BG9008W

User Manual

Guangzhou Gaoke Communications Technology Co., LTD.

BG9008W

User Manual

Version: BG9008W-13-12-100

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

Guangzhou Gaoke Communications Technology Co., LTD.

Address: GaoKe Science Park, No.168 Gaopu Road, Guangzhou, P.R.C
Tel: Central: +86-20-82598555 Customer services: +86-20-82598191
Fax: +86-20-82598121 +86-20-82599989
P.C.: 510663
Website: www.gktel.cn
E-mail: info@gktel.com.cn

Copyright

Disclaimer

Guangzhou Gaoke Communications Technology Company Limited 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 BG9008W 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 BG9008W unit.

Chapter 1: Provides an overview of BG9008W

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.
host(italic)	Indicates user specified parameters. e.g. for command: tftp *host* {get | put} {sys | cfg} *filename* The *host* and *filename* 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

1 Overview

A new series of ALL IN ONE INTELLIGENT Gateway BG9008W 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 IP PBX features are built in. Comparing with other Voice equipments, BG9008W 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 BG9008W has includes Ethernet, Optical and 3G.

2 Product Introduction

2.1 Appearance

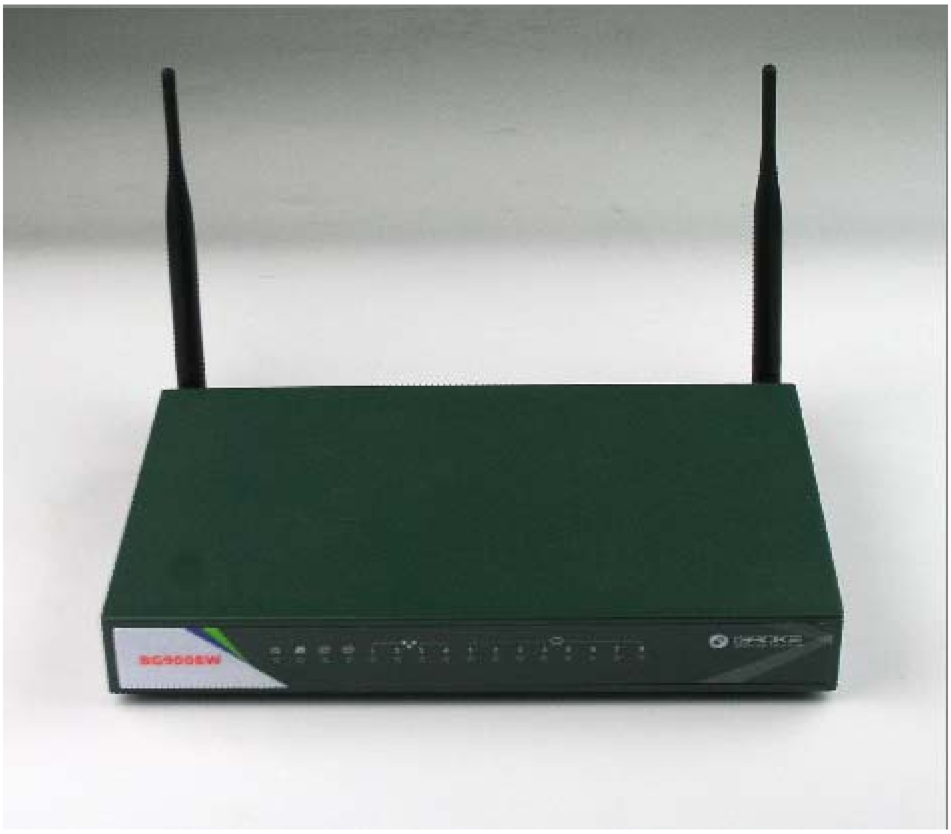


Figure 2-1 BG9008W Front View

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

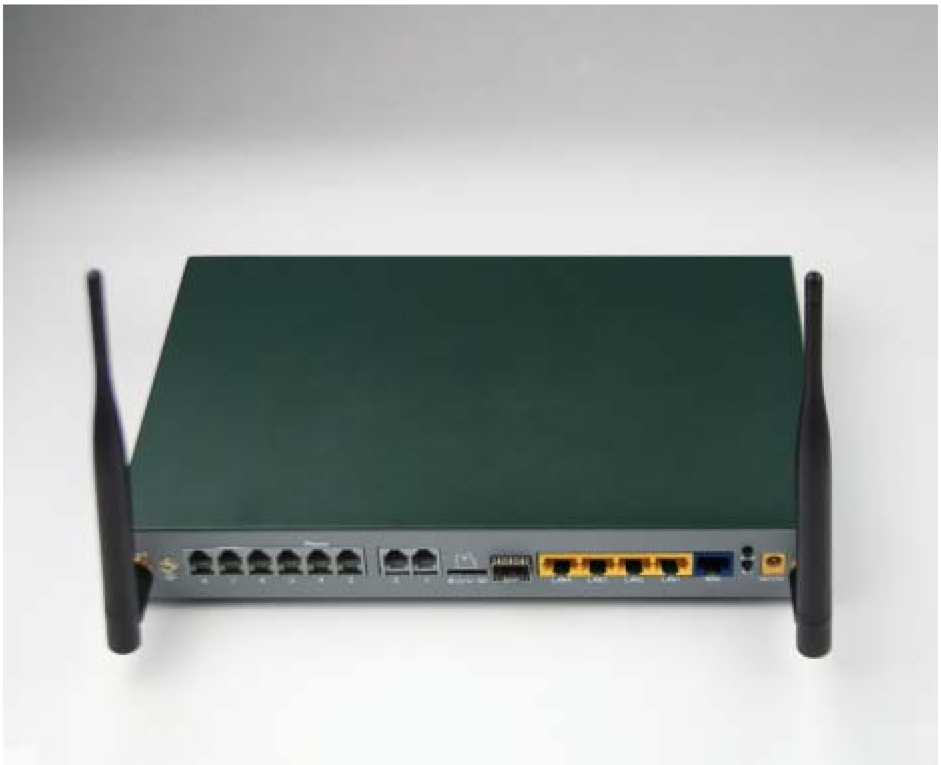


Figure 2-2 BG9008W Rear View

- WAN: 1000/100/10Mpbs ethernet ports.
- LAN(N): 1000/100/10Mpbs 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	2 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

IP PBX Functions List

- Call Forwarding on Busy
- Call Forwarding No Answer
- Call Forwarding Unconditional
- Call Forwarding Unregistered
- Caller ID
- Call Waiting/Call Holding/Call Transfer

- Call Pickup
- Three-way Calling
- Conference
- Ring groups
- Check phone number
- Time lock
- Auto attendant
- DISA
- Voicemail
- Call Restriction
- Color Ring
- Blacklist & Whitelist
- Alarm Clock
- Do Not Disturb (DND)
- Hotline
- Recording
- Call Back on Busy
- Centrex
- Abbreviated Dialing
- Ring Test
- Time Report

USB storage/Print

- Support USB storage
- Support print sharing

2.4 Working Environment

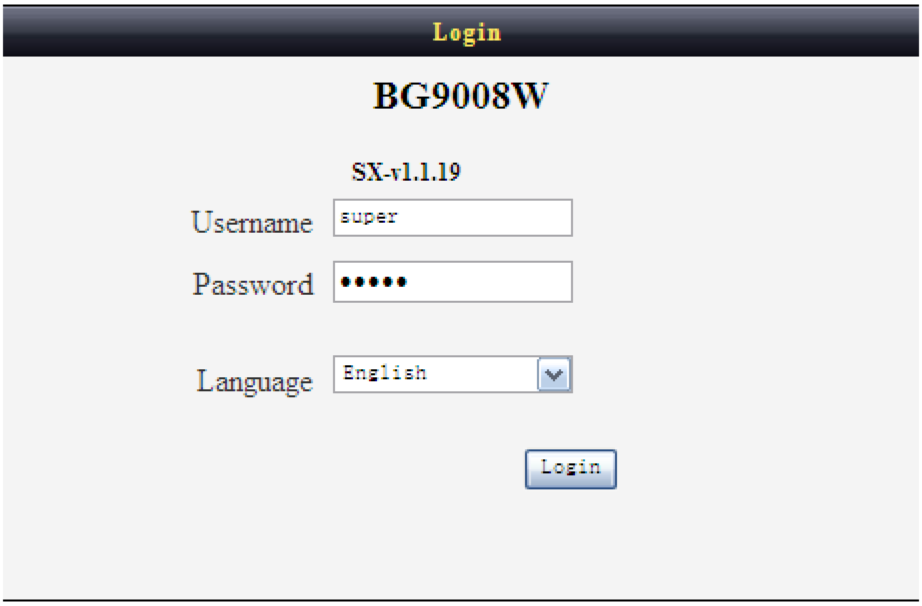
Environment requirement includes storage temperature, working temperature and humidity.

- Storage Temperature: -40ºC - 70ºC
- Long Time Working Temperature: -10ºC - 50ºC
- Short Time Working Temperature: -15ºC - 60ºC
- 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.



