```

```

BG9002N#set access-control rule
Access Control Rule List Config:
->Select config type<0-add,1-del,2-modify>[0]: 2
+-----+-----+-----+-----+
| No | Enable | Src IP Range | Service Name |
+-----+-----+-----+-----+
| 0 | Enable | 192.168.1.3-192.168.2.6 | 123 |
+-----+-----+-----+-----+
| 1 | Enable | 192.168.5.6-192.168.5.90 | 123 |
+-----+-----+-----+-----+
->Please input number which you will modify[0-1]:1
->Enable Rule? 'yes' or 'no'[yes]:
->Source IP<Start IP>[192.168.5.6]:
->Source IP<End IP>[192.168.5.90]:
->Destination IP<Start IP>[139.0.1.6]:
->Destination IP<End IP>[139.0.1.66]:
->Service Name<0-123,255-NULL>[0]:
->Active Time<Start Time>[00:00]:
->Active Time<End Time>[23:00]:
->Active Monday? 'yes' or 'no'[yes]:
->Active Tuesday? 'yes' or 'no'[yes]:
->Active Wednesday? 'yes' or 'no'[no]:y
->Active Thursday? 'yes' or 'no'[no]:y
->Active Friday? 'yes' or 'no'[no]:
->Active Saturday? 'yes' or 'no'[no]:
->Active Sunday? 'yes' or 'no'[no]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

```

```

BG9002N#set access-control rule
Access Control Rule List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+-----+-----+-----+-----+
| No | Enable | Src IP Range | Service Name |
+-----+-----+-----+-----+
| 0 | Enable | 192.168.1.3-192.168.2.6 | 123 |
+-----+-----+-----+-----+
| 1 | Enable | 192.168.5.6-192.168.5.90 | 123 |
+-----+-----+-----+-----+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

Figure 4-67 Configure Access Control Rule

The following items are displayed on this screen:

- **Enable Rule:** Enable or disable this rule.
- **Source IP Range:** Enter the source IP range in dotted-decimal format (e.g. 192.168.1.23).
- **Destination IP Range:** Enter the destination IP range in dotted-decimal format (e.g. 192.168.1.23).
- **Service Name:** Choose a service type that defined in **Service Type** page.
- **Active Time:** Specify the time range for the entry to take effect.
- **Active Day:** Specify the day range for the entry to take effect.

#### 4.3.3.3.2 User Authentication

The command “show user-authentication” shows the user authentication information as below:

```

BG9002N#show user-authentication
->Enable User Authentication.....: Enable
+-----+-----+-----+-----+
| No | Username | Password |
+-----+-----+-----+-----+
| 0 | 1234 | 1234 |
+-----+-----+-----+-----+

BG9002N#_

```

Figure 4-68 Show User Authentication Information

The command “set user-authentication” configures the user authentication parameters as below:

```

BG9002N#set user-authentication
->Enable User Authentication? 'yes' or 'no'[yes]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded?
BG9002N#

```

Figure 4-69 Configure User Authentication Parameters

The following items are displayed on this screen:

- **Enable User Authentication:** Enable or disable user authentication globally. If enabled, only the following list of users and passwords can access the Internet.

The command “set user authentication list” configures the user authentication list as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set user-authentication list
User Authentication List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->Username[1]:z41x43f
->Password[1]:bfzy
Auth Mode
0-Allow Multi-PC Access
1-Allow One PC Access
2-Allow Special IP Access
3-Allow Special MAC Access
->Auth Mode [0]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set user-authentication list
User Authentication List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+-----+
| No | Username | Password |
+-----+
| 0 | 1234 | 1234 |
+-----+
| 1 | z41x43f | bfzy |
+-----+
->Please input number which you will modify[0-1]:1
->Username[z41x43f]:
->Password[bfzy]:
Auth Mode
0-Allow Multi-PC Access
1-Allow One PC Access
2-Allow Special IP Access
3-Allow Special MAC Access
->Auth Mode [0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
```

```
BG9002N#set user-authentication list
User Authentication List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+-----+
| No | Username | Password |
+-----+
| 0 | 1234 | 1234 |
+-----+
| 1 | z41x43f | bfzy |
+-----+
->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#
```

**Figure 4-70 Configure User Authentication List**

The following items are displayed on this screen:



- ▶ **Username:** Enter the username of this entry.
- ▶ **Password:** Enter the password of this entry.
- ▶ **Auth Mode:** Choose the authentication mode of this entry. Provides four modes:
  - Allow Multi-PC Access:** Allows multiple computers to access the Internet using this account.
  - Allow One PC Access:** Only allows one computer to access the Internet using this account.
  - Allow Special IP Access:** Allowing only specified IP computer uses this account to access the Internet.
  - Allow Special MAC Access:** Allowing only specified MAC computer uses this account to access the Internet

#### 4.3.3.4 Network Access-Ctrl

##### 4.3.3.4.1 WEB

The command “show network-access-ctrl web” shows the web access control information as below:

```
BG9002N#show network-access-ctrl w
BG9002N#show network-access-ctrl web
->HTTP Port.....: 80
->HTTPS Port.....: 443
->Enable Internet Allow Access.....: Enable
->Enable Internet IP Limit.....: Disable
->Internet IP Range<Start IP>.....: 138.0.60.1
->Internet IP Range<End IP>.....: 138.0.255.255
->Internet IPv6 Range<Start IP>.....: 2001::60
->Internet IPv6 Range<End IP>.....: 2001::ffff
->Enable Intranet Allow Access.....: Enable
->Enable Intranet IP Limit.....: Disable
->Intranet IP Range<Start IP>.....: 192.168.1.2
->Intranet IP Range<End IP>.....: 192.168.1.255
->Intranet IPv6 Range<Start IP>.....: 2001::60
->Intranet IPv6 Range<End IP>.....: 2001::ffff
BG9002N#
```

Figure 4-71 Show Web Access Control Information

The command “set network-access-ctrl web” configures the web access control parameters as below:

```

BG9002N#set network-access-ctrl web
->HTTP Port[80]:
->HTTPS Port[443]:
->Enable Internet Allow Access? 'yes' or 'no' [yes]: y
->Enable Internet IP Limit? 'yes' or 'no' [no]: y
->Internet IP Range<Start IP>[138.0.60.1]:
->Internet IP Range<End IP>[138.0.255.255]:
->Internet IPv6 Range<Start IP>[2001::60]:
->Internet IPv6 Range<End IP>[2001::ffff]:
->Enable Intranet Allow Access? 'yes' or 'no' [yes]:
->Enable Intranet IP Limit? 'yes' or 'no' [no]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

**Figure 4-72 Configure Web Access Control Parameters**

The following items are displayed on this screen:

- ▶ **HTTP Port:** Port used with HTTP access device.  
**HTTP:** Hypertext Transfer Protocol.
- ▶ **HTTPS Port:** Port used with HTTPS access device.  
**HTTPS:** it is the result of simply layering the Hypertext Transfer Protocol (HTTP) on top of the SSL/TLS protocol.

#### Internet Web Access:

- ▶ **Allow Access:** If enabled, allow user to access the device from the Internet via WEB.
- ▶ **IP Limit:** If enabled, allow only specific IP range to access the device from the Internet via WEB.
- ▶ **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that is only allowed to access to the device from the Internet via WEB.
- ▶ **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that is only allowed to access to the device from the Internet via WEB.

#### Intranet Web Access:

- ▶ **Allow Access:** If enabled, allow user to access the device from the Intranet via WEB.
- ▶ **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via WEB.
- ▶ **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that is only allowed to access the device from the Intranet via WEB.
- ▶ **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that is only allowed to access the device from the Intranet via WEB.

#### 4.3.3.4.2 TELNET

The command “show network-access-ctrl telnet” shows the telnet access control information as below:

```

BG9002N#show network-access-ctrl telnet
->Port.....: 23
->Enable Internet Allow Access.....: Disable
->Enable Internet IP Limit.....: Disable
->Internet IP Range<Start IP>.....: 138.0.60.1
->Internet IP Range<End IP>.....: 138.0.255.255
->Internet IPv6 Range<Start IP>.....: 2001::60
->Internet IPv6 Range<End IP>.....: 2001::ffff
->Enable Intranet Allow Access.....: Enable
->Enable Intranet IP Limit.....: Disable
->Intranet IP Range<Start IP>.....: 192.168.1.2
->Intranet IP Range<End IP>.....: 192.168.1.255
->Intranet IPv6 Range<Start IP>.....: 2001::60
->Intranet IPv6 Range<End IP>.....: 2001::ffff
BG9002N#

```

**Figure 4-73 Show Telnet Access Control Information**

The command “set network-access-ctrl telnet” configures the telnet access control parameters as below:

```

BG9002N#set network-access-ctrl telnet
->Port[23]:
->Enable Internet Allow Access? 'yes' or 'no' [no]: y
->Enable Internet IP Limit? 'yes' or 'no' [no]: y
->Internet IP Range<Start IP>[138.0.60.1]:
->Internet IP Range<End IP>[138.0.255.255]:
->Internet IPv6 Range<Start IP>[2001::60]:
->Internet IPv6 Range<End IP>[2001::ffff]:
->Enable Intranet Allow Access? 'yes' or 'no' [yes]:
->Enable Intranet IP Limit? 'yes' or 'no' [no]:
Really want to modify? 'yes' or 'no' [yes]:
The configuration will take effect after saved and reloaded!
BG9002N#

```

**Figure 4-74 Configure Telnet Access Control Parameters**

The following items are displayed on this screen:

► **Port:** Port when using telnet tools access device.

#### Internet Telnet Access:

- **Allow Access:** If enabled, allow access to the device from the Internet via telnet.
- **IP Limit:** If enabled, allow only specific IP range to access the device from the Internet via telnet
- **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Internet via telnet.
- **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that only allow access to the device from the Internet via telnet.

#### Intranet Telnet Access:

- **Allow Access:** If enabled, allow access to the device from the Intranet via telnet.
- **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via telnet
- **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Intranet via telnet.
- **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that only allow access to the

device from the Intranet via telnet.

#### 4.3.3.4.3 SSH

The command “show network-access-ctrl ssh” shows the SSH access control information as below:

```
BG9002N#show network-access-ctrl ssh
->Port.....: 22
->Enable Internet Allow Access.....: Disable
->Enable Internet IP Limit.....: Disable
->Internet IP Range(Start IP).....: 138.0.60.1
->Internet IP Range(End IP).....: 138.0.255.255
->Internet IPv6 Range(Start IP).....: 2001::60
->Internet IPv6 Range(End IP).....: 2001::ffff
->Enable Intranet Allow Access.....: Enable
->Enable Intranet IP Limit.....: Disable
->Intranet IP Range(Start IP).....: 192.168.1.2
->Intranet IP Range(End IP).....: 192.168.1.255
->Intranet IPv6 Range(Start IP).....: 2001::60
->Intranet IPv6 Range(End IP).....: 2001::ffff
BG9002N#
```

Figure 4-75 Show SSH Access Control Information

The command “set network-access-ctrl ssh” configures the SSH access control parameters as below:

```
BG9002N#set network-access-ctrl ssh
->Port[22]:
->Enable Internet Allow Access? 'yes' or 'no' [no]: y
->Enable Internet IP Limit? 'yes' or 'no' [no]: y
->Internet IP Range(Start IP)[138.0.60.1]:
->Internet IP Range(End IP)[138.0.255.255]:
->Internet IPv6 Range(Start IP)[2001::60]:
->Internet IPv6 Range(End IP)[2001::ffff]:
->Enable Intranet Allow Access? 'yes' or 'no' [yes]:
->Enable Intranet IP Limit? 'yes' or 'no' [no]:
Really want to modify? 'yes' or 'no' [yes]:
The configuration will take effect after saved and reloaded!
BG9002N#
```

Figure 4-76 Configure SSH Access Control Parameters

The following items are displayed on this screen:

► **Port:** Port when using SSH tools access device.

##### Internet SSH Access:

► **Allow Access:** If enabled, allow access to the device from the Internet via SSH.

► **IP Limit:** If enabled, allow only specific IP range to access the device from the Internet via SSH

► **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Internet via SSH.

► **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that only allow access to the device from the Internet via SSH.

##### Intranet SSH Access:

- **Allow Access:** If enabled, allow access to the device from the Intranet via SSH.
- **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via SSH
- **IP Range:** If **IP Limit** enabled, specifies the IPv4 address range that only allow access to the device from the Intranet via SSH.
- **IPv6 Range:** If **IP Limit** enabled, specifies the IPv6 address range that only allow access to the device from the Intranet via SSH.

### 4.3.3.5 Filter Strategy

#### 4.3.3.5.1 Keyword Filter

The command “show keyword-filter” shows the keyword filter information as below:

```
BG9002N#show keyword-filter

Enable Keyword Filter.....: Enable
Policy.....: Deny

+---+-----+
| No |          Keyword          |
+---+-----+
| 0  | 12345                     |
+---+-----+

BG9002N#
```

Figure 4-77 Show Keyword Filter Information

The command “set keyword-filter” configures the keyword filter parameters as below:

```
BG9002N#set keyword-filter
->Enable Keyword Filter? 'yes' or 'no'[yes]:
->Policy(0-Deny,1-Allow)[0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 4-78 Configure Keyword Filter Parameters

The command “set keyword-filter list” configures the keyword filter list as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set keyword-filter list
Keyword Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->Keyword[]:qwer
The configuration will take effect after saved and reloaded!

BG9002N#
```

```

BG9002N#set keyword-filter list
Keyword Filter List Config:
->Select Config type(0-add,1-del,2-modify)[0]: 2
+-----+
| No |           Keyword           |
+-----+
|0   |1234qwe                     |
+-----+
|1   |qweaszyd                     |
+-----+
->Please input number which you will modify[0-1]:0
->Keyword[1234qwe]:bgzy41
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

```

```

BG9002N#set keyword-filter list
Keyword Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+-----+
| No |           Keyword           |
+-----+
|0   |12345                       |
+-----+
|1   |asdf                        |
+-----+
->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

**Figure 4-79 Configure Keyword Filter List**

The following items are displayed on this screen:

- **Keyword Filter:** If enabled, packet filtering is enabled by keyword.
- **Policy:** The policy for filtering web page, Deny and Allow.

#### 4.3.3.5.2 IP Filter

The command “show ip-filter” shows the IP filter information as below:

```

BG9002N#show ip-filter

Enable MAC Filter.....: Enable
Policy.....: Deny

+-----+
| No |      IPv4      |      IPv6      |
+-----+
|0   |192.168.2.3     |                |
+-----+
BG9002N#

```

**Figure 4-80 Show IP Filter Information**

The command “set ip-filter” configures the IP filter parameters as below:



```

BG9002N#set ip-filter
->Enable IP Filter? 'yes' or 'no'[yes]:
->Policy<0-Deny,1-Allow>[0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!
BG9002N#

```

Figure 4-81 Configure IP Filter Parameters

The command “set ip-filter list” configures the IP filter list as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```

BG9002N#set ip-filter list
IP Filter List Config:
->Select config type<0-add,1-del,2-modify>[0]:
->IPv4[1]:192.168.5.6
The configuration will take effect after saved and reloaded!
BG9002N#

```

```

BG9002N#set ip-filter list
IP Filter List Config:
->Select config type<0-add,1-del,2-modify>[0]: 2
+-----+-----+-----+
| No |      IPv4      |      IPv6      |
+-----+-----+-----+
| 0  | 192.168.2.3    |                 |
+-----+-----+-----+
| 1  | 192.168.5.6    |                 |
+-----+-----+-----+
->Please input number which you will modify[0-1]:1
->IPv4[192.168.5.6]:192.168.6.9
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

```

```

BG9002N#set ip-filter list
IP Filter List Config:
->Select config type<0-add,1-del,2-modify>[0]: 1
+-----+-----+-----+
| No |      IPv4      |      IPv6      |
+-----+-----+-----+
| 0  | 192.168.2.3    |                 |
+-----+-----+-----+
| 1  | 192.168.6.9    |                 |
+-----+-----+-----+
->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

Figure 4-82 Configure IP Filter List

The following items are displayed on this screen:

- ▶ **IP Filter:** If enabled, packet filtering is enabled by IP address.
- ▶ **Policy:** The policy for IP address list. Deny and Allow.

#### 4.3.3.5.3 MAC Filter

The command “show mac-filter” shows the MAC filter information as below:

```
BG9002N#show mac-filter

Enable MAC Filter.....: Enable
Policy.....: Deny

+-----+-----+
| No |      MAC      |
+-----+-----+
| 0  | 11:a3:f6:33:44:55 |
+-----+-----+

BG9002N#
```

Figure 4-83 Show MAC Filter Information

The command “set mac-filter ” configures the MAC filter parameters as below:

```
BG9002N#set mac-filter
->Enable MAC Filter? 'yes' or 'no'[yes]:
->Policy(0-Deny,1-Allow)[0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```

Figure 4-84 Configure IP Filter Parameters

The command “set mac-filter list” configures the MAC filter list as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set mac-filter list
MAC Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]: 0
->MAC[00:00:00:00:00:00]:11:23:4e:d6:56:98
The configuration will take effect after saved and reloaded!