Login

BG9008W

SX-v1.1.19

Username: super

Password: •••••

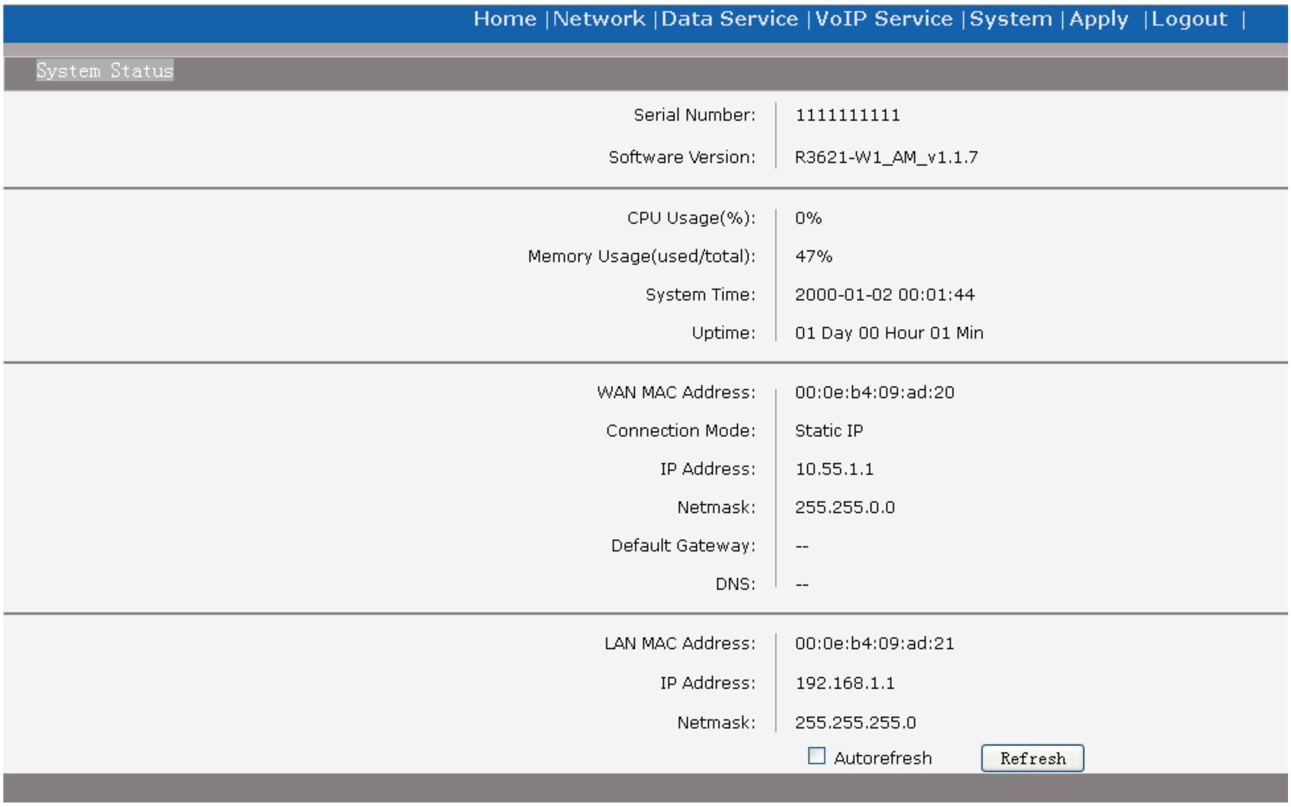
Language: English

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
□ Autorefresh
Refresh

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

Figure 3-2 System Status

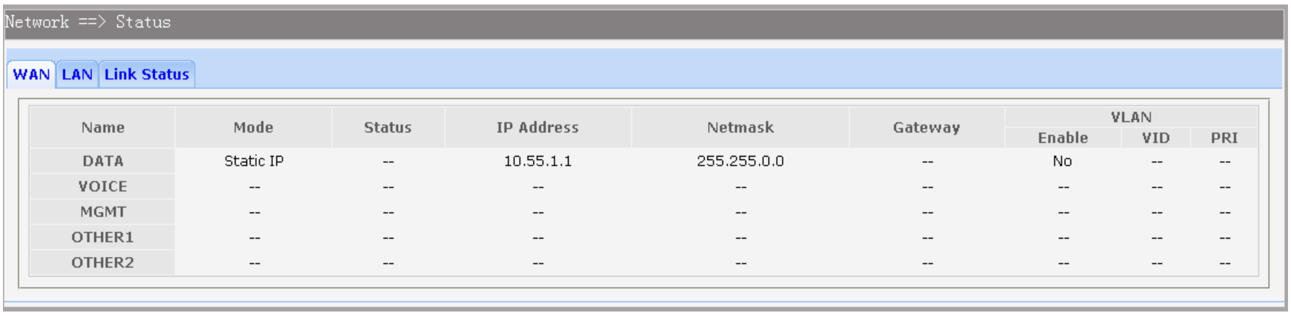
3.3 Network Configuration

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.

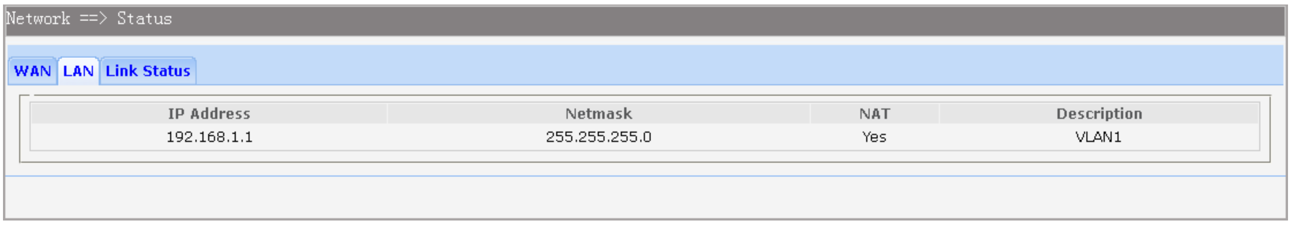


Name	Mode	Status	IP Address	Netmask	Gateway	VLAN		
						Enable	VID	PRI
DATA	Static IP	--	10.55.1.1	255.255.0.0	--	No	--	--
VOICE	--	--	--	--	--	--	--	--
MGMT	--	--	--	--	--	--	--	--
OTHER1	--	--	--	--	--	--	--	--
OTHER2	--	--	--	--	--	--	--	--

Figure 3-3 WAN Status

3.3.1.2 LAN Status

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

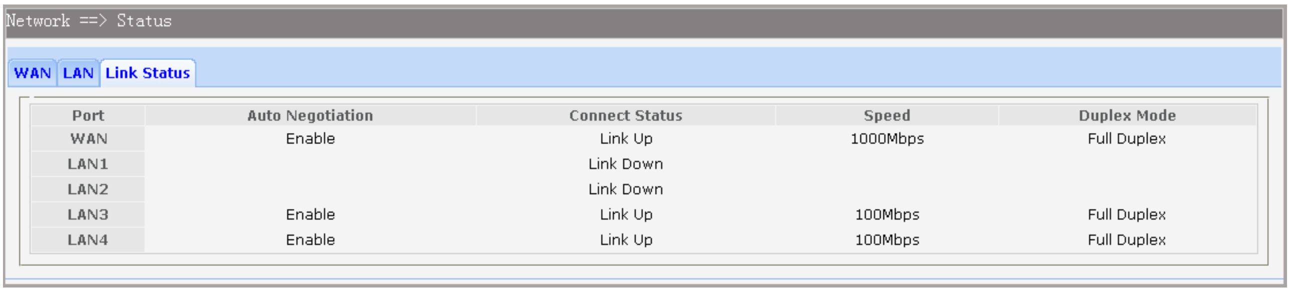


IP Address	Netmask	NAT	Description
192.168.1.1	255.255.255.0	Yes	VLAN1

Figure 3-4 LAN Status

3.3.1.3 Link Status

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



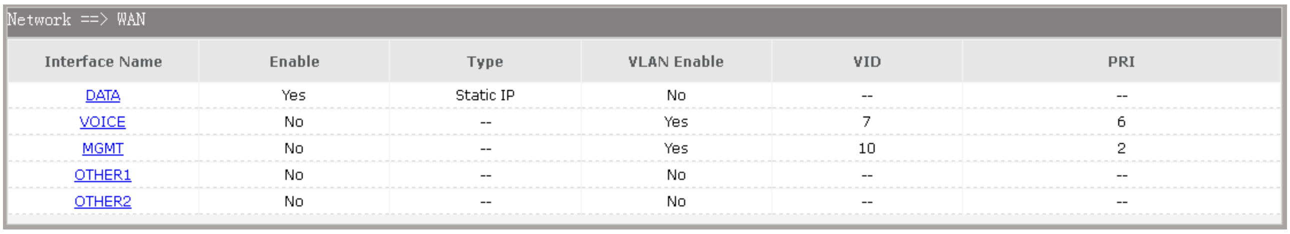
Port	Auto Negotiation	Connect Status	Speed	Duplex Mode
WAN	Enable	Link Up	1000Mbps	Full Duplex
LAN1		Link Down		
LAN2		Link Down		
LAN3	Enable	Link Up	100Mbps	Full Duplex
LAN4	Enable	Link Up	100Mbps	Full Duplex

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.