BG9002N#
```

```
BG9002N#set mac-filter list
MAC Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+-----+-----+
| No |      MAC      |
+-----+-----+
| 0  | 11:a3:f6:33:44:55 |
+-----+-----+
| 1  | 11:23:4e:d6:56:98 |
+-----+-----+
->Please input number which you will modify[0-1]: 1
->MAC[11:23:4e:d6:56:98]:33:56:86:25:41:43
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

BG9002N#
```



```

BG9002N#set mac-filter list
MAC Filter List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+-----+-----+
| No |          MAC          |
+-----+-----+
| 0  | 11:a3:f6:33:44:55    |
+-----+-----+
| 1  | 33:56:86:25:41:43    |
+-----+-----+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

Figure 4-85 Configure MAC Filter List

The following items are displayed on this screen:

- **MAC Filter:** If enabled, packet filtering is enabled by MAC.
- **Policy:** The policy for MAC list. Deny and Allow.

#### 4.3.4 QoS

##### 4.3.4.1 Basic Settings

The command “show qos basic-settings” shows the QoS basic settings as below:

```

BG9002N#show qos basic-settings
->Enable QoS.....: Enable
->Scheduling mode.....: PQ
->QoS Priority.....: 802.1P
->Upstream Bandwidth(Kbps).....: 0
->Downstream Bandwidth(Kbps).....: 0
->Enable Voice Reservation.....: Enable
->Voice Reservation Bandwidth(Kbps).....: 96
->Enable Video Reservation.....: Disable
->Enable Remap ToS/DSCP to CoS.....: Disable

BG9002N#_

```

Figure 4-86 Show QoS Basic Settings

The command “set qos basic-settings” configures the QoS basic settings as below:

```

BG9002N#set qos basic-settings
->Enable QoS? 'yes' or 'no' [yes]:
->Scheduling mode<0: PQ, 1: WRR, 2: PQ+WRR>[0]: 1
->Weight[0]: 1
->Weight[0]: 2
->Weight[0]: 3
->Weight[0]: 4
->QoS Priority<0:DSCP, 1:802.1p>[1]: 0
->Upstream Bandwidth(Kbps)<[0]:
->Downstream Bandwidth(Kbps)<[0]:
->Enable Voice Reservation? 'yes' or 'no' [yes]:
->Voice Reservation Bandwidth(Kbps)<[96]:
->Enable Video Reservation? 'yes' or 'no' [no]:
->Enable Remap ToS/DSCP to CoS? 'yes' or 'no' [no]:
Really want to modify? 'yes' or 'no' [yes]:
The configuration will take effect after saved and reloaded!
BG9002N#

```

**Figure 4-87 Configure QoS Basic Settings**

The following items are displayed on this screen:

- ▶ **Qos Enable:** Enable or disable QoS functionality.
- ▶ **Scheduling Mode:**
  - PQ:** PQ means strict priority, that is, when congestion occurs, first sending packets of high priority queue.
  - WRR:** All queues use weighted fair queuing scheme which is defined in **Weight Ratio**
  - PQ+WRR:** Only highest queue use strict priority; others use weighted fair queuing scheme.
- ▶ **Qos Priority:** **DSCP** and **802.1P:** depending on the value of priority classification into different queues.
- ▶ **Upstream Bandwidth:** Configure the bandwidth of upstream.
- ▶ **Downstream Bandwidth:** Configure the bandwidth of downstream.
- ▶ **Enable Voice Reservation:** Enable voice reservation and give the value to reserved for voice
- ▶ **Enable Video Reservation:** Enable video reservation and give the value to reserved for video
- ▶ **Remap Tos/DSCP to CoS:** Check the box that the system will remark 802.1P value with TOS/DSCP of upstream packets, the mapping relationship is as follows:

#### 4.3.4.2 Port Rate Limit

The command “show qos port-limit” shows the port rate limit information as below:

```

BG9002N#show qos port-limit
Tips:UP:Unicast; MP:Multicast; BP:Broadcast;
      UUP:Unknown Unicast; UMP:Unknown Multicast;
+-----+-----+-----+-----+-----+
|Port|Enable |Incoming Rate Limit|Outgoing Rate Limit|Limit Packet type |
+-----+-----+-----+-----+-----+
|LAN1|Disable | 0 kbps           | 0 kbps           |All               |
+-----+-----+-----+-----+-----+
|LAN2|Disable | 0 kbps           | 0 kbps           |UP,MP,UUP,UMP     |
+-----+-----+-----+-----+-----+
|LAN3|Disable | 0 kbps           | 0 kbps           |                  |
+-----+-----+-----+-----+-----+
|LAN4|Disable | 0 kbps           | 0 kbps           |                  |
+-----+-----+-----+-----+-----+
BG9002N#

```

Figure 4-88 Show Port Rate Limit Information

The command “set qos port-limit” configures the port rate limit as below:

```

BG9002N#set qos port-limit
->Input port index<1-LAN1, 2-LAN2, 3-LAN3, 4-LAN4>[1]: 1
->Enable rate limit 'yes' or 'no' [no]:y
->Incoming Rate Limit(Kbps)<0~1024000>[0]: 102400
->Outgoing Rate Limit(Kbps)<0~1024000>[0]:
packet type:
->all 'yes' or 'no' [yes]:n
->unicast 'yes' or 'no' [no]:
->multicast 'yes' or 'no' [no]:
->broadcast 'yes' or 'no' [no]:
->unknown unicast 'yes' or 'no' [no]:
->unknown multicast 'yes' or 'no' [no]:
Really want to modify? 'yes' or 'no'[yes]:y
The configuration will take effect after saved and reloaded!
BG9002N#

```

Figure 4-89 Configure Port Rate Limit

The following items are displayed on this screen:

- ▶ **Port:** Physical LAN port
- ▶ **Enable:** Enable or disable rate limit function.
- ▶ **Incoming Rate Limit:** Enter incoming maximum rate, which must be times of 32Kbps.
- ▶ **Limit Packet Type:** Select the packet type which is limited rate.
- ▶ **Outgoing Rate Limit:** Enter Outgoing maximum rate, which must be times of 32Kbps.

#### 4.3.4.3 Flow Rate Limit

The command “show qos flow-limit” shows the flow rate limit information as below:

```

BG9002N#show qos flow-limit
+-----+-----+-----+-----+-----+
| No | Protocol | Direction | CIR(Kbps) | PIR(Kbps) |
+-----+-----+-----+-----+-----+
| 0 | ANY | up | 0 | 0 |
+-----+-----+-----+-----+-----+

->Enter the index to show(0-0)[0]:0
->IP Range(Start IP).....:1.0.0.1
->IP Range(End IP).....:1.0.0.2
->Active Time(Start Time).....:00:00
->Active Time(End Time).....:00:00
->Active Monday.....:Disable
->Active Tuesday.....:Disable
->Active Wednesday.....:Disable
->Active Thursday.....:Disable
->Active Friday.....:Disable
->Active Saturday.....:Disable
->Active Sunday.....:Disable
->Direction.....:up
->Protocol Type.....:ANY
->Port Range(Start Port).....:0
->Port Range(End Port).....:0
->CIR.....:0
->PIR.....:0

->Show flow rate limit detail para continue or not?[yes]:n
BG9002N#

```

**Figure 4-90 Show Flow Rate Limit Information**

The command “set qos flow-limit” configures the flow rate limit as below. Enter 0 add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```

BG9002N#show qos flow-limit
+-----+-----+-----+-----+-----+
| No |Protocol|Direction| CIR(Kbps) | PIR(Kbps) |
+-----+-----+-----+-----+-----+
| 0  |ANY     |up       | 0         | 0         |
+-----+-----+-----+-----+-----+

->Enter the index to show(0-0)[0]:

BG9002N#set qos flow-limit
Flow Limit List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->IP Range(Start IP)[1:192.168.5.6
->IP Range(End IP)[1:192.168.9.60
->Active Time(Start Time)[00:00]:
->Active Time(End Time)[00:00]:23:00
->Active Monday? 'yes' or 'no'[no]:y
->Active Tuesday? 'yes' or 'no'[no]:y
->Active Wednesday? 'yes' or 'no'[no]:
->Active Thursday? 'yes' or 'no'[no]:
->Active Friday? 'yes' or 'no'[no]:
->Active Saturday? 'yes' or 'no'[no]:
->Active Sunday? 'yes' or 'no'[no]:
->Direction(0-up,1-down,2-all)[0]:1
->Type(0-application,1-Custom)[0]:
->Protocol Type(0-HTTP,1-HTTPS,2-FTP,3-TFTP,4-SMTP,5-POP3,6-TELNET,7-ANY)[0]:
->CIR[0]: 102400
->PIR[0]: 102400
The configuration will take effect after saved and reloaded!

BG9002N#

```

```

BG9002N#set qos flow-limit
Flow Limit List Config:
->Select config type<0-add,1-del,2-modify>[0]: 2
+-----+
| No |Protocol|Direction|  CIR(Kbps)  |  PIR(Kbps)  |
+-----+
| 0  |ANY     |up        |  0          |  0          |
+-----+
| 1  |HTTP    |up        | 102400      | 102400      |
+-----+
->Please input number which you will modify[0-1]:1
->IP Range<Start IP>[192.168.1.2]:
->IP Range<End IP>[192.168.2.3]:
->Active Time<Start Time>[00:00]:
->Active Time<End Time>[12:12]:
->Active Monday? 'yes' or 'no'[yes]:
->Active Tuesday? 'yes' or 'no'[yes]:
->Active Wednesday? 'yes' or 'no'[no]:y
->Active Thursday? 'yes' or 'no'[no]:
->Active Friday? 'yes' or 'no'[no]:
->Active Saturday? 'yes' or 'no'[no]:
->Active Sunday? 'yes' or 'no'[no]:
->Direction<0-up,1-down,2-all>[0]:1
->Type<0-Application,1-Custom>[0]:
->Protocol Type<0-HTTP,1-HTTPS,2-FTP,3-TFTP,4-SMTP,5-POP3,6-TELNET,7-ANY>[0]:2
->CIR[102400]: 10240
->PIR[102400]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reloaded!

```

```

BG9002N#set qos flow-limit
Flow Limit List Config:
->Select config type<0-add,1-del,2-modify>[0]: 1
+-----+
| No |Protocol|Direction|  CIR(Kbps)  |  PIR(Kbps)  |
+-----+
| 0  |ANY     |up        |  0          |  0          |
+-----+
| 1  |FTP     |down      | 10240       | 102400       |
+-----+
->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#_

```

**Figure 4-91 Configure Flow Rate Limit**

The following items are displayed on this screen:

- ▶ **IP Range:** The IP range of LAN's PC.
- ▶ **Active Time:** If not configured, which means that all time are in active
- ▶ **Active Day:** If not configured, which means that all time in active
- ▶ **Direction:**
  - Up:** Check the frame from the direction of the LAN port to the WAN port, and match the source IP and destination port;
  - Down:** Check the frame from the direction of the WAN port to the LAN port, and match the destination IP and source port;
  - Bidirectional:** Limit both upstream and downstream speed.



- ▶ **Limited Bandwidth(CIR):** The limited bandwidth.
- ▶ **Maximal Bandwidth(PIR):** The maximum bandwidth.

If **Application** is selected:

- ▶ **Application Protocol:** Such as HTTP, HTTPS, FTP, TFTP, SMTP, POP3, TELNET, etc.

#### 4.3.4.4 Service

The command “show qos service” shows the QoS service information as below:

```
BG9002N#show qos service
->Enable service queue.....: Enable
->Remap Voice Queue Priority.....: Enable
->Voice Priority.....: 3
->Enable remark Voice 802.1p.....: Disable
->Enable remark Voice DSCP.....: Disable
->Remap MGMT Queue Priority.....: Disable
->Enable remark MGMT 802.1p.....: Disable
->Enable remark MGMT DSCP.....: Disable
->Remap Video Queue Priority.....: Disable
->Enable remark Video 802.1p.....: Disable
->Enable remark Video DSCP.....: Disable
BG9002N#
```

**Figure 4-92 Show QoS Service Information**

The command “set qos service” configures the QoS service as below:

```
BG9002N#set qos service
service qos:
->Enable service queue? 'yes' or 'no'[yes]:
->Remap Voice Queue Priority? 'yes' or 'no'[yes]:
->Voice Priority(0~3)[3]:
->Enable remark Voice 802.1p? 'yes' or 'no'[no]:
->Enable remark Voice DSCP? 'yes' or 'no'[no]:
->Remap MGMT Queue Priority? 'yes' or 'no'[no]:
->Enable remark MGMT 802.1p? 'yes' or 'no'[no]:
->Enable remark MGMT DSCP? 'yes' or 'no'[no]:
->Remap Video Queue Priority? 'yes' or 'no'[no]:
->Enable remark Video 802.1p? 'yes' or 'no'[no]:
->Enable remark Video DSCP? 'yes' or 'no'[no]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#
```

**Figure 4-93 Configure QoS Service**

The following items are displayed on this screen:

- ▶ **Name:** Service name. Read only.
- ▶ **Remap Queue Priority:** Check the box to remap scheduling queue.
- ▶ **Priority:** There are four levels of priority. Priority 3 is highest, and priority 0 is the lowest
- ▶ **Remark 802.1p:** Check the box to enable 802.1p priority remarking.
- ▶ **802.1p Value:** The value of remarking 802.1P.
- ▶ **Remark DSCP:** Check the box to enable DSCP remarking.
- ▶ **DSCP Value:** The value of remarking DSCP.

#### 4.3.4.5 ACL

The command “show qos acl-rule” shows the ACL rule information as below:

```

BG9002N#show qos acl-rule
->input rule id<0~23,all>[0]:
->Rule Name.....: 123
->Bind Port<1-LAN1,2-LAN2,3-LAN3,4-LAN4,5-WAN>....: 0x06
->Rule Type.....: L3 Data
->Src IP.....: 192.168.1.2/255.255.0.0
->Dst IP.....: 139.6.5.9/255.255.0.0
->Drop.....: Disable
->Enable Remark UID.....: Disable
->Enable Remark 802.1P.....: Disable
->Enable Remark DSCP.....: Disable
->Enable Priority.....: Disable
->PIR.....: 0

BG9002N#

```

Figure 4-94 Show ACL Rule Information

The command “set qos acl-rule” configures the ACL rule as below:

```

BG9002N#set qos acl-rule
->Enable ACL 'yes' or 'no' [yes]:
->input rule id<0~23>[0]:
->enable rule 0 'yes' or 'no' [yes]:
->Rule Name[123]:
->Input port member bitmap<Eg: 0x12 include port1,4>[0x11]:
->Rule Type<0-L2 Data,1-L3 Data>[1]:
->Src IP[192.168.1.2]:
->Src Netmask[255.255.0.0]:
->Dst IP[139.6.5.9]:
->Dst Netmask[255.255.0.0]:
->Protocol Type<1: icmp, 6: tcp, 17: udp>[0]: 1
->Drop 'yes' or 'no' [yes]:
->PIR<0~1024000 Kbps>[0]: 1024000
Really want to modify? 'yes' or 'no' [yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

Figure 4-95 Configure ACL Rule

The following items are displayed on this screen:

- ▶ **Rule Name:** The custom name.
- ▶ **Physical Port:** Rule's source port
- ▶ **Rule Type:** Type of rule: **L2 data** or **L3 data**.
- ▶ **Src IP/Netmask:** The source IP address and netmask of packets, such as 192.168.100.1/255.255.255.0.
- ▶ **Dest IP/Netmask:** The destination IP address and netmask of packets.
- ▶ **Protocol:** E.g. ICMP, UDP, TCP, or custom IP protocol types.
- ▶ **SRC MAC:** Source MAC address of packets.
- ▶ **DEST MAC:** Destination MAC address of packets.



- ▶ **Ether Type:** The ether type of packets.
- ▶ **VLAN ID:** The VLAN id of packets.
- ▶ **802.1p:** The VLAN priority of packets.
- ▶ **Drop:** Drop the packets matched with the rule.
- ▶ **Remark VID:** Change the VID of packets matched with the rule.
- ▶ **Remark 802.1p:** Change the 802.1P priority of packets matched with the rule.
- ▶ **Remark DSCP:** Change the DSCP of packets matched with the rule.
- ▶ **Priority:** Change the scheduling queue of packets matched with the rule.
- ▶ **Maximal Bandwidth:** Limit the bandwidth of packet matched with the rule.

#### 4.3.5 DDNS

The command "show ddns status" shows the DDNS status as below:

```
BG9002N#show ddns status
DDNS status.....: DDNS_TASK_NOT_INIT
BG9002N#
```

**Figure 4-96 Show DDNS Status**

The command "show ddns parameter" shows the DDNS parameters as below:

```
BG9002N#show ddns parameter
Enable DDNS.....: Enable
Username.....: dydns
Password.....: 123456
First Url.....: dydns1.com
Second Url.....: dydns2.com
Update Interval.....: 600
Server Type.....: CUSTOM
Server Name.....: dydns.com
Server Url.....: dydns.com
Dyn DNS Server Name.....: dydns.com
Dyn DNS Server Url.....: dydns.com
System Item.....: dydns.com
BG9002N#
```

**Figure 4-97 Show DDNS Parameters**

The command "set ddns" configures the DDNS parameters as below:

```

BG9002N#set ddns
->Enable DDNS 'yes' or 'no' [no]:y
->Username[dydns]:
->Password[123456]:
->First Url[dydns1.com]:
->Second Url[dydns2.com]:
->Update Interval[600]:
->Server Type(0-DYNDNS,1-FREEDNS,2-ZONE,3-NOIP,4-3322,5-CUSTOM)[0]:5
->Server Name[dydns.com]:
->Server Url[dydns.com]:
->Dyn DNS Server Name[dydns.com]:
->Dyn DNS Server Url[dydns.com]:
->System Item[dydns.com]:
Really want to modify? 'yes' or 'no'[yes]:y
The configuration will take effect after saved and reloaded!

BG9002N#

```

**Figure 4-98 Configure DDNS Parameters**

The following items are displayed on this screen:

- ▶ **DDNS Enable:** Active or inactive dynamic DNS service.
- ▶ **Username:** Enter account name of your DDNS account.
- ▶ **Password:** Enter password of your DDNS account.
- ▶ **First Url:** First domain name that you registered your DDNS service provider.
- ▶ **Second Url:** First domain name that you registered your DDNS service provider.
- ▶ **Update Interval:** How often, in seconds, the IP is updated.
- ▶ **Server Type:** optional DDNS server type, can select from pull-down list:
  - DYNDNS:** For dyndns.org
  - FREEDNS:** For freedns.afraid.org
  - ZONE:** For zoneedit.com
  - NOIP:** For no-ip.com
  - 3322:** For 3322.org
  - CUSTOM:** For custom self-defined DDNS server type.
- ▶ **Server Name:** If CUSTOM is selected, specify server name of the device.
- ▶ **Server Url:** If CUSTOM is selected, specify server URL of the device.
- ▶ **Dyn DNS Server Name:** If CUSTOM is selected, specify dyndns DNS server name of custom self-defined.
- ▶ **Dyn DNS Server Url:** If CUSTOM is selected, specify dyndns DNS server URL of custom self-defined.
- ▶ **System Item:** If CUSTOM is selected, specify system item of custom self-defined.
- ▶ **DDNS Status:** Display the status of DDNS service. Read only.

#### 4.3.6 VPN

##### 4.3.6.1 PPTP Server

The command “show pptp-server” shows the pptp server information as below:

```

BG9002N#show ptp-server
Enable PTP Server.....: Enable
IP Address Pool Range(Start IP).....: 192.168.1.1
IP Address Pool Range(End IP).....: 192.168.1.6
Enable Authentication.....: Enable
Enable Encryption.....: Disable
+-----+-----+-----+-----+
! No !      Username      !      Password      !      Binding IP      !
+-----+-----+-----+-----+
!0   !123              !123              !192.168.5.6          !
+-----+-----+-----+-----+
BG9002N#

```

Figure 4-99 Show PPTP Server Information

The command “set ptp-server” configures the ptp server parameters as below:

```

BG9002N#set ptp-server
->Enable PTP Server 'yes' or 'no' [yes]:
->IP Address Pool Range(Start IP)[192.168.1.1]:
->IP Address Pool Range(End IP)[192.168.1.6]:
->Enable Authentication 'yes' or 'no' [yes]:
->Enable Encryption 'yes' or 'no' [no]:
Are you sure save parameter? 'yes' or 'no' [yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

Figure 4-100 Configure PPTP Server Parameters

The following items are displayed on this screen:

- ▶ **Enable PPTP Server:** Enable or disable the PPTP server function globally.
- ▶ **IP Address Pool Range:** Specify the start and the end IP address for IP Pool. The start IP address should not exceed the end address and the IP ranges must not overlap.
- ▶ **Enable Authentication:** Specify whether to enable authentication for the tunnel.
- ▶ **Enable Encryption:** Specify whether to enable the encryption for the tunnel. If enabled, the PPTP tunnel will be encrypted by MPPE.

The command “set ptp-server user” configures the ptp server user list as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```

BG9002N#set ptp-server user
PPTP Server User List Config:
->Select config type(0-add,1-del,2-modify)[0]:
->Username[]:wepasd
->Password[]:123456
->Bind IP[]:136.5.6.9
The configuration will take effect after saved and reset!
BG9002N#

```

```

BG9002N#set ptp-server user
PPTP Server User List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+-----+-----+-----+-----+
| No | Username | Password | Binding IP |
+-----+-----+-----+-----+
| 0 | 123 | 123 | 192.168.5.6 |
+-----+-----+-----+-----+
| 1 | lwepasd | 123456 | 136.5.6.9 |
+-----+-----+-----+-----+
->Please input number which you will modify[0-1]:1
->Username[lwepasd]:
->Password[123456]:
->Bind IP[136.5.6.9]:136.23.6.8
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

```

BG9002N#set ptp-server user
PPTP Server User List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+-----+-----+-----+-----+
| No | Username | Password | Binding IP |
+-----+-----+-----+-----+
| 0 | 123 | 123 | 192.168.5.6 |
+-----+-----+-----+-----+
| 1 | lwepasd | 123456 | 136.23.6.8 |
+-----+-----+-----+-----+
->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

**Figure 4-101 Configure PPTP Server User**

The following items are displayed on this screen:

- ▶ **Username:** Enter the account name of PPTP tunnel. It should be configured identically on server and client.
- ▶ **Password:** Enter the password of PPTP tunnel. It should be configured identically on server and client.
- ▶ **Binding IP:** Enter the IP address of the client which is allowed to connect to this PPTP server.

#### 4.3.6.2 L2TP Server

The command “show l2tp-server” shows the l2tp server information as below:

```

BG9002N#show l2tp-server
Enable L2TP Server.....: Enable
Local IP.....: 10.0.0.1
IP Address Pool Range<Start IP>.....: 10.0.0.1
IP Address Pool Range<End IP>.....: 10.0.0.1
Enable Authentication.....: Enable
L2TP Auth Secret.....: 123456
Enable Debug.....: Enable
+-----+-----+-----+-----+
| No | Username | Password | Binding IP |
+-----+-----+-----+-----+
| 0 | 1234 | 1234 | 138.2.61.136 |
+-----+-----+-----+-----+
| 1 | 1123 | 154321 | 136.56.22.65 |
+-----+-----+-----+-----+
BG9002N#

```

Figure 4-102 Show L2TP Server Information

The command “set l2tp-server” configures the l2tp server parameters as below:

```

BG9002N#set l2tp-server
->Enable L2TP Server 'yes' or 'no' [yes]:
->Local IP[10.0.0.1]:
->IP Address Pool Range<Start IP>[10.0.0.2]:
->IP Address Pool Range<End IP>[10.0.0.2]:
->Enable Authentication 'yes' or 'no' [yes]:
->L2TP Auth Secret[123456]:
->Enable Debug 'yes' or 'no' [yes]:
Are you sure save parameter? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

Figure 4-103 Configure L2TP Server Parameters

The following items are displayed on this screen:

- ▶ **Enable L2TP Server:** Enable or disable the L2TP server function globally.
- ▶ **Local IP:** Enter the local IP address of L2TP server.
- ▶ **IP Address Pool Range:** Specify the start and the end IP address for IP Pool. The start IP address should not exceed the end address and the IP ranges must not overlap.
- ▶ **Enable Authentication:** Specify whether to enable authentication for the tunnel. If enabled, enter the authentication secret.
- ▶ **Enable Debug:** Specify whether to enable the debug for L2TP.

The command “set l2tp-server user” configures the l2tp server user list as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify .If you want to delete the entry, enter 1 and choose the corresponding entry.

```

BG9002N#set l2tp-server user
L2TPServer User List Config:
->Select config type<0-add,1-del,2-modify>[0]:
->Username[1]:yzasd
->Password[1]:123654
->Pointed IP[1]:195.6.5.9
The configuration will take effect after saved and reset!
BG9002N#

BG9002N#set l2tp-server user
L2TPServer User List Config:
->Select config type<0-add,1-del,2-modify>[0]: 2
+-----+-----+-----+-----+
| No | Username | Password | Binding IP |
+-----+-----+-----+-----+
| 0 | 1234 | 1234 | 138.2.61.136 |
+-----+-----+-----+-----+
| 1 | 1123 | 54321 | 136.56.22.65 |
+-----+-----+-----+-----+
| 2 | yzasd | 123654 | 195.6.5.9 |
+-----+-----+-----+-----+
->Please input number which you will modify[0-2]:2
->Username[yzasd]:
->Password[123654]:123456
->Pointed IP[195.6.5.9]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#_

BG9002N#set l2tp-server user
L2TPServer User List Config:
->Select config type<0-add,1-del,2-modify>[0]: 1
+-----+-----+-----+-----+
| No | Username | Password | Binding IP |
+-----+-----+-----+-----+
| 0 | 1234 | 1234 | 138.2.61.136 |
+-----+-----+-----+-----+
| 1 | 1123 | 54321 | 136.56.22.65 |
+-----+-----+-----+-----+
| 2 | yzasd | 123456 | 195.6.5.9 |
+-----+-----+-----+-----+
->Please choose the start index of deleting entry[0-2]:2
->Please choose the end index of deleting entry[0-2]:2
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

Figure 4-104 Configure L2TP Server User

The following items are displayed on this screen:

- **Username:** Enter the account name of L2TP tunnel. It should be configured identically on server and client.
- **Password:** Enter the password of L2TP tunnel. It should be configured identically on server and client.
- **Binding IP:** Enter the IP address of the client which is allowed to connect to this L2TP server.



### 4.3.6.3 IPSEC

#### 4.3.6.3.1 IKE Safety Proposal

The command “show ike-proposal” shows the IKE Proposal information as below:

```
BG9002N#show ike-proposal1
+-----+-----+-----+-----+-----+
| No | Proposal Name | Encryption Algorithm | Auth Algorithm | DH Group |
+-----+-----+-----+-----+-----+
| 0 | ike123 | 3DES | SHA1 | modp1536 |
+-----+-----+-----+-----+-----+

BG9002N#
```

Figure 4-105 Show IKE Proposal Information

The command “set ike-proposal” configures the IKE Proposal as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set ike-proposal1

->IKE Proposal:0-Add,1-Delete,2-Modify[0]:
->Proposal Name[:ike_pro_11
->Encryption Algorithm(0-3DES,1-DES,2-AES)[0]:
->Auth Algorithm(0-SHA1,1-MD5)[0]:
->DH Group(0-modp1536,1-modp1024,2-modp768)[0]:
->Really want to modify? 'yes' or 'no'[yes]:

Oprate success!
The configuration will take effect after saved and reset!
BG9002N#

BG9002N#set ike-proposal1

->IKE Proposal:0-Add,1-Delete,2-Modify[0]:2
+-----+-----+-----+-----+-----+
| No | Proposal Name | Encryption Algorithm | Auth Algorithm | DH Group |
+-----+-----+-----+-----+-----+
| 0 | ike1 | DES | MD5 | modp1536 |
+-----+-----+-----+-----+-----+
| 1 | ike_pro_11 | 3DES | SHA1 | modp1536 |
+-----+-----+-----+-----+-----+

->Enter the index to modify(0-1)[0]:0
->Proposal Name[ike1]:
->Encryption Algorithm(0-3DES,1-DES,2-AES)[1]:0
->Auth Algorithm(0-SHA1,1-MD5)[1]:0
->DH Group(0-modp1536,1-modp1024,2-modp768)[0]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#
```

```

BG9002N#set ike-proposal1
->IKE Proposal:0-Add,1-Delete,2-Modify[0]:1
+-----+-----+-----+-----+-----+
| No | Proposal Name | Encryption Algorithm | Auth Algorithm | DH Group |
+-----+-----+-----+-----+-----+
| 0 | ike1 | DES | MD5 | modp1536 |
+-----+-----+-----+-----+-----+
| 1 | ike_pro_11 | 3DES | SHA1 | modp1536 |
+-----+-----+-----+-----+-----+

->Please choose the start Index of deleting entry[0-1]:1
->Please choose the end Index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

**Figure 4-106 Configure IKE Proposal**

The following items are displayed on this screen:

- ▶ **Proposal Name:** Specify a unique name to the IKE proposal for identification and management purposes. The IKE proposal can be applied to IPSEC proposal.
- ▶ **Encryption Algorithm:** Specify the encryption algorithm for IKE negotiation. Options include:
  - DES:** DES (Data Encryption Standard) encrypts a 64-bit block of plain text with a 56-bit key.
  - 3DES:** Triple DES, encrypts a plain text with 168-bit key.
  - AES:** Uses the AES algorithm for encryption.
- ▶ **Auth Algorithm:** Select the authentication algorithm for IKE negotiation. Options include:
  - MD5:** MD5 (Message Digest Algorithm) takes a message of arbitrary length and generates a 128-bit message digest.
  - SHA1:** SHA1 (Secure Hash Algorithm) takes a message less than  $2^{64}$  (the 64th power of 2) in bits and generates a 160-bit message digest.
- ▶ **DH Group:** Select the DH (Diffie-Hellman) group to be used in key negotiation phase 1. The DH Group sets the strength of the algorithm in bits. Options include **DH 768 modp**, **DH 1024 modp** and **DH 1536 modp**.