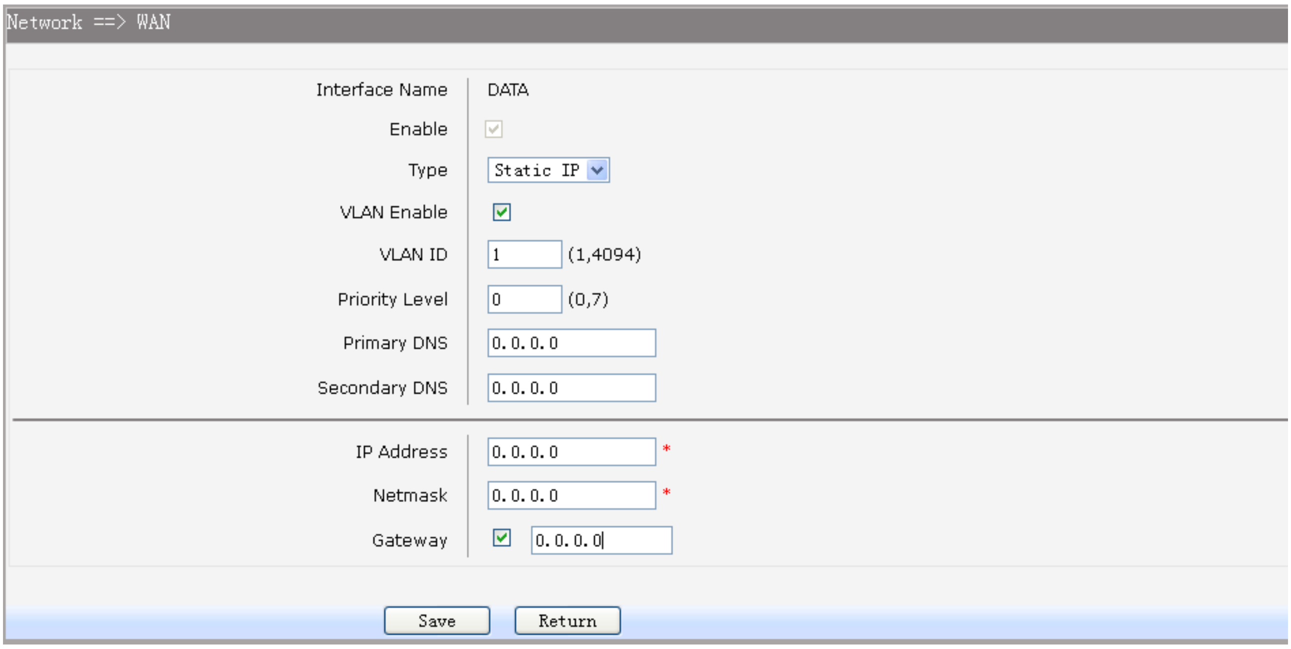
Interface Name	Enable	Type	VLAN Enable	VID	PRI
DATA	Yes	Static IP	No	--	--
VOICE	No	--	Yes	7	6
MGMT	No	--	Yes	10	2
OTHER1	No	--	No	--	--
OTHER2	No	--	No	--	--

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	☑
Type	Static IP
VLAN Enable	☑
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	☑ 0.0.0.0

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.

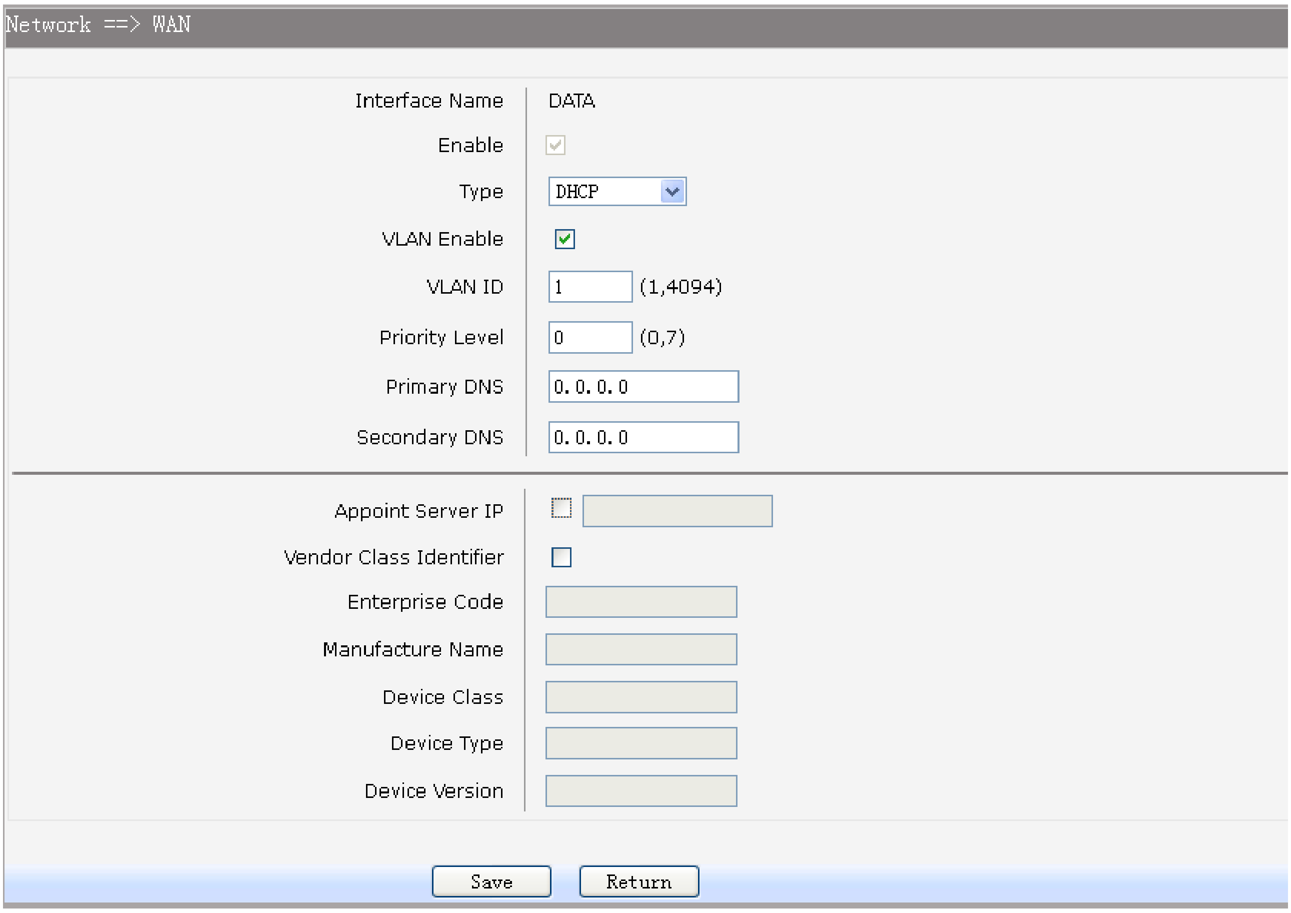
► **IP Address:** Enter the IP address assigned by your ISP. If you are not clear, please consult your ISP.

► **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.



Network ==> WAN

Interface Name	DATA
Enable	☑
Type	DHCP
VLAN Enable	☑
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	□
Vendor Class Identifier	□
Enterprise Code	
Manufacture Name	
Device Class	
Device Type	
Device Version	

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.

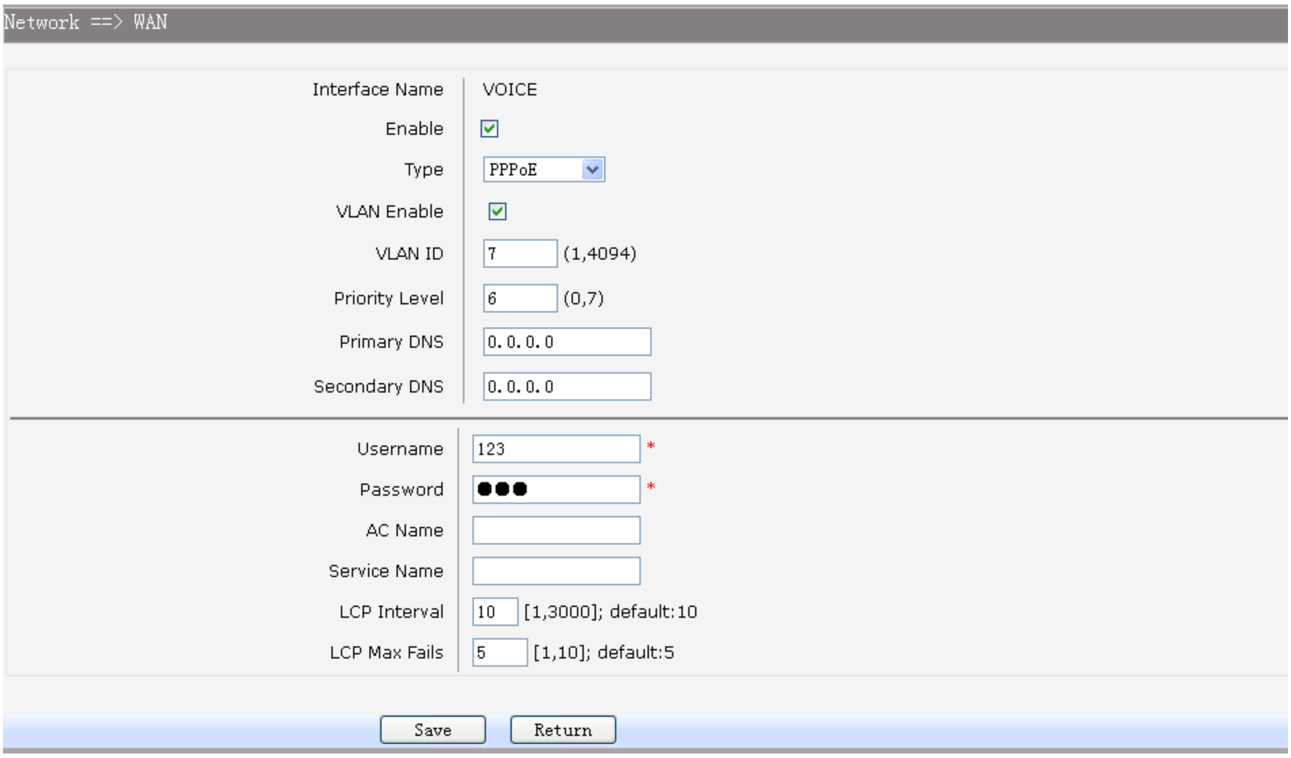
► **Device Class:** Optional.