#### 4.3.6.3.2 IKE Safety Policy

The command “show ike-policy” shows the IKE Policy information as below:



```

BG9002N#show ike-policy
+-----+-----+-----+-----+-----+
| No | Policy Name | Operation Mode | Auth Mode | PreShareKey |
+-----+-----+-----+-----+-----+
| 0 | ike_policy_1 | Main Mode | PSK | 123321 |
+-----+-----+-----+-----+-----+

->Enter the index to show(0-0)[0]:
Policy Name.....:ike_policy_1
Operation Mode.....:Main Mode
Enable Local ID.....:Disable
Enable Remote ID.....:Disable
Auth Mode.....:PSK
Pre Share Key.....:123321
Enable Safety Proposal1.....:Enable
Proposal Name1.....:ike1
Enable Safety Proposal2.....:Disable
Enable Safety Proposal3.....:Disable
Enable Safety Proposal4.....:Disable

->Show IKE policy detail para continue or not?[yes]:n
BG9002N#

```

Figure 4-107 Show IKE Policy Information

The command “set ike-policy” configures the IKE Policy as below. Enter 0 add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```

BG9002N#set ike-policy
->IKE Policy:0-Add,1-Delete,2-Modify[0]:
->Policy Name[]:ike_po_2
->Operation Mode(0-Main Mode,1-Challenge Mode)[0]:1
->Enable Local ID(yes/no)[no]:
->Enable Remote ID(yes/no)[no]:
->Auth Mode(0-PSK,1-RSA,2-Certificate)[0]:1
->Pre Share Key[]:123456
->Enable Safety Proposal 1(yes/no)[no]:
->Enable Safety Proposal 2(yes/no)[no]:
->Enable Safety Proposal 3(yes/no)[no]:
->Enable Safety Proposal 4(yes/no)[no]:
->Really want to modify? 'yes' or 'no'[yes]:

Oprate success!
The configuration will take effect after saved and reset!
BG9002N#_

```

```

BG9002N#set ike-policy

->IKE Policy:0-Add,1-Delete,2-Modify[0]:2
+-----+-----+-----+-----+-----+
| No | Policy Name | Operation Mode | Auth Mode | PreShareKey |
+-----+-----+-----+-----+-----+
| 0 | ike_policy_1 | Main Mode | PSK | 123321 |
+-----+-----+-----+-----+-----+
| 1 | ike_po_2 | Challenge Mode | RSA | 123456 |
+-----+-----+-----+-----+-----+

->Enter the index to modify(0-1)[0]:1
->Policy Name[ike_po_2]:
->Operation Mode(0-Main Mode,1-Challenge Mode)[1]:0
->Enable Local ID(yes/no)[no]:
->Enable Remote ID(yes/no)[no]:
->Auth Mode(0-PSK,1-RSA,2-Certificate)[1]:
->Pre Share Key[123456]:
->Enable Safety Proposal 1(yes/no)[no]:
->Enable Safety Proposal 2(yes/no)[no]:
->Enable Safety Proposal 3(yes/no)[no]:
->Enable Safety Proposal 4(yes/no)[no]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

BG9002N#set ike-policy

->IKE Policy:0-Add,1-Delete,2-Modify[0]:1
+-----+-----+-----+-----+-----+
| No | Policy Name | Operation Mode | Auth Mode | PreShareKey |
+-----+-----+-----+-----+-----+
| 0 | ike_policy_1 | Main Mode | PSK | 123321 |
+-----+-----+-----+-----+-----+
| 1 | ike_po_2 | Main Mode | RSA | 123456 |
+-----+-----+-----+-----+-----+

->Please choose the start Index of deleting entry[0-1]:1
->Please choose the end Index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

**Figure 4-108 Configure IKE Policy**

The following items are displayed on this screen:

- **Policy Name:** Specify a unique name to the IKE policy for identification and management purposes. The IKE policy can be applied to IPSEC policy.
- **Operation Mode:** Select the IKE Exchange Mode in phase 1, and ensure the remote VPN peer uses the same mode.
  - Main:** Main mode provides identity protection and exchanges more information, which applies to the scenarios with higher requirement for identity protection.
  - Challenge:** Challenge Mode establishes a faster connection but with lower security, which applies to scenarios with lower requirement for identity protection.
- **Enable Local ID:** If enabled, enter a name for the local device as the ID in IKE negotiation.
- **Enable Remote ID:** If enabled, enter the name of the remote peer as the ID in IKE negotiation.

- **Auth Mode:** Select the authentication mode for this IKE policy entry.
- **Pre Share Key:** Enter the Pre-shared Key for IKE authentication, and ensure both the two peers use the same key. The key should consist of visible characters without blank space.
- **Enable Safety Proposal:** Select the Proposal for IKE negotiation phase 1. Up to four proposals can be selected.

#### 4.3.6.3.3 IPSEC Safety Proposal

The command “show ipsec-proposal” shows the IPSEC Proposal information as below:

```
BG9002N#show ipsec-proposal
+-----+-----+-----+-----+-----+
| No | Proposal Name | Encryption Algorithm | Auth Algorithm | IPSEC Protocol |
+-----+-----+-----+-----+-----+
| 0 | ipsec123 | 3DES | SHA1 | ESP |
+-----+-----+-----+-----+-----+

BG9002N#
```

Figure 4-109 Show IPSEC Proposal Information

The command “set ipsec-proposal” configures the IPSEC Proposal as below. Enter 0 add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```
BG9002N#set ipsec-proposal
->IPSEC Proposal:0-Add,1-Delete,2-Modify[0]:
->Proposal Name[:1234
->Encryption Algorithm(0-3DES,1-DES,2-AES)[0]:1
->Auth Algorithm(0-SHA1,1-MD5)[0]:1
->IPSEC Protocol(0-ESP,1-AH,2-ESP+AH)[0]:1
->Really want to modify? 'yes' or 'no'[yes]:

Oprate success!
The configuration will take effect after saved and reset!
BG9002N#

BG9002N#set ipsec-proposal
->IPSEC Proposal:0-Add,1-Delete,2-Modify[0]:2
+-----+-----+-----+-----+-----+
| No | Proposal Name | Encryption Algorithm | Auth Algorithm | IPSEC Protocol |
+-----+-----+-----+-----+-----+
| 0 | ipsec123 | 3DES | SHA1 | ESP |
+-----+-----+-----+-----+-----+
| 1 | 1234 | DES | MD5 | AH |
+-----+-----+-----+-----+-----+
->Enter the index to modify(0-1)[0]:1
->Proposal Name[1234]:
->Encryption Algorithm(0-3DES,1-DES,2-AES)[1]:2
->Auth Algorithm(0-SHA1,1-MD5)[1]:
->IPSEC Protocol(0-ESP,1-AH,2-ESP+AH)[1]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#
```

```

BG9002N#set ipsec-proposal1
->IPSEC Proposal:0-Add,1-Delete,2-Modify[0]:1
+-----+-----+-----+-----+-----+
| No | Proposal Name | Encryption Algorithm | Auth Algorithm | IPSEC Protocol |
+-----+-----+-----+-----+-----+
| 0 | ipsec123 | 3DES | SHA1 | ESP |
+-----+-----+-----+-----+-----+
| 1 | 1234 | AES | MD5 | AH |
+-----+-----+-----+-----+-----+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

**Figure 4-110 Configure IPSEC Proposal**

The following items are displayed on this screen:

- ▶ **Proposal Name:** Specify a unique name to the IPSEC Proposal for identification and management purposes. The IPSEC proposal can be applied to IPSEC policy.
- ▶ **IPSec Protocol:** Select the security protocol to be used. Options include:
  - AH:** AH (Authentication Header) provides data origin authentication, data integrity and anti-replay services.
  - ESP:** ESP (Encapsulating Security Payload) provides data encryption in addition to origin authentication, data integrity, and anti-replay services.
  - ESP+AH:** Both ESP and AH security protocol.
- ▶ **Encryption Algorithm:** Select the algorithm used to encrypt the data for ESP encryption. Options include:
  - DES:** DES (Data Encryption Standard) encrypts a 64-bit block of plain text with a 56-bit key. The key should be 8 characters.
  - 3DES:** Triple DES, encrypts a plain text with 168-bit key. The key should be 24 characters.
  - AES:** Uses the AES algorithm for encryption. The key should be 16 characters.
- ▶ **Auth Algorithm:** Select the algorithm used to verify the integrity of the data. Options include:
  - MD5:** MD5 (Message Digest Algorithm) takes a message of arbitrary length and generates a 128-bit message digest.
  - SHA:** SHA (Secure Hash Algorithm) takes a message less than the 64th power of 2 in bits and generates a 160-bit message digest.

#### 4.3.6.3.4 IPSEC Safety Policy

The command “show ipsec-policy” shows the IPSEC Policy information as below:

```

BG9002N#show ipsec-policy
+-----+-----+-----+-----+-----+-----+
| NO | IPSEC Policy Name | Enable IPSEC | Interface | UPN Mode | Remote Address |
+-----+-----+-----+-----+-----+-----+
| 0 | ipsec_policy_1 | Enable | DATA | PC To Site | 138.60.61.20 |
+-----+-----+-----+-----+-----+-----+

->Enter the index to show(0-0)[0]:
Proposal Name.....:ipsec_policy_1
Enable IPSEC.....:Enable
UPN Mode.....:PC To Site
Interface.....:DATA
Local Subnet IP.....:192.168.20.9
Local Subnet Netmask.....:255.255.255.0
Remote Address.....:138.60.61.20
Remote Subnet IP.....:0.0.0.0
Remote Subnet Netmask.....:0.0.0.0
IKE Policy Name.....:ike_policy_1
Enable IPSEC Proposal1.....:Enable
Proposal Name1.....:ipsec123
Enable IPSEC Proposal2.....:Disable
Enable IPSEC Proposal3.....:Disable
Enable IPSEC Proposal4.....:Disable

->Show IPSEC policy detail para continue or not?[yes]:n
BG9002N#

```

Figure 4-111 Show IPSEC Policy Information

The command “set ipsec-policy” configures the IPSEC Policy as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```

BG9002N#set ipsec-policy
->IPSEC Policy:0-Add,1-Delete,2-Modify[0]:
->Proposal Name[1]:12345
->Enable IPSEC<yes/no>[no]:y
->UPN Mode<0-Site To Site,1-PC To Site>[0]:1
->Interface<[0]DATA [1]VOICE>[0]:
->Local Subnet IP[1]:192.168.1.2
->Local Subnet Netmask[1]:255.255.0.0
->Remote Address[1]:139.6.5.8
->IKE Safety Policy<0-0>[0]:
->Enable IPSEC Proposal 1<yes/no>[no]:
->Enable IPSEC Proposal 2<yes/no>[no]:
->Enable IPSEC Proposal 3<yes/no>[no]:
->Enable IPSEC Proposal 4<yes/no>[no]:
->Really want to modify? 'yes' or 'no'[yes]:

Oprate success!
The configuration will take effect after saved and reset!
BG9002N#

```



```

BG9002N#set ipsec-policy
->IPSEC Policy:0-Add,1-Delete,2-Modify[0]:2
+-----+-----+-----+-----+-----+-----+
| NO | IPSEC Policy Name | Enable IPSEC | Interface | VPN Mode | Remote Address |
+-----+-----+-----+-----+-----+-----+
| 0 | ipsec_policy_1 | Enable | DATA | PC To Site | 138.60.61.20 |
+-----+-----+-----+-----+-----+-----+
| 1 | 12345 | Enable | DATA | PC To Site | 139.6.5.8 |
+-----+-----+-----+-----+-----+-----+
->Enter the index to modify(0-1)[0]:1
->Proposal Name[12345]:
->Enable IPSEC(yes/no)[yes]:
->VPN Mode(0-Site To Site,1-PC To Site)[1]:
->Interface([0]DATA [1]VOICE)[0]:1
->Local Subnet IP[192.168.1.2]:
->Local Subnet Netmask[255.255.0.0]:
->Remote Address[139.6.5.8]:
->IKE Safety Policy(0-0)[0]:
->Enable IPSEC Proposal 1(yes/no)[yes]:
->IPSEC Proposal Name(0-0)[0]:
->Enable IPSEC Proposal 2(yes/no)[no]:
->Enable IPSEC Proposal 3(yes/no)[no]:
->Enable IPSEC Proposal 4(yes/no)[no]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

BG9002N#set ipsec-policy
->IPSEC Policy:0-Add,1-Delete,2-Modify[0]:1
+-----+-----+-----+-----+-----+-----+
| NO | IPSEC Policy Name | Enable IPSEC | Interface | VPN Mode | Remote Address |
+-----+-----+-----+-----+-----+-----+
| 0 | ipsec_policy_1 | Enable | DATA | PC To Site | 138.60.61.20 |
+-----+-----+-----+-----+-----+-----+
| 1 | 12345 | Enable | VOICE | PC To Site | 139.6.5.8 |
+-----+-----+-----+-----+-----+-----+
->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

**Figure 4-112 Configure IPSEC Policy**

The following items are displayed on this screen:

- ▶ **Enable Ipsec:** Enable or disable this IPSEC entry.
- ▶ **IPSEC Policy Name:** Specify a unique name to the IPSEC policy.
- ▶ **Select Interface:** Specify the local WAN port for this Policy.
- ▶ **VPN Mode:** Select the network mode for IPSEC policy. Options include:
  - Site To Site:** Select this option when the client is a network.
  - PC to Site:** Select this option when the client is a host.
- ▶ **Local Subnet IP & Local Subnet Netmask:** Specify IP address range on your local LAN to identify which PCs on your LAN are covered by this policy.
- ▶ **Remote Address:** If **PC to Site** is selected, specify IP address on your remote network to identify which PCs on the remote network are covered by this policy.

- ▶ **Remote Subnet IP & Remote Subnet Netmask:** Specify IP address range on your remote network to identify which PCs on the remote network are covered by this policy.
- ▶ **IKE Safety Policy:** Specify the IKE policy.
- ▶ **Enable Safety Prososal: If enabled,** Select IPSEC Proposal.

### 4.3.7 Routing

#### 4.3.7.1 Static Route

##### 4.3.7.1.1 IPv4

The command “show static-route ipv4” shows the IPv4 static route information as below:

```
BG9002N#show static-route ipv4
```

No	Enable	Destination	Netmask	Next Hop	Valid
10	Enable	192.168.12.6	255.255.255.0	DATA	Invalid

```
BG9002N#
```

Figure 4-113 Show IPv4 Static Route Information

The command “set static-route ipv4” configures the IPv4 static route as below.

```
BG9002N#set static-route ipv4
->Please input ipv4 static route index<0-9>[0]: 1
->Enable Route 'yes' or 'no' [no]: y
->Destination[192.168.16.5]:
->Netmask[255.255.255.0]:
->Next Hop Type<0-Interface,1-Address>[1]:
->Gateway[192.168.10.1]:
Really want to modify? 'yes' or 'no' [yes]:
The configuration will take effect after saved and reset!
BG9002N#
```

Figure 4-114 Configure IPv4 Static Route

The following items are displayed on this screen:

- ▶ **Enable:** Select it to add and modify the current route. Conversely, disable the current route.
- ▶ **Destination IP:** Enter the destination host the route leads to.
- ▶ **Netmask:** Enter the Subnet mask of the destination network.
- ▶ **Next Hop Type:** Include **Next Hop Interface** and **Next Hop Address**(see following option)
- ▶ **Next Hop Interface:** Specify the interface of next hop for current route
- ▶ **Next Hop Address:** Specify the address of next hop for current route
- ▶ **Valid:** Show the status of current route.

##### 4.3.7.1.2 IPv6

The command “show static-route ipv6” show the IPv6 static route information as below:

```

BG9002N#show static-route ipv6
+-----+-----+-----+-----+-----+
| No | Enable | Destination IPv6/Prefix Length | Next Hop | Valid |
+-----+-----+-----+-----+-----+
| 0 | Enable | 2001::1/64 | WAN | Valid |
+-----+-----+-----+-----+-----+
BG9002N#

```

**Figure 4-115 Show IPv6 Static Route Information**

The command “set static-route ipv6” configures the IPv6 static route as below.

```

BG9002N#set static-route ipv6
->Please input ipv6 static route index<0-9>[0]: 1
->Enable Route 'yes' or 'no' [no]: y
->Destination IPv6 [2001::2]:
->IPv6 Prefix Length [64]:
->Next Hop Type<0-Interface,1-Address>[0]:
->Next Hop Interface<0-WAN>[0]:
Really want to modify? 'yes' or 'no' [yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

**Figure 4-116 Configure IPv6 Static Route**

The configuration options of Ipv6 is similar to Ipv4, the prefix length is equal to mask of Ipv4 address.

#### 4.3.7.2 Policy Route

The command “show policy-route” shows the policy route information as below:



```

BG9002N#show policy-route
+-----+-----+-----+-----+-----+
| No | Enable | Src IP Range | Dst Port Range | Next Hop |
+-----+-----+-----+-----+-----+
| 0 | Enable | 0.0.0.0-0.0.0.0 | 0-0 | DATA |
+-----+-----+-----+-----+-----+

->Enter the index to show(0-0)[0]:
Enable Policy Route.....:Enable
Next Hop Type(0-Interface,1-Address).....:Interface
Next Hop Interface.....:DATA
Protocol Type(0-ALL,1-TCP,2-UDP).....:ALL
Source IP(Start IP).....:0.0.0.0
Source IP(End IP).....:0.0.0.0
Destination IP(Start IP).....:0.0.0.0
Destination IP(End IP).....:0.0.0.0
Destination Port(Start Port).....:0
Destination Port(End Port).....:0
Active Time(Start Time).....:00:00
Active Time(End Time).....:23:59
Active Monday.....:Disable
Active Tuesday.....:Disable
Active Wednesday.....:Disable
Active Thursday.....:Disable
Active Friday.....:Disable
Active Saturday.....:Disable
Active Sunday.....:Disable

->Show policy route detail para continue or not?[yes]:n
BG9002N#

```

**Figure 4-117 Show Policy Route Information**

The command “set policy-route” configure the policy route as below. Enter 0 to add a new entry. Enter 2 and choose the entry you want to modify. If you want to delete the entry, enter 1 and choose the corresponding entry.