► **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	☑
Type	PPPoE
VLAN Enable	☑
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

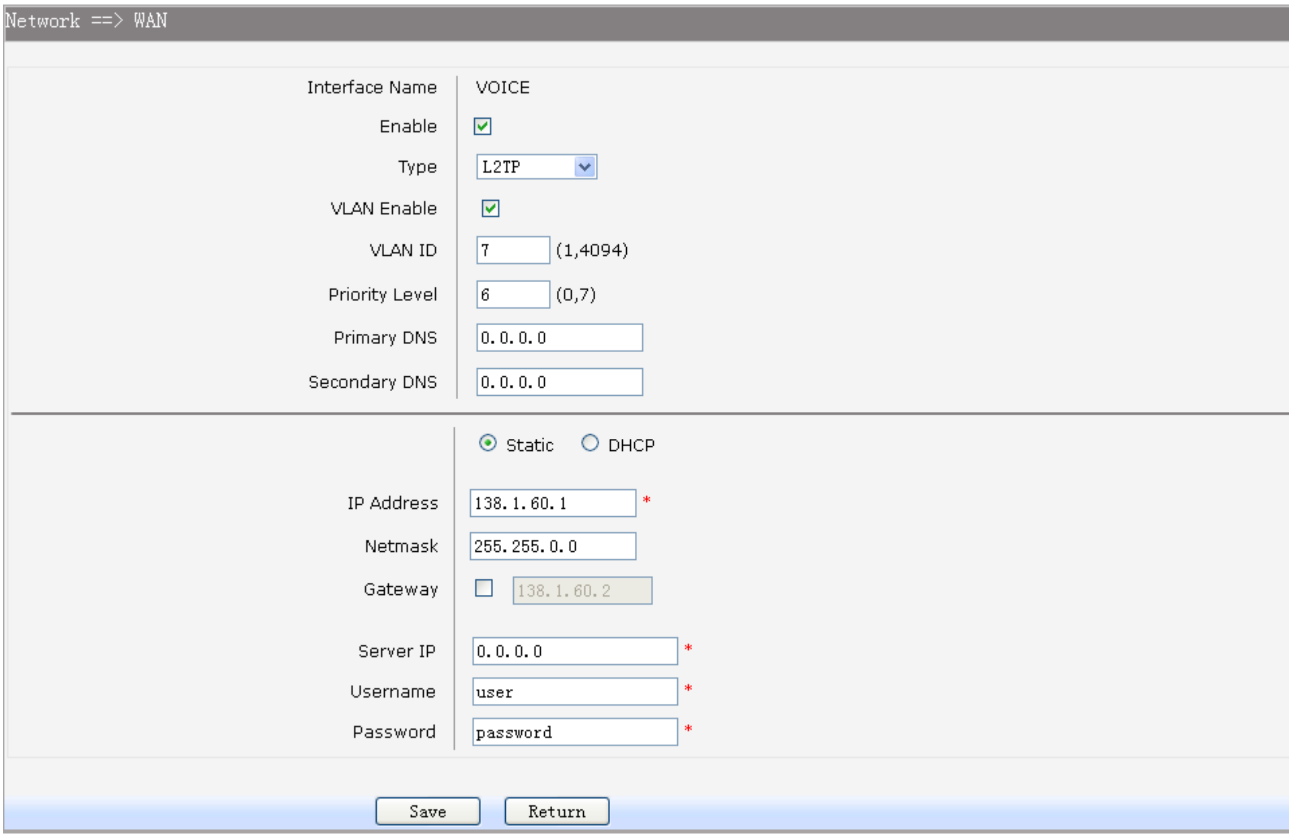
Figure 3-9 WAN-PPPoE

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.



Network ==> WAN

Interface Name	VOICE
Enable	☑
Type	L2TP
VLAN Enable	☑
VLAN ID	7 (1,4094)
Priority Level	6 (0,7)
Primary DNS	0.0.0.0
Secondary DNS	0.0.0.0
	● Static ○ DHCP
IP Address	138.1.60.1 *
Netmask	255.255.0.0
Gateway	□ 138.1.60.2
Server IP	0.0.0.0 *
Username	user *
Password	password *

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:

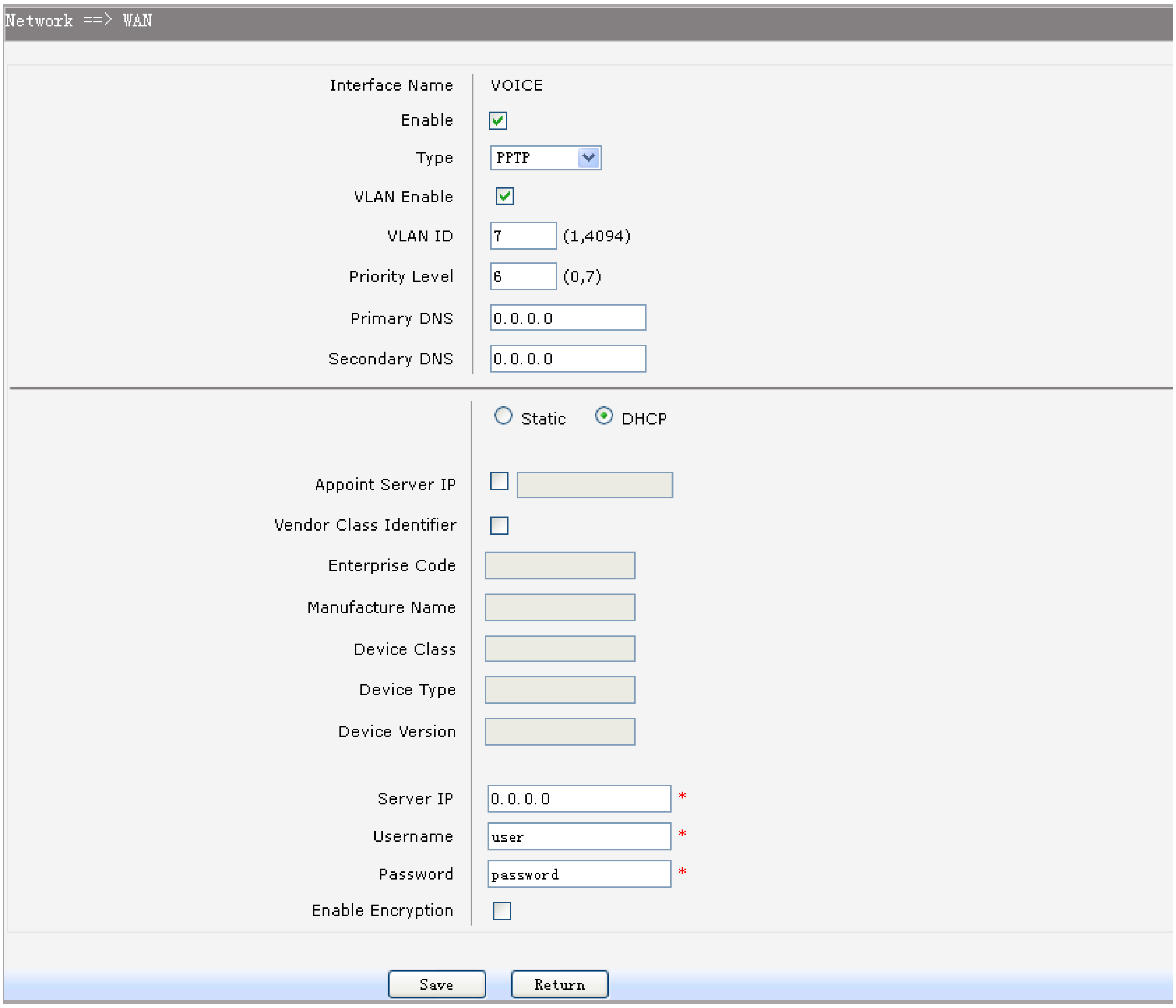
- ► **Appoint Server IP:** Optional. If network has multiple DHCP servers, enter the IP address of your ISP's DHCP server.
- ► **Vendor Class Identifier:** Optional. This option (60) is used by DHCP clients to optionally identify the

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 ☑
Type PPTP
VLAN Enable ☑
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 □
Vendor Class Identifier □
Enterprise Code
Manufacture Name
Device Class
Device Type
Device Version

Server IP 0.0.0.0 *
Username user *
Password password *
Enable Encryption □

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.

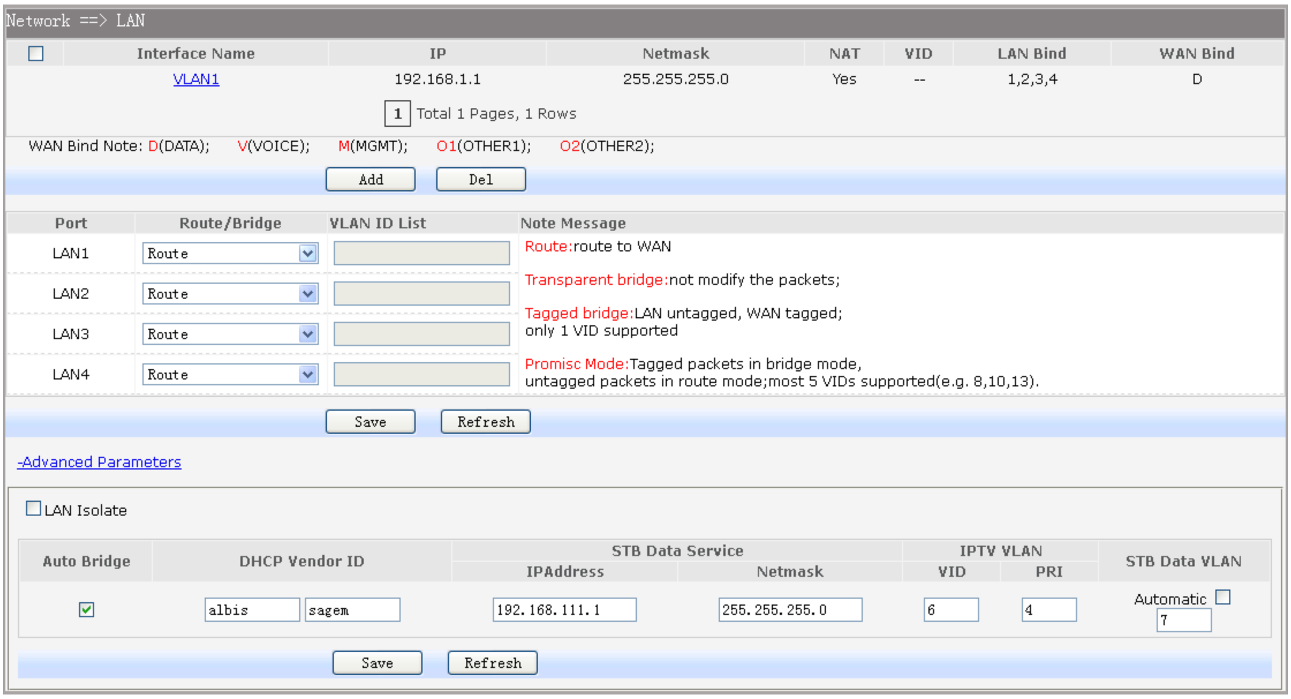
► **Device Type:** Optional.

► **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

☐	Interface Name	IP	Netmask	NAT	VID	LAN Bind	WAN Bind
	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

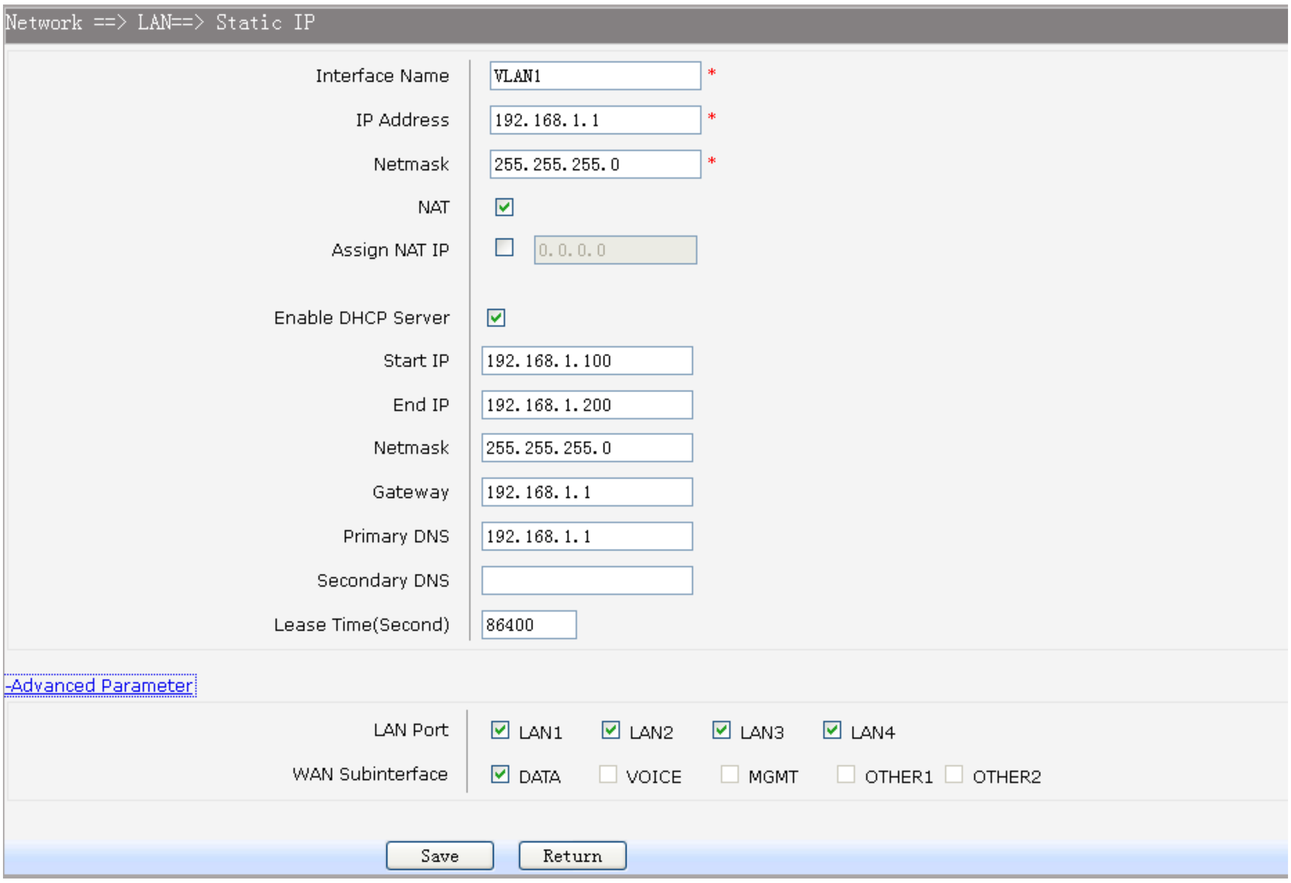
Auto Bridge	DHCP Vendor ID	STB Data Service		IPTV VLAN		STB Data VLAN
		IPAddress	Netmask	VID	PRI	
☑	albis sagem	192.168.111.1	255.255.255.0	6	4	Automatic ☐ 7

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.

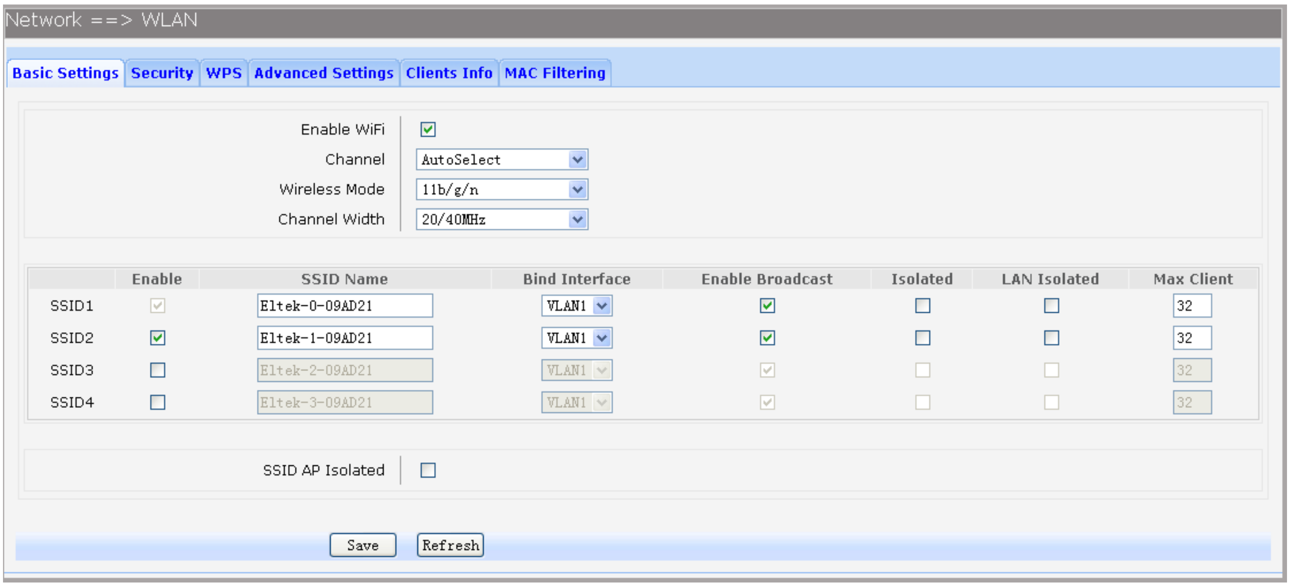
- ► **LAN Isolate:** Check the box to prohibit the access between LAN interfaces.
- ► **Auto Bridge:** Check the box to dynamically create IPTV bridge for STB.
- ► **DHCP Vendor ID:** Vendor class identifier List (DHCP 60 option), support at most two vendor IDs.
- ► **IPAddress:** IP address of interface 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 WiFi ☑
Channel AutoSelect
Wireless Mode 11b/g/n
Channel Width 20/40MHz

	Enable	SSID Name	Bind Interface	Enable Broadcast	Isolated	LAN Isolated	Max Client
SSID1	☑	Eltek-0-09AD21	VLAN1	☑	☐	☐	32
SSID2	☑	Eltek-1-09AD21	VLAN1	☑	☐	☐	32
SSID3	☐	Eltek-2-09AD21	VLAN1	☑	☐	☐	32
SSID4	☐	Eltek-3-09AD21	VLAN1	☑	☐	☐	32

SSID AP Isolated ☐

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. BG9008W 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.