```

BG9002N#set policy-route
Policy Route List Config:
->Select config type(0-add,1-del,2-modify)[0]: 0
->Enable Polocy Route? 'yes' or 'no'[no]:y
->Next Hop Type(0-Interface,1-Address)[0]:
->Next Hop Interface([0]DATA [30]3G Modem [31]DATA UPN)[0]:
->Protocol Type(0-ALL,1-TCP,2-UDP)[0]:1
->Source IP<Start IP>[1]:192.55.66.22
->Source IP<End IP>[1]:192.168.66.99
->Destination IP<Start IP>[1]:135.6.5.2
->Destination IP<End IP>[1]:135.6.8.9
->Destination Port<Start Port>[0]:1000
->Destination Port<End Port>[0]:2000
->Active Time<Start Time>[00:00]:
->Active Time<End Time>[00:00]:23:25
->Active Monday? 'yes' or 'no'[no]:y
->Active Tuesday? 'yes' or 'no'[no]:y
->Active Wednesday? 'yes' or 'no'[no]:
->Active Thursday? 'yes' or 'no'[no]:
->Active Friday? 'yes' or 'no'[no]:
->Active Saturday? 'yes' or 'no'[no]:
->Active Sunday? 'yes' or 'no'[no]:
The configuration will take effect after saved and reloaded!

```

```

BG9002N#set policy-route
Policy Route List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
+-----+-----+-----+-----+-----+-----+
| No | Enable |      Src IP Range      | Dst Port Range |   Next Hop   |
+-----+-----+-----+-----+-----+-----+
| 0  | Enable | 0.0.0.0-0.0.0.0        | 0-0            | DATA        |
+-----+-----+-----+-----+-----+-----+
| 1  | Enable | 192.168.3.6-192.168.3.60 | 1000-2000      | DATA        |
+-----+-----+-----+-----+-----+-----+
->Please input number which you will modify[0-1]:1
->Enable Polocy Route? 'yes' or 'no'[yes]:
->Next Hop Type(0-Interface,1-Address)[0]:
->Next Hop Interface([0]DATA [1]VOICE [30]3G Modem [31]DATA UPN)[0]:30
->Protocol Type(0-ALL,1-TCP,2-UDP)[0]:
->Source IP<Start IP>[192.168.3.6]:
->Source IP<End IP>[192.168.3.60]:
->Destination IP<Start IP>[138.0.65.2]:
->Destination IP<End IP>[138.0.65.9]:
->Destination Port<Start Port>[1000]:
->Destination Port<End Port>[2000]:
->Active Time<Start Time>[00:00]:
->Active Time<End Time>[23:59]:
->Active Monday? 'yes' or 'no'[no]:
->Active Tuesday? 'yes' or 'no'[no]:
->Active Wednesday? 'yes' or 'no'[no]:
->Active Thursday? 'yes' or 'no'[no]:
->Active Friday? 'yes' or 'no'[no]:
->Active Saturday? 'yes' or 'no'[no]:
->Active Sunday? 'yes' or 'no'[no]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

```

BG9002N#set policy-route
Policy Route List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
+-----+-----+-----+-----+-----+
| No | Enable | Src IP Range | Dst Port Range | Next Hop |
+-----+-----+-----+-----+-----+
| 0 | Enable | 0.0.0.0-0.0.0.0 | 0-0 | DATA |
+-----+-----+-----+-----+-----+
| 1 | Enable | 192.168.3.6-192.168.3.60 | 1000-2000 | 3G |
+-----+-----+-----+-----+-----+

->Please choose the start index of deleting entry[0-1]:1
->Please choose the end index of deleting entry[0-1]:1
->Are you sure to delete?'yes' or 'no'[yes]:
Delete success
BG9002N#

```

Figure 4-118 Configure Policy Route

The following items are displayed on this screen:

- ▶ **Enable PoliceRoute:** Enable or disable the entry
- ▶ **Next Hop Type:** Select from pull-down list: **Interface**, **Address**.
- ▶ **Interface:** Specify the interface of next hop for the entry.
- ▶ **Address:** Specify the address of next hop for the entry.
- ▶ **Description:** Give description for the entry.
- ▶ **Protocol:** Specify the protocol, **TCP**, **UDP** or **ALL**.
- ▶ **Source IP:** Enter IP address or IP range of source in the rule entry.
- ▶ **Destination IP:** Enter IP address or IP range of destination in the rule entry.
- ▶ **Destination Port:** Specify port or port range of destination in the rule entry.
- ▶ **Active Time:** Specify the active time range for the rule entry.
- ▶ **Active Day:** Specify the active days for the rule entry.

#### 4.3.7.3 RIP

##### 4.3.7.3.1 RIP Service

The command “show rip” shows the RIP information as below:

```

BG9002N#show rip
->Enable RIP Protocol:Enable

RIP Interface List:
+-----+-----+-----+-----+-----+-----+
| NO | Interface | Version | Auth | AuthKeyMode | KeyFrom | Key |
+-----+-----+-----+-----+-----+-----+
| 0 | DATA | R2 S2 | disable | simple key | string | |
+-----+-----+-----+-----+-----+-----+

->Key Chain Name:12345

Key List of Key-Chain:
+-----+-----+-----+
| No | Key ID | Key-String |
+-----+-----+-----+
| 0 | 1 | 12345 |
+-----+-----+-----+

BG9002N#

```

**Figure 4-119 Show RIP Information**

The command “set rip switch” configures the RIP switch as below:

```
BG9002N#set rip switch
->Enable RIP Protocol 'yes' or 'no' [yes]:
Really want to modify? 'yes' or 'no' [yes]:

BG9002N#_
```

**Figure 4-120 Configure RIP Switch**

The following items are displayed on this page:

- **Enable RIP Service:** Enable or disable RIP service function globally.

The command “set rip interface” configures the RIP interface as below.

```
BG9002N#set rip interface

RIP Interface List:
+-----+-----+-----+-----+-----+-----+-----+
| NO | Interface | Version | Auth | AuthKeyMode | KeyFrom | Key |
+-----+-----+-----+-----+-----+-----+-----+
| 0 | DATA | R2 S2 | disable | simple key | string | |
+-----+-----+-----+-----+-----+-----+-----+

Rip Interface List Config:
->Select config type<0-add,1-del,2-modify>[0]:
->Interface<0-Data,1-Voice,2-Mgmt,3-Other1,4-Other2>:[0] 1
->Interface Recv RIP Version<1-RIPv1, 2-RIPv2>[2]:
->Interface Send RIP Version<1-RIPv1, 2-RIPv2>[2]:
->Enable Interface RIP Authentication 'yes' or 'no' [no]:y
->Interface RIP Authentication Key Mode<0-text, 1-md5>[0]:
->Interface RIP Authentication Key Get Mode<0-simple Key, 1-key chain>[0]:
->Interface RIP Authentication Simple Key[]: 123
->Continue to Add RIP Interface? 'yes' or 'no' [no]: n

BG9002N#
```

```

BG9002N#set rip interface

RIP Interface List:
+-----+-----+-----+-----+-----+-----+-----+
| NO | Interface | Version | Auth | AuthKeyMode | KeyFrom | Key |
+-----+-----+-----+-----+-----+-----+-----+
| 0 | DATA | R2 S2 | disable | simple key | string | |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | VOICE | R2 S2 | enable | simple key | string | 123 |
+-----+-----+-----+-----+-----+-----+-----+

Rip Interface List Config:
->Select config type(0-add,1-del,2-modify)[0]: 2
Enter the index to modify(0-1)[0]: 1
->Interface(0-Data,1-Voice,2-Mgmt,3-Other1,4-Other2)[1]: 2
->Interface Recv RIP Version(1-RIPv1, 2-RIPv2)[2]: 1
->Interface Send RIP Version(1-RIPv1, 2-RIPv2)[2]:
->Enable Interface RIP Authentication 'yes' or 'no' [yes]:
->Interface RIP Authentication Key Mode(0-text, 1-md5)[0]:
->Interface RIP Authentication Key Get Mode(0-simple Key, 1-key chain)[0]:
->Interface RIP Authentication Simple Key[123]:
->Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!

RIP Interface List:
+-----+-----+-----+-----+-----+-----+-----+
| NO | Interface | Version | Auth | AuthKeyMode | KeyFrom | Key |
+-----+-----+-----+-----+-----+-----+-----+
| 0 | DATA | R2 S2 | disable | simple key | string | |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | MGMT | R1 S2 | enable | simple key | string | 123 |
+-----+-----+-----+-----+-----+-----+-----+

Rip Interface List Config:
->Select config type(0-add,1-del,2-modify)[0]: 1
->Please input begin index(0-1)[0]: 1
->Please input end index(0-1)[0]: 1
Delete success

BG9002N#

```

Figure 4-121 Configure RIP Interface

The following items are displayed on this screen:

- ▶ **Interface:** Specify the interface for the entry.
- ▶ **Receive RIP Version:** Specify receiving RIP version for the entry.
- ▶ **Send RIP Version:** Specify sending RIP version for the entry.
- ▶ **Authorization Enable:** Check the box to enable authorization.
- ▶ **Key Mode:** Specify the encryption mode of key, **TEXT**(plaintext),**MD5**(cipertext).
- ▶ **Key Type:** Specify the key from **Simple String** or **Key Chain**.
- ▶ **Simple String:** If select Simple String in item of Key Type, enter simple string as key.

#### 4.3.7.3.2 Key Chain

The command “set rip key-chain” configures the RIP key chain as below.



```

BG9002N#set rip key-chain
Current Key-Chain Name:12345
Want to Modify Key Chain Name? 'yes' or 'no'[no]n

Key List of Key-Chain:
+-----+-----+-----+
| No |Key ID|Key-String  |
+-----+-----+-----+
| 0  | 3    |12345       |
+-----+-----+-----+

Sure to Config Key List of the Key-Chain? 'yes' or 'no'[no]: y
Key List Config of Key-Chain:
->Select config type<0-add,1-del,2-modify>[0]:
->Key ID: 1
->Key String: qwer
->Continue to Add Key to Key Chain? 'yes' or 'no'[no]: n

BG9002N#

```

```

BG9002N#set rip key-chain
Current Key-Chain Name:12345
Want to Modify Key Chain Name? 'yes' or 'no'[no]:n

Key List of Key-Chain:
+-----+-----+-----+
| No |Key ID|Key-String  |
+-----+-----+-----+
| 0  | 3    |12345       |
+-----+-----+-----+
| 1  | 1    |qwer        |
+-----+-----+-----+

Sure to Config Key List of the Key-Chain? 'yes' or 'no'[no]: y
Key List Config of Key-Chain:
->Select config type<0-add,1-del,2-modify>[0]: 2
->Please input index to modify<0-1>[0]: 1
->Key ID[1]: 2
->Key String[qwer]:
->Really want to modify? 'yes' or 'no'[yes]:
    The configuration will take effect after saved and reset!

BG9002N#_

```

```

BG9002N#set rip key-chain
Current Key-Chain Name:12345
Want to Modify Key Chain Name? 'yes' or 'no'[no]

Key List of Key-Chain:
+-----+-----+-----+
| No | Key ID | Key-String |
+-----+-----+-----+
| 0 | 13 | 12345 |
+-----+-----+-----+
| 1 | 12 | qwer |
+-----+-----+-----+

Sure to Config Key List of the Key-Chain? 'yes' or 'no'[no]: y
Key List Config of Key-Chain:
->Select config type<0-add,1-del,2-modify>[0]: 1
->Please input begin index<0-1>[0]: 1
->Please input end index<0-1>[0]: 1
Delete success

BG9002N#

```

Figure 4-122 Configure RIP Key Chain

The following items are displayed on this screen:

- ▶ **Key Chain Name:** Enter the name of key chain.
- ▶ **Key ID:** Enter the ID of the entry.
- ▶ **Key String:** Enter the Key of the entry.

### 4.3.8 Advanced Parameters

#### 4.3.8.1 UPnP Parameter

The command “show upnp” shows the UPnP information as below:

```

BG9002N#show upnp

Enable Upnp.....: Enable
Upstream Interface.....: VLAN1
Downstream Interface.....: STB

BG9002N#

```

Figure 4-123 Show UPnP Information

The command “set upnp” configures the UPnP parameters as below.

```

BG9002N#set upnp
->Enable Upnp 'yes' or 'no' [yes]:
->Upstream Interface<[0]DATA [1]VOICE [5]VLAN1>[5]:
->Downstream Interface<[5]VLAN1 [21]STB>[21]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#_

```

Figure 4-124 Configure UPnP Parameters

The following items are displayed on this screen:

- ▶ **Enable UPnP:** Enable or disable the UPnP function globally.
- ▶ **Upstream Interface:** The network interface connected to the DLNA server.

- **Downstream Interface:** The network interface connected to the DLNA client.

### 4.3.9 Multicast

The command “show multicast” shows the multicast information as below:

```
BG9002N#show multicast
  Enable IGMP proxy.....: Enable
BG9002N#
```

**Figure 4-125 Show Multicast Information**

The command “set multicast” configures the multicast parameters as below.

```
BG9002N#set multicast
->Enable IGMP proxy? 'yes' or 'no'[yes]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!
BG9002N#_
```

**Figure 4-126 Configure Multicast Parameters**

The following items are displayed on this screen:

- **Enable IGMP Proxy:** Enable or disable the IGMP proxy function globally. Currently, IGMP proxy is mainly used for IPTV.

## 4.4 VOIP Service

### 4.4.1 SIP Service

The command “show sip” shows the sip service information as bellow:

```
BG9002N#show sip
+-----+
|No. | ID |   Register Server |   Server IP/Domain   | Port |Register Cycle |
+-----+-----+-----+-----+-----+-----+
|  0  |  1  |   RegServer1     |   192.168.100.124   | 5060 |       1200    |
+-----+-----+-----+-----+-----+-----+

Enable backup server or not.....:yes
Backup Register server IP or domain.....:192.168.100.106
Backup Register server port.....:5060
Enable proxy server or not.....:yes
Proxy server domain name or IP.....:192.168.100.123
Proxy server port.....:5060
Enable backup agent register or not.....:yes
Back agent register server ip or domain.....:192.168.100.122
Back agent Register server port.....:5060
RTP Port.....:1024-65535
Local SIP Port<1024-65535>.....:5060
BG9002N#
```



**Figure 4-127 Show Sip Server Information**

Execute the command “set sip” to set the sip information as below:

```

BG9002N#set sip
+-----+
+No. | ID | Register Server | Server IP/Domain | Port | Register Cycle |
+-----+-----+-----+-----+-----+-----+
+ 0 | 1 | RegServer1 | 192.168.100.124 | 5060 | 1200 |
+-----+-----+-----+-----+-----+-----+
->Input register server name[RegServer1]:
->Register server ip or domain[192.168.100.124]:
->Register server port<1024-65535>[5060]:
->Enable backup server or not[yes]:
->Backup Register server IP or domain<Enter SPACE key to clear>[192.168.100.106]:
:
->Backup Register server port<1024-65535>[5060]:
->Enable proxy server or not[yes]:n
->Enable backup proxy register or not[yes]:
->Backup proxy register server ip or domain[192.168.100.122]:
->Backup proxy Register server port<1024-65535>[5060]:
->Register interval<60-3600s>[1200]:
->Rtp begin Port<1024-65535>[1024]:
->Rtp end Port<1024-65535>[65535]:
->Local SIP Port<1024-65535>[5060]:
->Really want to modify? 'yes' or 'no'[yes]:

Operate success!

The configuration will take effect after saved and reloaded!