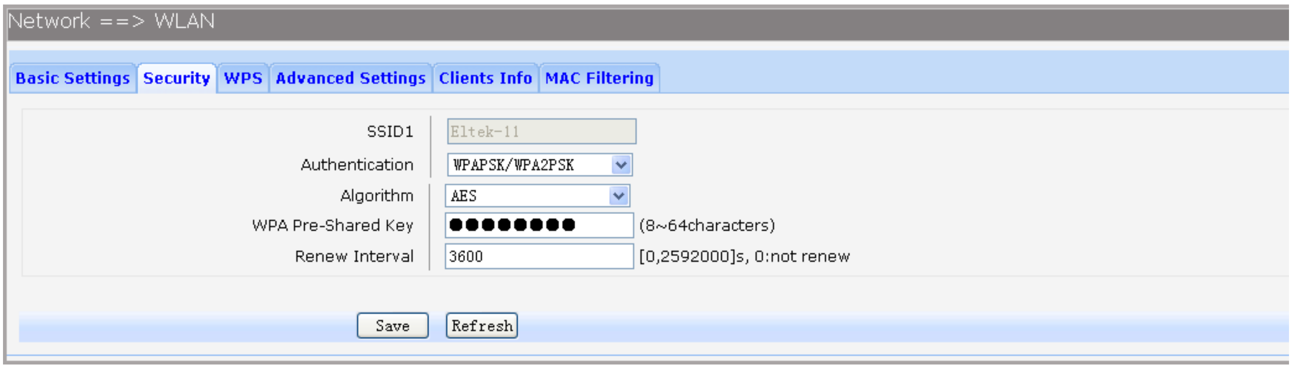
► **SSID AP Isolated:** This function can isolate wireless stations on your network from each other. Wireless devices will be able to communicate with the Router but not with each other. To use this function, check this box. AP Isolation is disabled by default.

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.



SSID1: Eltek-11
Authentication: WPAPSK/WPA2PSK
Algorithm: AES
WPA Pre-Shared Key: ●●●●●●●●● (8~64characters)
Renew Interval: 3600 [0,2592000]s, 0:not renew

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

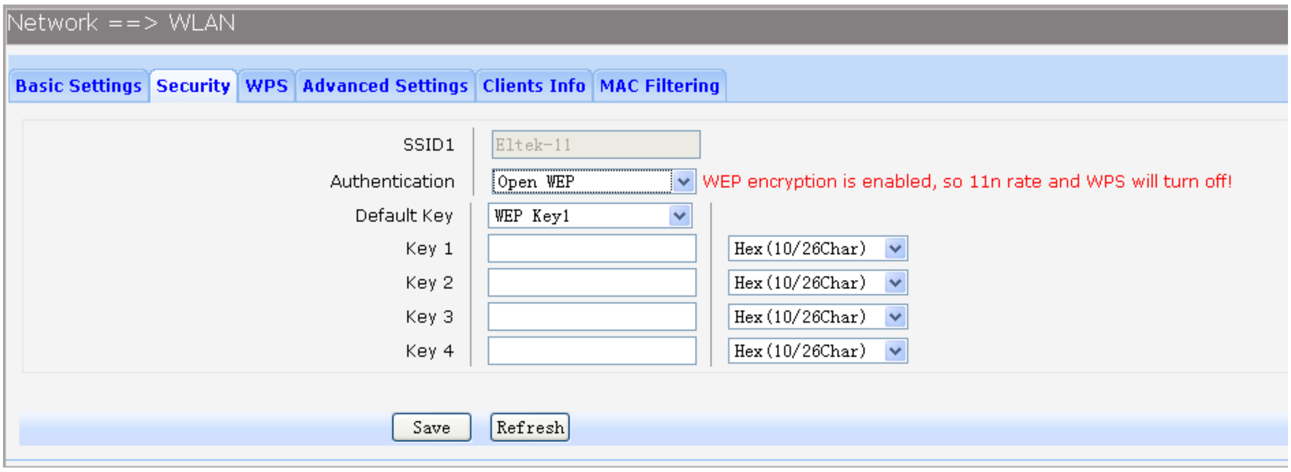
► **Authentication:** The authentication type selected: WPA-PSK, WPA2-PSK, WPAPSK/WPA2PSK.

► **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.



SSID1: Eltek-11

Authentication: Open WEP — WEP encryption is enabled, so 11n rate and WPS will turn off!

Default Key: WEP Key1

Key 1: Hex(10/26Char)

Key 2: Hex(10/26Char)

Key 3: Hex(10/26Char)

Key 4: Hex(10/26Char)

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.

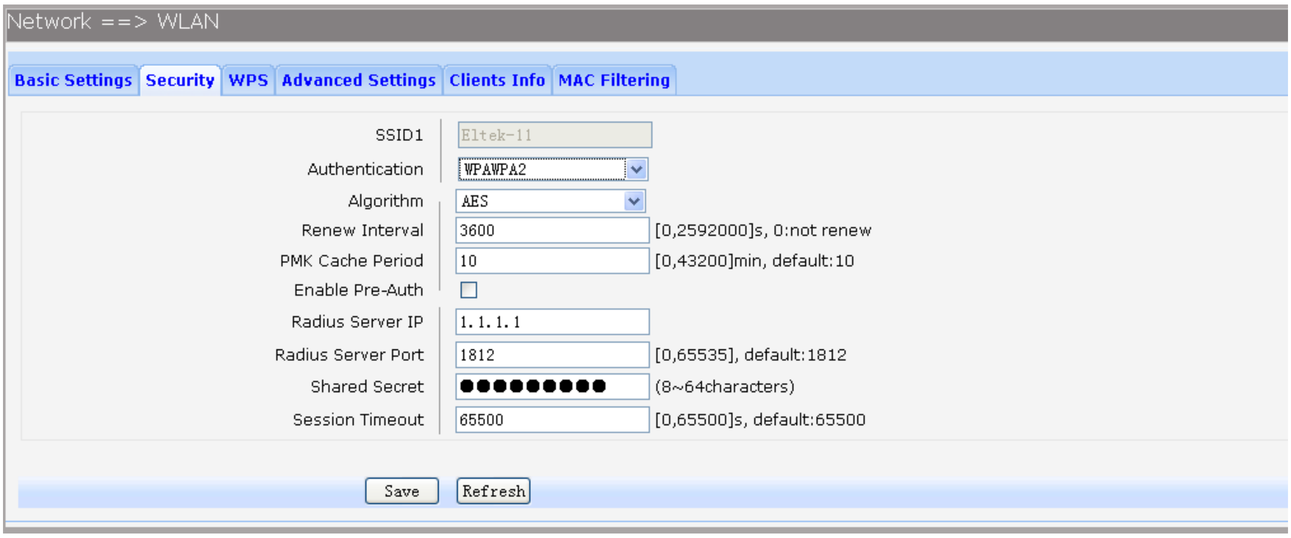
► **Default Key:** Select the default WEP key configure below.

► **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.



SSID1: Eltek-11

Authentication: WPAWPA2

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

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.

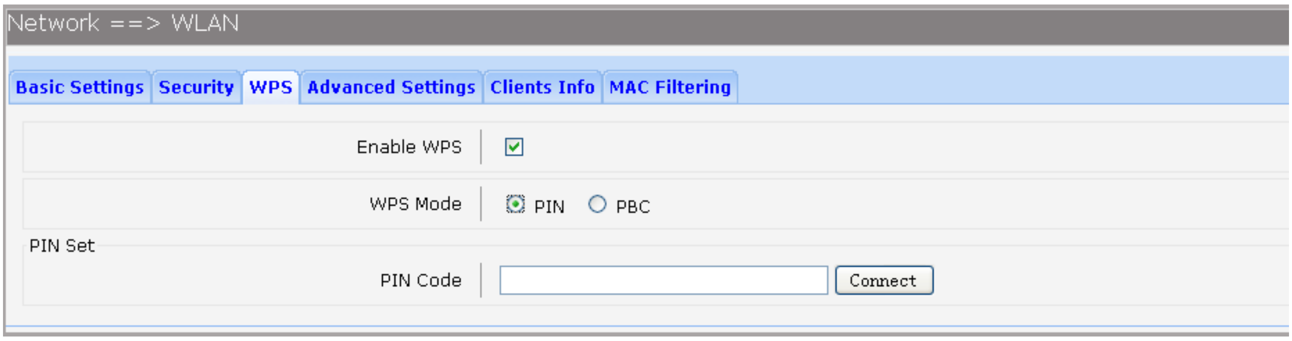
The **PIN** method involves entering a client device PIN, obtained either from a client application GUI or a label on a device, into the appropriate admin screen on a Registrar device.

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.