```

**Figure 4-128 Configure Sip Server**

At first, the command will show the sip server information, and then begin to configure sip server.

The following items are displayed on this screen:

- ▶ **Register server ip or domain:** Domain or IP of SIP server.
- ▶ **Register Server Port:** Listening port of SIP server.
- ▶ **Enable Backup Server or not:** Enable or disable backup SIP server.
- ▶ **Backup Server IP or Domain:** Domain or IP of backup SIP server.
- ▶ **Backup Register Server Port:** Listening port of backup SIP server.
- ▶ **Enable Proxy Server or not:** Enable or disable Proxy server.
- ▶ **Proxy Server domain name or IP:** Domain or IP of proxy server.
- ▶ **Proxy Server Port:** Listening port of proxy server.
- ▶ **Enable Backup Proxy register or not:** Enable or disable backup proxy server.
- ▶ **Backup Proxy Register Server ip or domain:** Domain or IP of backup proxy server.
- ▶ **Backup Proxy Register Server Port:** Listening port of backup proxy server.
- ▶ **Register Interval:** Enter the desired time interval at which the sip UA will send register message.
- ▶ **RTP begin:** Local RTP port range begin.
- ▶ **RTP end:** Local RTP port range end.
- ▶ **Local SIP Port:** Local listening port.

The command “show sipadvance” shows the advanced SIP information as below:

```

BG9002N#show sipadvance

SBC enable or not.....:no
Enable Keeping Alive.....:yes
Alive Time(20-3600s).....:500
Keep Alive Mode.....:OPTIONS
Enable Realm.....:yes
Realm PIN.....:
Enable Session .....:yes
Conversation Refresh Interval(90-3600s).....:90
Conversation Refresh Preference.....:UAS
Enable Sip Retrans Timer.....:yes
Retrans Interval.....:200
Retrans Times.....:3
User Agent.....:usersec
SDP Mode When Call holding.....:Send-Only
Enable NextNonce.....:yes
Max Value of NextNonce.....:9
Support PRACK or not.....:yes
Support USER-PHONE or not.....:yes
Auto Update Register Cycle or not.....:yes
Support Full Register or not.....:yes
First Package with Information.....:yes
SDP with Audio when T38 Faxing.....:no
Tos/DiffServ settings.....:DiffServ(Dscp)
Signaling Precedence.....:0
Voice Precedence.....:0
Enable Call In Black&White.....:Black User List
Enable Call Out Black&White.....:Black User List
BG9002N#

```

**Figure 4-129 Show Advance Sip Information**

The command “set sipadvance” configures the advanced SIP information as below:

```

BG9002N#set sipadvance
->SBC enable or not[no]:
->Enable Keeping Alive[yes]:
->Alive Time(20-3600s)[500]:
->Keep Alive Mode(0-CLRF,1-OPTIONS,2-PING)[1]:
->Enable Realm[yes]:
->Realm PIN[]:
->Enable Session [yes]:
->Conversation Refresh Interval(90-3600s)[90]:
->Conversation Refresh Preference(0-UAC,1-UAS)[1]:
->Enable Sip Retrans Timer[yes]:
->Retrans Interval(1-360s)[200]:
->User Agent[usersec]:
->SDP Mode When Call holding(0-0.0.0.0,1-Send-Only)[1]:
->Enable NextNonce[yes]:
->Max Value of NextNonce(1-65535)[9]:8
->Tos/DiffServ settings(0-Tos Ip Precedence,1-DiffServ(Dscp))[1]:
->Signaling Precedence(0-7)[0]:
->Voice Precedence(0-7)[0]:
->Support PRACK or not[yes]:
->Support USER-PHONE or not[yes]:
->Auto Update Register Cycle or not[yes]:
->Support Full Register or not[yes]:
->First Package with Information[yes]:
->SDP with Audio when T38 Faxing[no]:
->Enable Call In Black&White(0-Black User List,1-White User List)[0]:
->Enable Call Out Black&White(0-Black User List,1-White User List)[0]:
->Really want to modify? 'yes' or 'no'[yes]:

The configuration will take effect after saved and reloaded!

```

**Figure 4-130 Configure Advance Sip Parameter**

The following items are displayed on this screen:

- ▶ **Enable Keeping Alive:** After successful registration, whether to send keep-alive packets.
- ▶ **Keep Alive Mode:** Keep alive mode: **CLRF**, **OPTIONS** or **PING**.
- ▶ **Enable Realm:** Check the box to enable SIP signaling packets with realm field information.
- ▶ **Enable Session:** Enable or disable UAC / UAS session refresh mode.
- ▶ **Enable SIP Retrans Timer:** When registration fails, whether to initiate retransmission, retransmission cycle and time with configuration.
- ▶ **User Agent:** Check the box to enable signaling packets with **User Agent** field.
- ▶ **SDP Mode When Call holding:** Select the SIP signal format of call hold.
- ▶ **Enable Next Nonce:** Enable SIP packets with nonce count field information, incremented each one and with a maximum value.
- ▶ **Support PRACK or not:** Enable or disable provisional response. If enabled, 1xx (except 100rel) messages are required to respond with ACK.
- ▶ **Support User-Phone or not:** Whether SIP signaling packets with User = Phone field information.
- ▶ **Auto Update Register Cycle:** Based on server response to update registration period.
- ▶ **Support Full Register or not:** Each registration packets are generated, rather than re-issued.
- ▶ **First Package With Infomation:** The first registration packet with authentication information.
- ▶ **SDP With Audio When T38 Faxing:** T38 fax signaling packet with audio information.

## 4.4.2 User

### 4.4.2.1 User

The command “show sipuser” shows the sip user parameters as below:

```
BG9002N#show sipuser
+-----+
|No. | ID | Account Name | Extension | Register Account | Register | Authen User |
+-----+-----+-----+-----+-----+-----+-----+
| 0 | 1 | Phone_001 | 700 | phone1 | no | phonetest |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | 2 | Phone_002 | 701 | ghjfh | no | |
+-----+-----+-----+-----+-----+-----+-----+

->Enter the index to show<0-1>[0]:
Register State.....:Unregister
Phone Number.....:700
Register Account.....:phone1
Auth User Name.....:phonetest
Password.....:*****
Enable Register.....:no

->See detail information continue or not?[yes]:n
BG9002N#
```

Figure 4-131 Show sip user Parameter

The command “set sipuser” configures the sip parameter as below:

```
BG9002N#set sipuser
+-----+
|No. | ID | Account Name | Extension | Register Account | Register | Authen User |
+-----+-----+-----+-----+-----+-----+-----+
| 0 | 1 | Phone_001 | 700 | phone1 | no | phonetest |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | 2 | Phone_002 | 701 | ghjfh | no | |
+-----+-----+-----+-----+-----+-----+-----+

->Enter the index to modify<0-1>[0]:
->Phone number[700]:
->Register Account[phone1]:
->Auth User Name[phonetest]:phoneauth
->Password[*****]:
->Enable Register<yes/no>[no]:
->Really want to modify? 'yes' or 'no'[yes]:

Operate success!

The configuration will take effect after saved and reloaded!
```

Figure 4-132 Configure sip user Parameter

The following items are displayed on this screen:

- ▶ **Register Account:** Account name registered to SIP server.
- ▶ **Auth Username:** Username of the account.
- ▶ **Password:** Password of the account.
- ▶ **Phone number:** Caller and called number of subscriber line.

- **Enable Register:** Enable registering.

#### 4.4.2.2 Wildcard Group

The command “show groupregister” show wildcard group as below:

```
BG9002N#show groupregist
+-----+
|No. | ID | Register Name | Wildcard Grp | wildcard account | Register State |
+-----+
| 0 | 1 | phone1 | 0 | yes | Unregister |
+-----+
| 1 | 2 | ghjfh | 0 | yes | Unregister |
+-----+

BG9002N#
```

Figure 4-133 Show Wildcard Group Parameter

The command “set groupregister” sets wildcard group as below:

```
BG9002N#set groupregist
+-----+
|No. | ID | Register Name | Wildcard Grp | wildcard account | Register State |
+-----+
| 0 | 1 | phone1 | 0 | yes | Unregister |
+-----+
| 1 | 2 | ghjfh | 0 | yes | Unregister |
+-----+

->Please input wildcard group number(0-99)>[0]:
->Please input the sequence number of account for the group(0-1)>[0]:
->Is it wildcard account(yes/no)>[no]:y
->Are you continue?'yes' or 'no'>(yes/no)>[no]:y
->Please input the sequence number of account for the group(0-1)>[0]:1
->Are you continue?'yes' or 'no'>(yes/no)>[no]:y
->Please input the sequence number of account for the group(0-1)>[0]:
->Are you continue?'yes' or 'no'>(yes/no)>[no]:
->->Really want to modify? 'yes' or 'no'[yes]:

The configuration will take effect after saved and reloaded!
```

Figure 4-134 Configure Wildcard Group Parameter

#### 4.4.3 Supplementary

The command “show extended-server” shows user supplementary as below:

```

BG9002N#show extended-service

Min Flash Detect Time(50-750).....:90 ms
Max Flash Detect Time.....:500 ms
Switch&Release Call.....:Flash+1
Enable flash key or not.....:yes
Reject key.....:Flash+0
Switch call key.....:Flash+2
Three Party Call.....:Flash+3
Keep the hold call when onhook or not.....:no
# is quick dial key or not.....:no
Adterisk to be the function key or not.....:no
Tap Report.....:no
Escape Seq.....:no
CID Enable.....:yes
Enable Callee Inverse Polarity.....:no
Enable Caller Inverse Polarity.....:no
+-----+
|No. | ID |      Account Name      | Extension |Extention Type|
+-----+-----+-----+-----+-----+
| 0 | 1 |      Phone_001      | 700 | Intern/Extern|
+-----+-----+-----+-----+
| 1 | 2 |      Phone_002      | 701 | Intern/Extern|
+-----+-----+-----+-----+
->Enter the index to show(0-1)[0]:

Call Forwarding Unconditional.....:no
Call Forwarding When No Reply.....:yes
Transfer Call Number.....:701
Wait Time Long.....:0s
Call Forwarding On Busy.....:no
Phone Number.....:
Set to Instant Hotline.....:no
Delay Time.....:0s
CID Restriction.....:no
Enable No Disturb.....:no
Enable Call Waiting.....:yes
CID Enable.....:yes
CID Mode.....:FSK
Enable MWI.....:yes
->Show account extended srvice para continue or not?[yes]:n

```

Figure 4-135 Show User Supplementary

The command “set extended-server” configures the user supplementary parameter as below:

```

BG9002N#set extended-service

->Min Flash Detect Time<50-750>[90 ms]:80
->Max Flash Detect Time<80-1200>[500 ms]:400
->Switch&Release Call:Flash+<1-9>[1]:
->Enable flash key or not<yes/no>[yes]:
->Reject key:Flash+<0-9>[0]:
->Switch call key:Flash+<0-9>[2]:
->Three Party Call:Flash+<1-9>[3]:
->Keep the hold call when onhook or not[no]:
-># is quick dial key or not[no]:
->Adterisk to be the function key or not[no]:
->Tap Report[no]:
->Escape Seq[no]:
->CID Enable[yes]:
->Enable Callee Inverse Polarity[no]:
->Enable Caller Inverse Polarity[no]:
+-----+
|No. | ID | Account Name | Extension | Register Account | Register | Authen User |
+-----+-----+-----+-----+-----+-----+-----+
| 0 | 1 | Phone_001 | 700 | phone1 | no | phoneauth |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | 2 | Phone_002 | 701 | ghjfh | no | |
+-----+-----+-----+-----+-----+-----+-----+

->Enter the index to modify<0-1>[0]:
->Call Forwarding Unconditional<yes/no>[no]:
->Call Forwarding When No Reply<yes/no>[yes]:
->Transfer Call Number[701]:
->Wait Time Long<1-120>[0]:
->Call Forwarding On Busy<yes/no>[no]:
->Phone Number[]:
->Set to Instant Hotline<yes/no>[no]:
->Delay Time<0-10s>[0]:
->CID Restriction<yes/no>[no]:
->Enable Call Waiting<yes/no>[yes]:
->CID Enable[yes]:
->CID Enable<0-FSK,2-FXS+TYPE II>[0]:
->Enable MWI<yes/no>[yes]:
->Really want to modify? 'yes' or 'no'[yes]:

The configuration will take effect after saved and reloaded!

```

**Figure 4-136 Configure User Supplementary**

The following items are displayed on this screen:

- ▶ **Min Flash Detect Time:** The minimum time to detect the flash.
- ▶ **Max Flash Detect Time:** The maximum time to detect the flash.
- ▶ **Flash Key Enable:** Whether to enable digit detect after flash.
- ▶ **Switch&Release Call:** If the digit specified is detected after flash, terminate the active call and recover the call on hold.
- ▶ **Three Party Call:** If the digit specified is detected after flash, enter the conference mode.
- ▶ **Reject Key:** If the digit specified is detected after flash, reject the call on hold.
- ▶ **Switch Call Key:** If the digit specified is detected after flash, hold the active call and recover the call on hold.
- ▶ **Keep the hold call when onhook:** If selected, when hanging up in this context, the telephone rings

- to notify the user there is still a call on hold.
- ▶ **(#)Quick Dial Key:** Whether to send telephone number immediately after receiving the # key.
  - ▶ **Asterisk Func Key:** Whether to use the '\*' key as flash key.
  - ▶ **Tap Report:** Whether to report an event to server when flash detected.
  - ▶ **Escape Seq:** Whether to use an escape characters when sending special DTMF.
  - ▶ **CID Enable:** Whether to enable caller id globally.
  - ▶ **Callee Inverse Polarity:** Whether to activate the Polarity Reversal for FXS callee.
  - ▶ **Caller Inverse Polarity:** Whether to activate the Polarity Reversal for FXS caller.
  - ▶ **Call Forwarding Unconditional:** Enable or disable CFU function, if enabled, enter **Call Number**.
    - 1) Set by keypad service system: **\*57\*TN#**, TN is the phone number to be redirected to.
    - 2) Cancel by keypad service system: **#57#**.
  - ▶ **Call Forwarding No Reply:** Enable or disable CFNR, if enabled, enter **Call Number** and **Wait Time Long**.
    - 1) Set by keypad service system: **\*41\*TN#**, TN is the phone number to be redirected to.
    - 2) Cancel by keypad service system: **#41#**.
  - ▶ **Call Forwarding On Busy:** Enable or disable CFB function, if enabled, enter **Call Number**.
    - 1) Set by keypad service system: **\*40\*TN#**, TN is the phone number to be redirected to.
    - 2) Cancel by keypad service system: **#40#**.
  - ▶ **Hotline Number:** Enter number to hotline function, empty expressed disable.
    - 1) Set **delay hotline** number by Keypad service system: **\*52\*TN#**, TN is the hotline number.
    - 2) Cancel **delay hotline** number by Keypad service system: **#52#**.
    - 3) Set **instant hotline** number by Keypad service system: **\*42\*TN#**, TN is the hotline number.
    - 4) Cancel **instant hotline** number by Keypad service system: **#42\*EN#**, instant hotline can only be deactivated with other extension; EN is the extension number which needs to deactivate instant hotline.
  - ▶ **Delay Time:** Time 0 indicates immediate Hotline, Otherwise, indicates delay Hotline. The Delay Time must be configured on the WEB.
  - ▶ **CID Restriction:** Enable or disable CID Restriction. If **Anonymous As UserName** is chosen, user name content is Anonymous also.
  - ▶ **Enable No Disturb:** Allows block incoming calls at any time.
  - ▶ **Enable Call Waiting:** When you talking, a third party phone comes in, you can hear the beep tone.
  - ▶ **Enable MWI:** Enable or disable MWI (Message-waiting indicator) function.
  - ▶ **Enable CID:** Enable or disable to send CID to phone.
  - ▶ **CID Mode:** There are two methods used for sending caller ID information depending on the application and country specific requirements:
    - FSK:** caller ID generation using Frequency Shift Keying (FSK)
    - DTMF:** caller ID generation using DTMF signaling.

The command "show abbr-dial" shows the abbreviated number of the user as below:



```

BG9002N#show abbr-dial
+-----+-----+-----+-----+-----+-----+-----+-----+
|No. | ID | Account Name | Extension | Register Account | Register | Authen User |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 0 | 1 | Phone_001 | 700 | phone1 | yes | phoneauth |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | 2 | Phone_002 | 701 | ghjfh | no | |
+-----+-----+-----+-----+-----+-----+-----+-----+

->Enter the index to show<0-1>[0]:
+-----+-----+-----+-----+-----+-----+-----+-----+
|No. | ID | Phone Number | Abbreviated Number |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 0 | 1 | 1112 | 10 |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 2 | 3 | 3445 | 34 |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 3 | 4 | 8493 | 84 |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Figure 4-137 Show Abbreviated Number

The command “set abbr-dial” sets the abbreviated number of the user as below:

```

BG9002N#set abbr-dial
+-----+-----+-----+-----+-----+-----+-----+-----+
|No. | ID | Account Name | Extension | Register Account | Register | Authen User |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 0 | 1 | Phone_001 | 700 | phone1 | no | phoneauth |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | 2 | Phone_002 | 701 | ghjfh | no | |
+-----+-----+-----+-----+-----+-----+-----+-----+

->Enter the index to modify<0-1>[0]:
+-----+-----+-----+-----+-----+-----+-----+-----+
|No. | ID | Phone Number | Abbreviated Number |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 0 | 1 | 1112 | 10 |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 2 | 3 | 3445 | 34 |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 3 | 4 | 8493 | 84 |
+-----+-----+-----+-----+-----+-----+-----+-----+

->0-add,1-delete,2-modify[0]:
->Phone Number[]:23534534
->Abbreviated Number[]:23
->Really want to modify? 'yes' or 'no'[yes]:

Operate success!

The configuration will take effect after saved and reloaded!

```

Figure 4-138 Configure Abbreviated Number

The following items are displayed on this screen:

- **0-add,1-delete,2-modify:** Input “0” to add new abbreviated number item, input “1” to delete a abbreviated numbe from thelist, input “2” to modify one of the

abbreviated numbe from the list.

- **Abbreviated Number:** The abbreviated number.
- **Phone Number:** The Actual phone number.

The command “show whiteblack-list” shows the white list and the black list of the user as below:

```
BG9002N#show whiteblack-list
+-----+
|No. | ID | Account Name | Extension |Extention Type|
+-----+-----+-----+-----+-----+
| 0 | 1 | Phone_001 | 700 | Intern/Extern|
+-----+-----+-----+-----+-----+
| 1 | 2 | Phone_002 | 701 | Intern/Extern|
+-----+-----+-----+-----+-----+
->Enter the index to show(0-1)[0]:
+-----+
|No. | ID | List Type | Phone Number |
+-----+-----+-----+-----+
| 0 | 1 | Call In Black List| 1134|
+-----+-----+-----+-----+
| 1 | 2 | Call In Black List| 6678|
+-----+-----+-----+-----+
| 6 | 7 | Call In Black List| 566874|
+-----+-----+-----+-----+
| 7 | 8 | Call In Black List| 5566|
+-----+-----+-----+-----+
->Show account white or black list para continue or not?[yes]:n
```

**Figure 4-139 Show White & Black List**

The command “set whiteblack-list” configures the white list and the black list of the user as below:

```

BG9002N#set whiteblack-list
+-----+
|No. | ID | Account Name | Extension | Register Account | Register | Authen User |
+-----+-----+-----+-----+-----+-----+-----+
| 0 | 1 | Phone_001 | 700 | phone1 | yes | phoneauth |
+-----+-----+-----+-----+-----+-----+-----+
| 1 | 2 | Phone_002 | 701 | ghjfh | no | |
+-----+-----+-----+-----+-----+-----+-----+

->Enter the index to modify<0-1>[0]:
+-----+
|No. | ID | List Type | Phone Number |
+-----+-----+-----+-----+
| 0 | 1 | Call In Black List | 1134 |
+-----+-----+-----+-----+
| 1 | 2 | Call In Black List | 6678 |
+-----+-----+-----+-----+
| 6 | 7 | Call In Black List | 566874 |
+-----+-----+-----+-----+
| 7 | 8 | Call In Black List | 5566 |
+-----+-----+-----+-----+

->0-add,1-delete,2-modify[0]:
->List Type<
0-Call In Black List
1-Call In White List
2-Call Out Black List
3-Call Out White List>[0]:2
->Phone Number[]:453656
->->Really want to modify? 'yes' or 'no'[yes]:

Operate success!

The configuration will take effect after saved and reloaded?

->Set account white or black list para continue or not?[yes]:

```

**Figure 4-140 Configure White & Black List**

The following items are displayed on this screen:

- **List Type:** Choose type of Black&White List, four types are provided:  
**Incoming Blacklist, Incoming Whitelist, Outgoing Blacklist, Outgoing Whitelist.**
- **Phone Number:** the phone number or sip account.

#### 4.4.4 Codec Parameters

The command “show codec” shows the codec parameters as below:

```

BG9002N#show codec

G.711A Packet Period<10-90,degeress of 10>.....:20
G.711U Packet Period<10-90,degeress of 10>.....:20
G.723 Packet Period<10-90,degeress of 10>.....:30
G.729 Packet Period<10-90,degeress of 10>.....:20
+-----+
|No. | ID | Account Name | Fax Mode| Priority 1| Priority 2| Priority 3| Priority 4|
+-----+-----+-----+-----+-----+-----+-----+-----+
| 0 | 1 | Phone_001 | T38 | G.711A | G.711U | G.723 | G.729 |
+-----+-----+-----+-----+-----+-----+-----+-----+
| 1 | 2 | Phone_002 | TRANSFE | G.711A | G.711U | G.723 | G.729 |
+-----+-----+-----+-----+-----+-----+-----+-----+

```

Figure 4-141 Show Codec Parameters

The command “set codec” configures the codec parameters as below:

```

BG9002N#set codec
->G.711A Packet Period<10-90,degeress of 10>[20]:
->G.711U Packet Period<10-90,degeress of 10>[20]:
->G.723 Packet Period<10-90,degeress of 10>[30]:
->G.729 Packet Period<10-90,degeress of 10>[20]:30
-> Batch All Endpoint Codec 'yes' or 'no' [no]:
->Enter the index to modify<0-1>[0]:
->T38 Transfe Mode<0-TRANSFER,1-T38,2-VBD>[1]:
->Codec Answer Strategy<0-Use Offerer Priority,1-Use Answerer Priority>[0]:
->Codec First Priority<0-G.711A,1-G.711U,2-G.723,3-G.729>[0]:
->Codec Second Priority<0-G.711A,1-G.711U,2-G.723,3-G.729>[1]:
->Codec Third Priority<0-G.711A,1-G.711U,2-G.723,3-G.729>[2]:
->Codec Fourth Priority<0-G.711A,1-G.711U,2-G.723,3-G.729>[3]:
->Really want to modify? 'yes' or 'no' [yes]:

The configuration will take effect after saved and reloaded!

```

Figure 4-142 Configure Codec Parameters

- ▶ **G.711A Packet Period:** RTP packetization period of G.711A codec.
- ▶ **G.711u Packet Period:** RTP packetization period of G.711U codec.
- ▶ **G.723 Packet Period:** RTP packetization period of G.723 codec.
- ▶ **G.729 Packet Period:** RTP packetization period of G.729 codec.
- ▶ **Fax Mode:** Choose fax mode, three types are provided: **Transparent, T38, VBD.**
- ▶ **Codec Answer Strategy:** Two modes are provided:
  - Use Answerer Priority:** Codec selection decisions based on the priority level configuration
  - Use Offerer Priority:** Codec selection decision based on caller's priority.
- ▶ **Codec Priority:** If **Use Answerer Priority** is selected, set the priority of codec.

#### 4.4.5 DSP Parameters

The command “show dsp” shows DSP information as below:

```

BG9002N#show dsp

Echo Clear up or not.....:no
Silence Compress.....:no
Input Gain<-10-12db>.....:0
Ouput Gain<-10-12db>.....:0
Delay Level.....:delay large
DTMF Transfer Model.....:RFC2833
T38 Max FAX Rate.....:Unlimited
T38 FAX Signaling Reduncancy<0-7>.....:4
T38 FAX Data Redundancy<0-3>.....:0
Ring Frequency.....:25HZ
Impedance.....:600 Ohm
BG9002N#_

```

Figure 4-143 Show DSP Parameter

The command “set dsp” configures DSP parameters as below:

```

BG9002N#set dsp

->Echo Clear up or not[nol]:
->Silence Compress[nol]:y
->Input Gain<-10-12db>[0]:
->Ouput Gain<-10-12db>[0]:
  Delay Level:
  0-delay mininum
  1-delay smaller
  2-delay moderate
  3-delay large
  4-delay Maxinum
->Delay Level<0-4>[3]:
->DTMF Transfer Model<0-info,1-In-band,2-RFC2833>[0]:
  T38 Max FAX Rate:
  0-Unlimited
  1-2400bps
  2-4800bps
  3-7200bps
  4-9600bps
  5-12000bps
  6-14400bps
->T38 Max FAX Rate<0-6>[0]:
->T38 FAX Signaling Reduncancy<0-7>[4]:
->T38 FAX Data Redundancy<0-3>[0]:
->Ring Frequency<0-20HZ,1-25HZ>[1]:
->Impedance<0-600 Ohm,1-Ternary,2-Switzerland standard>[0]:1
->Really want to modify? 'yes' or 'no'[yes]:

  The configuration will take effect after saved and reloaded!

```

Figure 4-144 Configure DSP Parameters

The following items are displayed on this screen:

- ▶ **Echo Cancellation:** Enable or disable echo cancellation.
- ▶ **Silence Detection/Suppression:** Enable or disable silence detection and silence suppression.
- ▶ **Input Gain:** Configure the input gain value.
- ▶ **Output Gain:** Configure the input gain value
- ▶ **Delay Level:** Choose the delay level, five levels are provided: **Minimum**,

- ▶ **DTMF Transfer Model:** **Smaller, Moderate, Larger, Maximum.**  
Select DTMF transmission mode: **In-Band, INFO, RFC2833.**
- ▶ **RFC2833 Load Type:** If RFC2833 is selected, specify payload type of RFC2833.
- ▶ **T38 Max FAX Rate:** Select the maximum rate, when using T38 fax mode: **Unlimited, 2400bps, 4800bps, 7200bps, 9600bps, 12000bps, 14400bps.**
- ▶ **T38 Signaling Redundancy:** Configure the redundancy of T38 signal.
- ▶ **T38 Data Redundancy:** Configure the redundancy of T38 data.
- ▶ **Ring Frequency:** Choose the ring frequency: **20Hz, 25Hz.**
- ▶ **Impedance Type:** Choose the impedance type: **600Ω, China Standard, Switzerland Standard.**

#### 4.4.6 Digitmap

The command “show digitmap” shows digitmap information as below:

```
BG9002N#show digitmap

Enable Digitmap.....:no
Digitmap Short Timer S<1-30>.....:5s
Digit Map Content.....:xxxxxxx
BG9002N#
```

**Figure 4-145 Show Digit Map Parameter**

The command “set digitmap” configures digitmap parameters as below:

```
BG9002N#set digitmap

->Enable Digitmap[nol]:
->Digitmap Short Timer S<1-30>[5s]:
->Digit Map Content[xxxxxxx]:
->Really want to modify? 'yes' or 'no'[yes]:

The configuration will take effect after saved and reloaded!
```

**Figure 4-146 Configure Digit Map Parameter**

- ▶ **Enable:** Enable or disable digit map function.
- ▶ **Short Timer:** The time of Short Timer in second.
- ▶ **Digit Map:** The digit map rules.

#### 4.4.7 Signal Tone

The command “show tone” shows signal tone information as below:

```

BG9002N#show tone

Tone Type.....:China
Dial Tone User Define Enable.....:no
Dial tone frequency 1<100-2000HZ>.....:0
Dial tone frequency 2<100-2000HZ>.....:0
Busy Tone User Define Enable.....:no
Busy Tone Frequency1<100-2000HZ>.....:0
Busy Tone Frequency2<100-2000HZ>.....:0
On Time<100-10000ms>.....:500
Off Time<100-10000ms>.....:500
Ring Back Tone User Define Enable.....:yes
Ring Back Tone Frequency 1<100-2000HZ>.....:400
Ring Back Tone Frequency 2<100-2000HZ>.....:500
On Time<100-10000ms>.....:500
Off Time<100-10000ms>.....:500
Internal ring on time1(*100ms).....:10
Internal ring off time1(*100ms).....:40
Internal ring on time2(*100ms).....:0
Internal ring off time2(*100ms).....:0
External ring on time1(*100ms).....:10
External ring off time1(*100ms).....:40
External ring on time2(*100ms).....:0
External ring off time2(*100ms).....:0
BG9002N#

```

**Figure 4-147 Show Signal Tone Parameter**

The command “set tone” configures signal tone parameters as below:

```

BG9002N#set tone

0----China
1----Chile
2----Peru
3----America
4----Mexico
5----Telmex_Columbia
6----Switzerland
7----Other
->Tone Type(0-7)[0]:
->Dial Tone User Define Enable[no]:
->Dial tone frequency 1(100-2000HZ)[0]:
->Dial tone frequency 2(100-2000HZ)[0]:
->Busy Tone User Define Enable[no]:
->Busy Tone Frequency1(100-2000HZ)[0]:
->Busy Tone Frequency2(100-2000HZ)[0]:
->On Time(100-10000ms)[500]:
->Off Time(100-10000ms)[500]:
->Ring Back Tone User Define Enable[yes]:
->Ring Back Tone Frequency 1(100-2000HZ)[400]:
->Ring Back Tone Frequency 2(100-2000HZ)[500]:
->On Time(100-10000ms)[500]:
->Off Time(100-10000ms)[500]:
->Internal ring on time1(1-100)(*100ms)[10]:
->Internal ring off time1(1-100)(*100ms)[40]:
->Internal ring on time2(1-100)(*100ms)[0]:
->Internal ring off time2(1-100)(*100ms)[0]:
->External ring on time1(1-100)(*100ms)[10]:
->External ring off time1(1-100)(*100ms)[40]:
->External ring on time2(1-100)(*100ms)[0]:
->External ring off time2(1-100)(*100ms)[0]:
->Really want to modify? 'yes' or 'no'[yes]:

The configuration will take effect after saved and reloaded!

```

Figure 4-148 Configure Signal Tone Parameter

The following items are displayed on this screen:

- ▶ **Tone Type:** Select the type of signal tone.

#### Dial Tone

- ▶ **User Define Enable:** Whether to use user-defined dial tone frequency.
- ▶ **Dial Tone Frequency 1:**
- ▶ **Dial Tone Frequency 2:**

#### Busy Tone

- ▶ **User Define Enable:** Whether to use user-defined busy tone frequency.
- ▶ **Busy Tone Frequency 1:**
- ▶ **Busy Tone Frequency 2:**
- ▶ **On Time:**
- ▶ **Off Time:**

#### Ring Back Tone

- ▶ **User Define Enable:** Whether to use user-defined ringback tone frequency.



- Ring Back Tone Frequency 1:
- Ring Back Tone Frequency 2:
- On Time:
- Off Time:

**Distinction Ring:** Specify the ring cadence for the FXS port. In these fields, you specify the on and off pulses for the ring. The ring cadence that should be configured differs between internal call and external call.

#### 4.4.8 Centrex

The command “show inline” shows centrex information as below:

```
BG9002N#show inline

Enable Centrex.....:yes
+-----+
|NO. | ID |Group |Ring Policy|Time|
+-----+
| 0 | 1 | 700 | Alternate |30s |
+-----+
| 1 | 2 | 111 | Alternate |20s |
+-----+
| 2 | 3 | 4356 | Alternate |20s |
+-----+
+-----+
|NO. | Group | Telephone |
+-----+
| 0 | 700 | 4321 |
+-----+
| 0 | 700 | 700 |
+-----+
| 1 | 111 | 987 |
+-----+
| 2 | 4356 | 4545 |
+-----+
```

**Figure 4-149 Show Centrex Parameter**

The command “set inline” configures centrex parameters as below:

```

BG9002N#set inline
->Enable Centrex<yes/no>[yes]:
+-----+
!NO.  ! ID !Group !Ring Policy!Time!
+-----+
!  0  !  1  !  700 !  Alternate!30s !
+-----+
!  1  !  2  !  111 !  Alternate!20s !
+-----+
!  2  !  3  !  4356!  Alternate!20s !
+-----+
+-----+
!NO.  !  Group  ! Telephone  !
+-----+
!  0  !      700 !      4321 !
+-----+
!  0  !      700 !      700 !
+-----+
!  1  !      111 !      987 !
+-----+
!  2  !      4356!      4545 !
+-----+

->Ring Group:0-add,1-delete,2-modify[0]:
->Group Number[1]:701
->Ring Policy<0-Alternate,1-Ordinal,2-Parallel>[0]:
->Ring Time<5-90>[20]:
->Really want to modify? 'yes' or 'no'[yes]:
  Operate success!