Network ==> WLAN

Enable WPS ☑

WPS Mode ● PIN ○ PBC

PIN Set

PIN Code

Figure 3-18 Configure WIFI WPS-PIN

The following items are displayed on this screen:

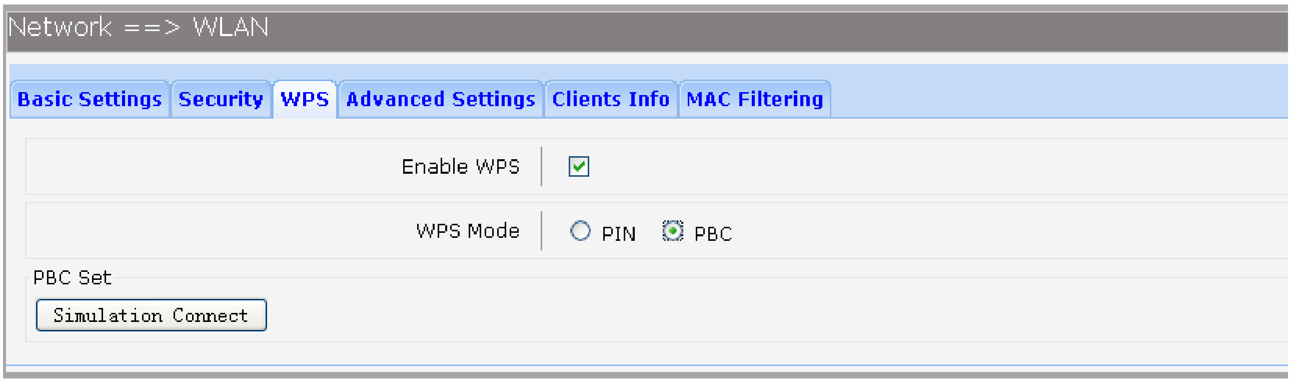
► **Enable WPS:** Enable or disable the WIFI WPS function globally.

► **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.



Network ==> WLAN

Enable WPS ☑

WPS Mode ○ PIN ● PBC

PBC Set

Figure 3-19 Configure WIFI WPS-PBC

The following items are displayed on this screen:

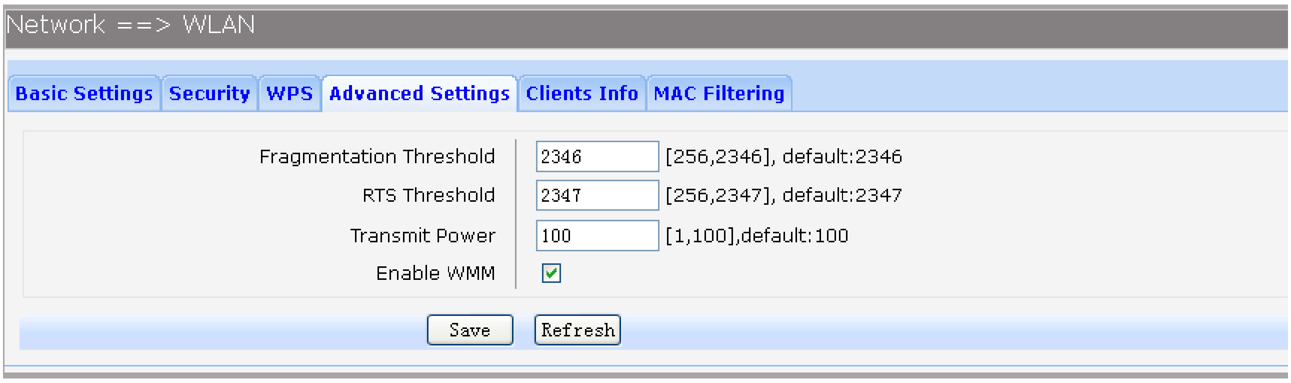
► **Enable WPS:** Enable or disable the WIFI WPS function globally.

► **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.



Network ==> WLAN

Fragmentation Threshold 2346 [256,2346], default:2346

RTS Threshold 2347 [256,2347], default:2347

Transmit Power 100 [1,100],default:100

Enable WMM ☑

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.

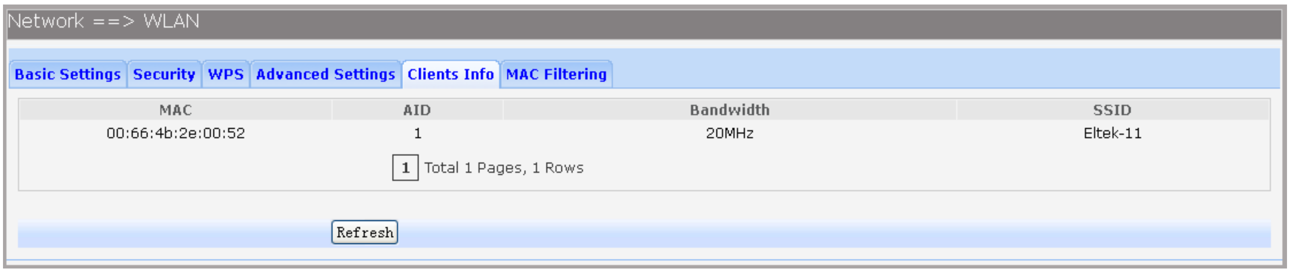
► **RTS Threshold:** Here you can specify the RTS (Request to Send) Threshold. If the packet is larger than the specified RTS Threshold size, the device will send RTS frames to a particular receiving station and negotiate the sending of a data frame. The default value is 2347.

► **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.



Network ==> WLAN

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

1 Total 1 Pages, 1 Rows

Figure 3-21 View Wifi Clients Info

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

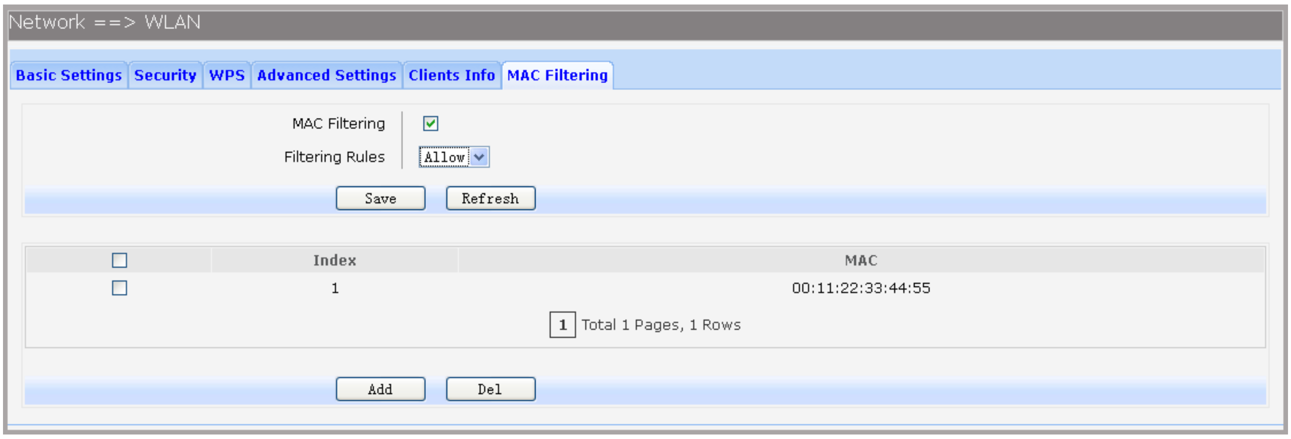
The following items are displayed on this screen:

- ► **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

MAC Filtering ☑

Filtering Rules Allow

□	Index	MAC
□	1	00:11:22:33:44:55

1 Total 1 Pages, 1 Rows

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.