->Set Group Member or not?[yes]:

->Ring Group Member:0-add,1-delete,2-modify[0]:
->Telephone number[1]:353543
->Really want to modify? 'yes' or 'no'[yes]:
  Operate success!

  The configuration will take effect after saved and reloaded!

```

**Figure 4-150 Configure Centrex Parameter**

The following items are displayed on this screen:

- ▶ **Enable Centrex:** Whether to enable centrex function globally.
- ▶ **Group Number:** The phone number of this ring group.
- ▶ **Ringing Policy:** Phone ringing policy: **Alternate**, **Ordinal**, **Parallel**.
- ▶ **Ring Time:** Ring time of each member.
- ▶ **Telephone Number:** The number will be added to the ring group.

#### 4.4.9 Phone Book

The command “show callroute” shows telephone book information as below:

```
BG9002N#show callroute
```

No.	Phone Prefix	Total Length	Prefix Mode	Modify Len	Modify Code
1	112	Unlimited	Normal	0	
2	435	Unlimited	Normal	0	

No.	IP/DOMAIN	Port	Description
1	138.0.60.3	5060	phoneroute
2	192.168.100.124	5060	phoneroute1

Figure 4-151 Show Phone Book Parameter

The command “set callroute” configures telephone book parameters as below:

```
BG9002N#set callroute
```

No.	Phone Prefix	Total Length	Prefix Mode	Modify Len	Modify Code
1	112	Unlimited	Normal	0	
2	435	Unlimited	Normal	0	

No.	IP/DOMAIN	Port	Description
1	138.0.60.3	5060	phoneroute
2	192.168.100.124	5060	phoneroute1

```

->Call Route:0-add,1-delete,2-modify[0]:
->Phone Prefix<length can't be zero>[1]:56756
->Total Length<0-32,0-unlimited><0-32>[0]:
->Description<length can't be zero>[1]:phoneroute2
->IP/DOMAIN[138.0.60.3]:192.168.100.106
->Input static-iptrunk port<1-65535>[5060]:
->Prefix Mode<0-Normal;1-Delete;2-add;3-modify>[0]:
->Really want to modify? 'yes' or 'no'[yes]:

Operate success!

The configuration will take effect after saved and reloaded!

```

Figure 4-152 Configure Phone Book Parameter

The following items are displayed on this screen:

- ▶ **Phone Prefix:** The prefix of this phone book.
- ▶ **Total Length:** The total length of number to wait before sending.
- ▶ **Prefix Mode:** Mode of processing number prefix: **Unmodify**, **Remove**, **Add**, **Modify**.
- ▶ **IP/Domain:** The IP address or domain of destination.
- ▶ **Port:** The port of destination.

► **Description:** Description of this rule.

#### 4.4.10 Save and Reload VOIP Parameter

VOIP parameter will take effect after save and reload commands:

```
BG9002N#save

  Save operation successful!

BG9002N#reload
Really want to modify? 'yes' or 'no'[yes]:
Voice parameter reload success!

BG9002N#
```

Figure 4-153 Save and Reload Parameter

## 4.5 System

### 4.5.1 Time Management

The command “show time-management” show the time management information as below:

```
BG9002N#show time-management

Enable NTP.....: Enable
NTP Service Mode.....: Client
Primary NTP Server.....: ntp.ucsd.edu
Secondary NTP Server.....: ntp.univ-lyon1.fr
Time Zone.....: -2
Update Interval.....: 3600
DST Config:
Enable DST.....: Enable
DST Offset(min): 0
DST Start At 1:00 on First Sunday in Jan.
DST End At 4:00 on Third Monday in Feb.

BG9002N#_
```

Figure 4-154 Show Time Management Information

The command “set time-management” configure the time management parameters as below.

```

BG9002N#set time-management
->Enable NTP? 'yes' or 'no'[yes]:
->NTP Service Mode<0-Client,1-Server And Client>[0]:
->Primary NTP Server[ntp.ucsd.edu]:
->Secondary NTP Server[ntp.univ-lyon1.fr]:
->Time Zone[-2]:
->Update Interval<60~36000s>[3600]:
->Enable Daylight Savings Time(DST)? 'yes' or 'no'[yes]:
->DST Offset<0-120min>[0]:
Start Time of DST:
->Month<1~12>[1]:
->Select Weekday:
    0-Sunday 1-Monday 2-Tuesday 3-Wednesday
    4-Thursday 5-Friday 6-Saturday
->Weekday<0~6>[0]:
->Select Order of Weekday in Month:
    1-First in Month 2-Second in Month 3-Third in Month
    4-Fourth in Month 5-Last in Month
->Order of Weekday in Month<1~5>[1]:
->Hour of Day<0~23>[0]:
End Time of DST:
->Month<1~12>[1]:
->Select Weekday:
    0-Sunday 1-Monday 2-Tuesday 3-Wednesday
    4-Thursday 5-Friday 6-Saturday
->Weekday<0~6>[0]:
->Select Order of Weekday in Month:
    1-First in Month 2-Second in Month 3-Third in Month
    4-Fourth in Month 5-Last in Month
->Order of Weekday in Month<1~5>[1]:
->Hour of Day<0~23>[0]:
Really want to modify? 'yes' or 'no'[yes]:
The configuration will take effect after saved and reset!

BG9002N#

```

**Figure 4-155 Configure Time Management Parameters**

The following items are displayed on this screen:

- ▶ **Enable NTP:** Enable or disable NTP.
- ▶ **Enable DST:** Enable or disable the Daylight Saving Time(DST).
- ▶ **DST Offset:** Enter the offset of DST.
- ▶ **Month:** Specify the month of DST, range from 1 to 12 in one year.
- ▶ **Weekday :** Specify the weekday of DST, range from Sunday to Saturday.
- ▶ **Order of Weekday in Month:** Specify the order of start weekday in the month from pull-down list as following:
  - **First in Month**
  - **Second in Month**
  - **Third in Month**
  - **Fourth in Month**
  - **Last in Month**
- ▶ **Hour of Day:** Specify the start hour of DST, range from 0 to 23 in one day.

### 4.5.2 Reboot System

Enter command "reset" to reset the device.

### 4.5.3 Backup/Restore

The command "load config" backup/restore the configurations as blow. Enter 0 to save current parameters as custom default configurations, Enter 1 to reset to custom default parameters, Enter 2 to reset to factory parameters.

```
BG9002N#load config
->Select Load config source<0-Default,1-FileSystem,2-Flash>[0]:
```

Figure 4-156 Backup/Restore Configurations

### 4.5.4 Diagnostic

#### 4.5.4.1 Ping

The command "ping" can used to check connectivity of your network in the following screen.

```
BG9002N#ping 192.168.100.182
->If Using Interface when ping 'yes' or 'no' [no]:
->Set ping packet size<0-65500>[56]:
->Set ping count<1-86400>[4]:
->If Using mark when ping 'yes' or 'no' [no]:
PING 192.168.100.182 (192.168.100.182): 56 data bytes
64 bytes from 192.168.100.182: seq=0 ttl=64 time=0.860 ms
64 bytes from 192.168.100.182: seq=1 ttl=64 time=1.260 ms
64 bytes from 192.168.100.182: seq=2 ttl=64 time=0.740 ms
64 bytes from 192.168.100.182: seq=3 ttl=64 time=0.740 ms

--- 192.168.100.182 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.740/0.900/1.260 ms

BG9002N#
```

Figure 4-157 PING Diagnostic

- ▶ **Ping:** Enter the IP Address or Domain Name of the PC whose connection you wish to diagnose.
- ▶ **Interface:** By selecting the interface, through this interface to send Echo Request messages.
- ▶ **Ping Packet Size:** Specifies the packet size of Echo Request messages sent.
- ▶ **Ping Count:** Specifies the number of Echo Request messages sent.

### 4.5.5 System Log

The command "show syslog" show the system log information as below:

```
BG9002N#show syslog
Log Level.....:INFO
Alarm Log.....:Enable
Login Log.....:Enable
Web Log.....:Enable
VoIP Log.....:Enable
Data Service Log.....:Enable
Others.....:Disable
Local Log Enable.....:Enable
Remote Log Enable.....:Disable
Syslog Log Address.....:/var/log/messages
BG9002N#
```

Figure 4-158 Show System Log Information

The command “set syslog” configure the system log parameters as below.

```
BG9002N#set syslog
0-EMERG
1-ALERT
2-CRIT
3-ERR
4-WARNING
5-NOTICE
6-INFO
7-DEBUG
->Select Log Level[6]:
Log Module Onoff:
->Alarm Log[yes]:
->Login Log[yes]:
->Web Log[yes]:
->VoIP Log[yes]:
->Data Service Log[yes]:
->Others[no]:
->Local Log Enable[yes]:
->Remote Log Enable[no]:
->Syslog Log Address[/var/log/messages]:
->Really want to modify? 'yes' or 'no'[yes]:
  Oprate success!
  The configuration will take effect after saved and reset!
BG9002N#
```

Figure 4-159 Configure System Log Parameters

The following items are displayed on this screen:

#### 4.5.6 TR069

The command “show tr069” show the tr069 information as below:

```

BG9002N#show tr069
Enable TR069.....: Enable
Enable TR069 SSL Encode.....: Disable
ACS Address.....: 10.250.0.10
ACS Server Name.....: ACS-server/ACS
ACS Port.....: 8080
Enable Single Account Mode.....: Enable
ACS Auth Username.....: acs
ACS Auth Password.....: acs
CPE Auth Username.....: cpe
CPE Auth Password.....: cpe
CPE Server Name.....: cpe
CPE Port.....: 8099
CPE Auth Enable.....: Disable
Enable Send Periodic Inform.....: Disable
Enable TR069 NAT.....: no
Root Device Type.....: InternetGatewayDevice
Custom Area.....: Switzerland
TR069 CPE User Agent.....: BG_TR69_CPE
Reboot System after Download.....: no
Non First Install.....: no
BG9002N#

```

Figure 4-160 Show TR069 Information

The command “set tr069” configure the tr069 parameters as below.

```

BG9002N#set tr069
->Enable TR069 'yes' or 'no' [yes]:
0 - China Mobile
1 - ShenZhen Telecom
2 - Switzerland
->Custom Area[2]:
->Enable TR069 SSL Encode 'yes' or 'no' [no]:
->ACS Address[10.250.0.10]:
->ACS Server Name[ACS-server/ACS]:
->ACS Port<1-65535>[8080]:
->ACS Auth Username[acs]:
->ACS Auth Password[acs]:
->CPE Auth Username[cpe]:
->CPE Auth Password[cpe]:
->CPE Server Name[cpe]:
->CPE Port<1-65535>[8099]:
->CPE Auth Enable 'yes' or 'no' [no]:
->Enable Send Periodic Inform 'yes' or 'no' [no]:
->Enable TR069 NAT 'yes' or 'no' [no]:
->TR069 CPE User Agent[BG_TR69_CPE]:
->Reboot System after Download 'yes' or 'no' [no]:
->Clean first install flag 'yes' or 'no' [no]:
->Are you sure save parameter? 'yes' or 'no' 'yes' or 'no' [yes]:
The configuration will take effect after saved and reset!
BG9002N#

```

Figure 4-161 Configure TR069 Parameters

The following items are displayed on this screen:

- ▶ **Serial Number:** The serial number of device. Read only.
- ▶ **Enable:** Enable or disable the TR069 function globally.



- ▶ **ACS Address:** Enter the IP address or domain name of ACS.
- ▶ **ACS Port:** Enter the port of ACS.
- ▶ **ACS Server Name:** Enter the TR069 server name of ACS.
- ▶ **SSL Enable:** Enable or disable the SSL(Secure Sockets Layer) for TR069.
- ▶ **Scheduler Send Inform:** Whether or not the CPE must periodically send CPE information to Server using the Inform method call. Enter the duration in seconds of the interval if enabled.
- ▶ **Single Account Enable:** Whether or not the TR069 Account is enabled.
- ▶ **TR069 Account:** Username used to authenticate the CPE when making a connection to the ACS.
- ▶ **TR069 password:** Password used to authenticate the CPE when making a connection to the ACS.
- ▶ **Connection Request Auth:** Whether to authenticate an ACS making a Connection Request to the CPE.
- ▶ **Connection Request Username:** Username used to authenticate an ACS making a Connection Request to the CPE.
- ▶ **Connection Request Password:** Password used to authenticate an ACS making a Connection Request to the CPE.
- ▶ **CPE Server Name:** A part of the HTTP URL for an ACS to make a Connection Request notification to the CPE. In the form: `http://host:port/path`
- ▶ **CPE Port:** A part of the HTTP URL for an ACS to make a Connection Request notification to the CPE. In the form: `http://host:port/path`
- ▶ **Status:** Connection Status when CPE making a connection to the ACS. Read only.
- ▶ **Fail Reason:** Show reason for the failure when CPE making a connection to the ACS. Read only.

#### 4.5.7 SNMP

The command “show snmp” show the snmp information as below:

```

BG9002N#show snmp
Enable Register Server.....: yes
Server Address or Domain.....: 138.0.60.2
Server Port.....: 162
Enable Double Register Server.....: no
TRAP Message Interval.....: 30s
Regional Identity.....: BG9002N
Device Identifier.....:
Discard Wrong Community Package.....: yes
Community Name.....: public
Registration Status.....: Register Failed
BG9002N#_

```

Figure 4-162 Show SNMP Information

The command “set snmp” configure the snmp parameters as below.

```

BG9002N#set snmp
->Enable Register Server 'yes' or 'no' [yes]:
->Server Address or Domain[138.0.60.2]:
->Server Port<1-65535>[162]:
->Enable Double Register Server 'yes' or 'no'[no]:
->TRAP Message Interval<30-3600s>[30]:
->Regional Identity[BG9002N]:
->Device Identifier[]:
->Enable Performance Statistics Upload'yes'or'no'[no]:
->Enable control when snmp register fail'yes'or'no'[yes]:
->Discard Wrong Community Package<yes/no>[yes]:
->Community Name[public]:
->Really want to modify? 'yes' or 'no'[yes]:

    The configuration will take effect after saved and reset!

BG9002N#
  
```

**Figure 4-163 Configure SNMP Parameters**

The following items are displayed on this screen:

- |   |  |
|---|--|
| ▶ <b>Register Enable:</b>                 | Check this box to enable SNMP register.                        |
| ▶ <b>Server Address or Domain:</b>        | Enter the IP address or domain name of register server.        |
| ▶ <b>Server Port:</b>                     | Enter the port of Register Server.                             |
| ▶ <b>TRAP Message Interval:</b>           | Set the sending interval between TRAP messages.                |
| ▶ <b>Regional Identity:</b>               | Set the identity of regional.                                  |
| ▶ <b>Device Identifier:</b>               | Set the identifier of device.                                  |
| ▶ <b>Enable Double Register Server:</b>   | Check this box to enable backup Register Server.               |
| ▶ <b>Backup Server Address or Domain:</b> | Enter the IP Address or Domain Name of Backup Register Server. |
| ▶ <b>Backup Server Port:</b>              | Enter the port of Backup Register Server.                      |
| ▶ <b>Registration Status:</b>             | The status of registration. Read only.                         |