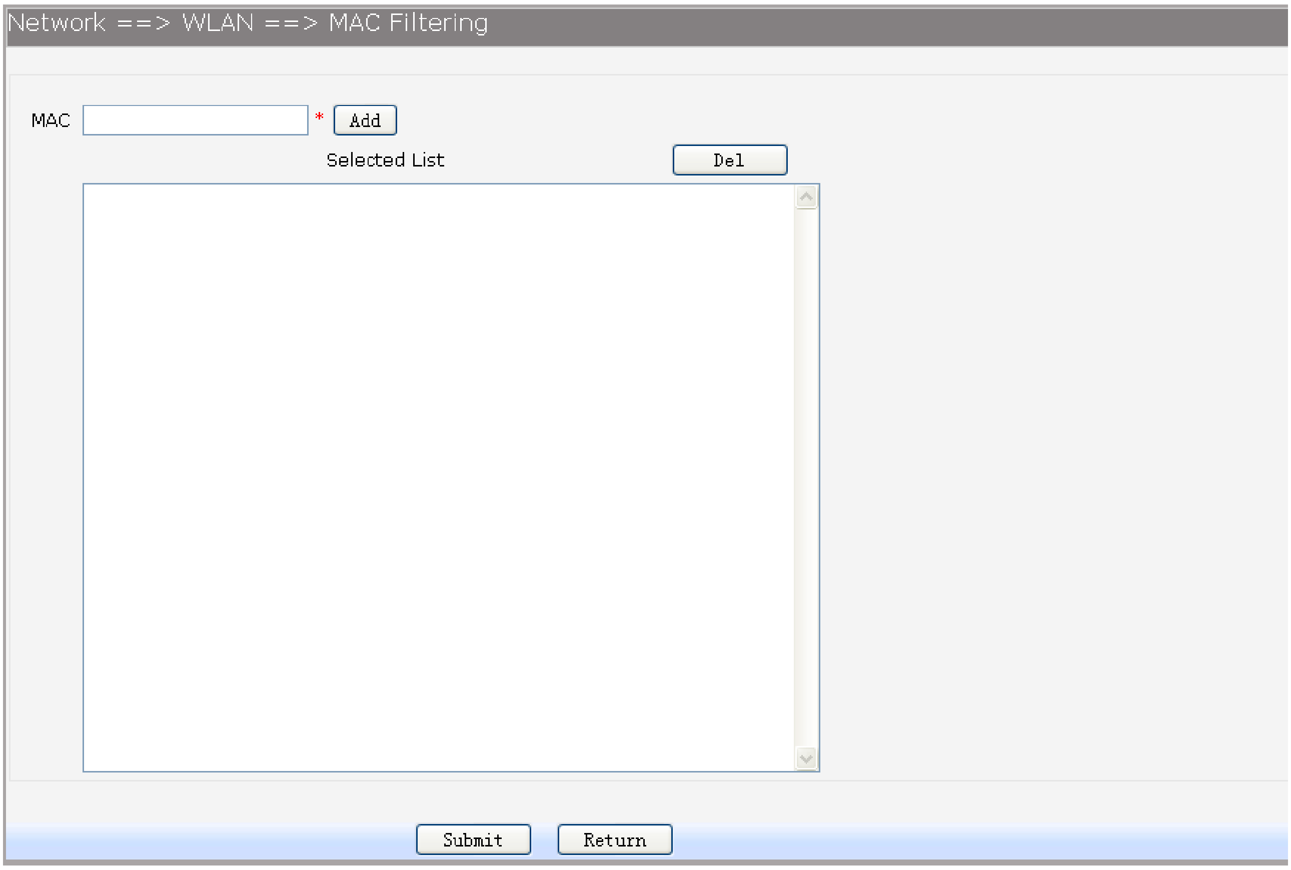


Figure 3-23 Add WIFI MAC Filtering Entry

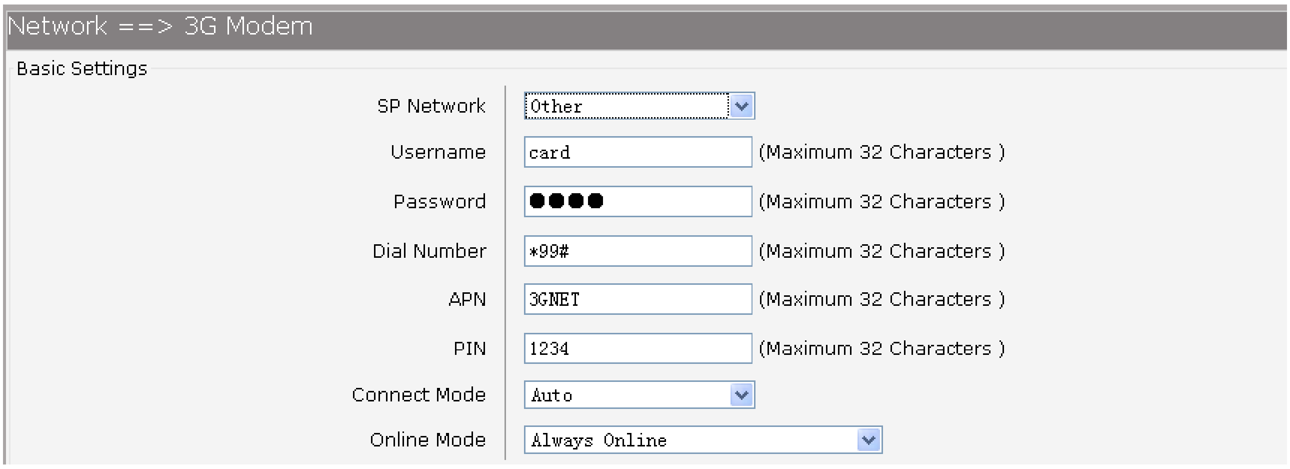
Enter the appropriate MAC Address into the **MAC** field. The format of the MAC Address is XX:XX:XX:XX:XX:XX (X is any hexadecimal digit). Click **Add** button to add MAC address to the **Selected List,** click **Del** button to delete the selected MAC address in the **Selected List.**

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.



Network ==> 3G Modem

Basic Settings

SP Network	Other	
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	
Online Mode	Always Online	

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.

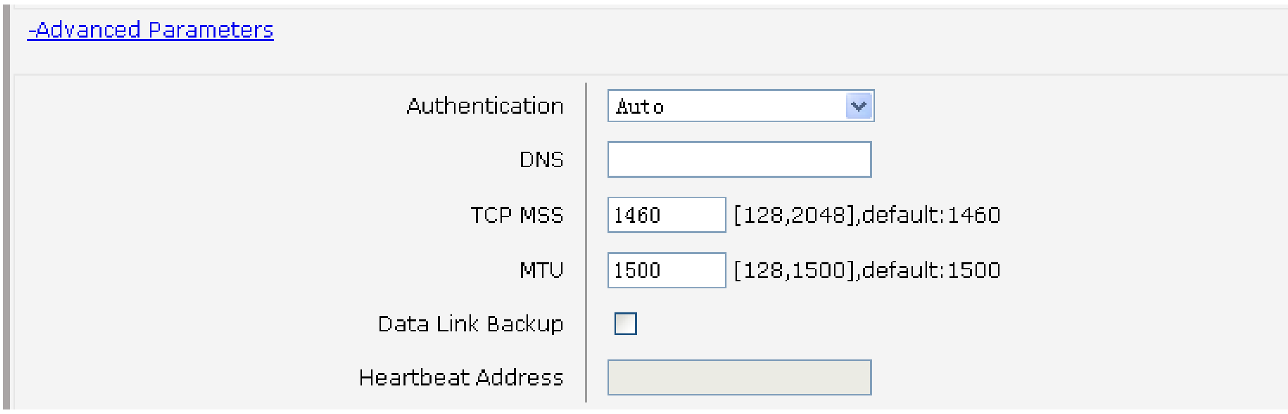
► **Dial Number:** 3G network dial numbers.

► **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	□	
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.

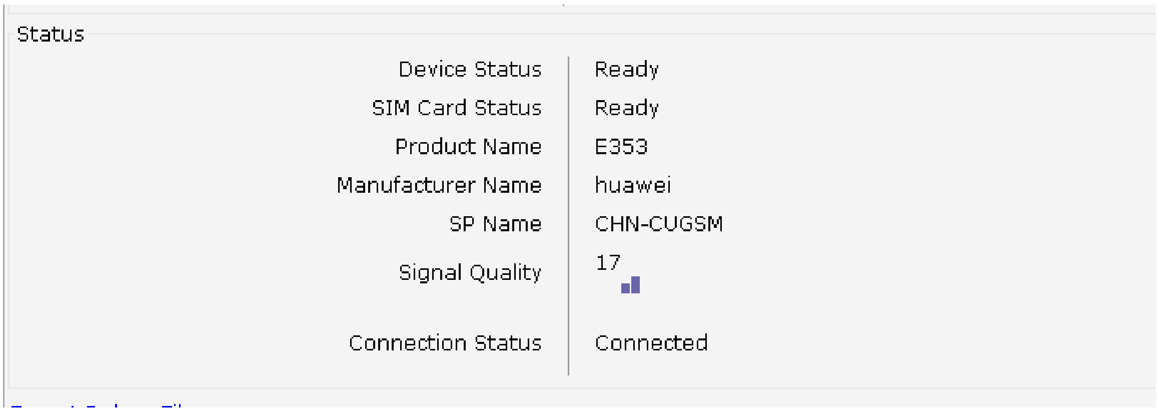
► **TCP MSS:** Configure TCP maximum segment, we recommend using the default value.

► **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:

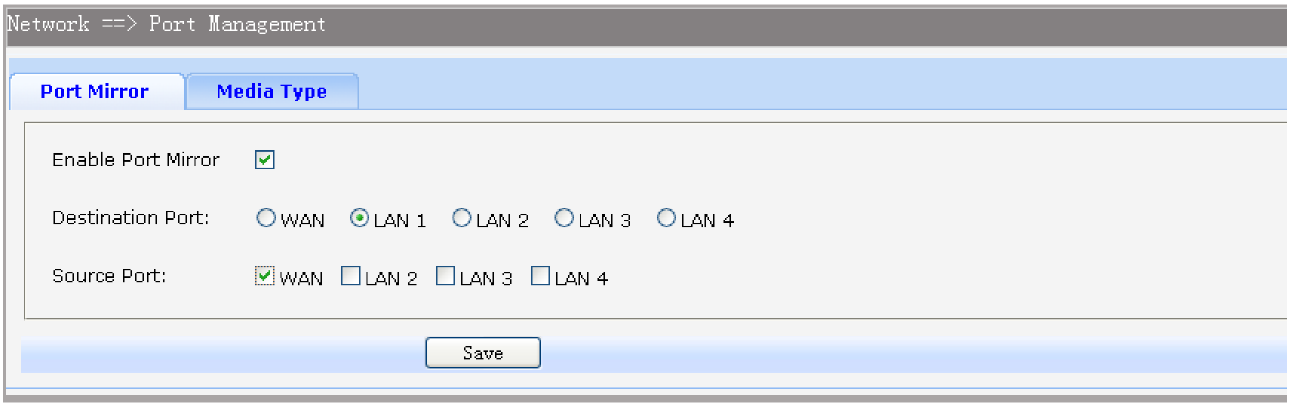
- ► **Device Status:** Indicates whether to insert 3G module.
- ► **SIM Card Status:** Indicates whether to insert 3G modem in the SIM card, the ready state means the SIM card is detected.
- ► **Product Name:** 3G modem Product Type.
- ► **Manufacturer Name:** 3G modem vendor name.
- ► **SP Name:** 3G 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.



Enable Port Mirror ☑

Destination Port: ○ WAN ● LAN 1 ○ LAN 2 ○ LAN 3 ○ LAN 4

Source Port: ☑ WAN □ LAN 2 □ LAN 3 □ LAN 4

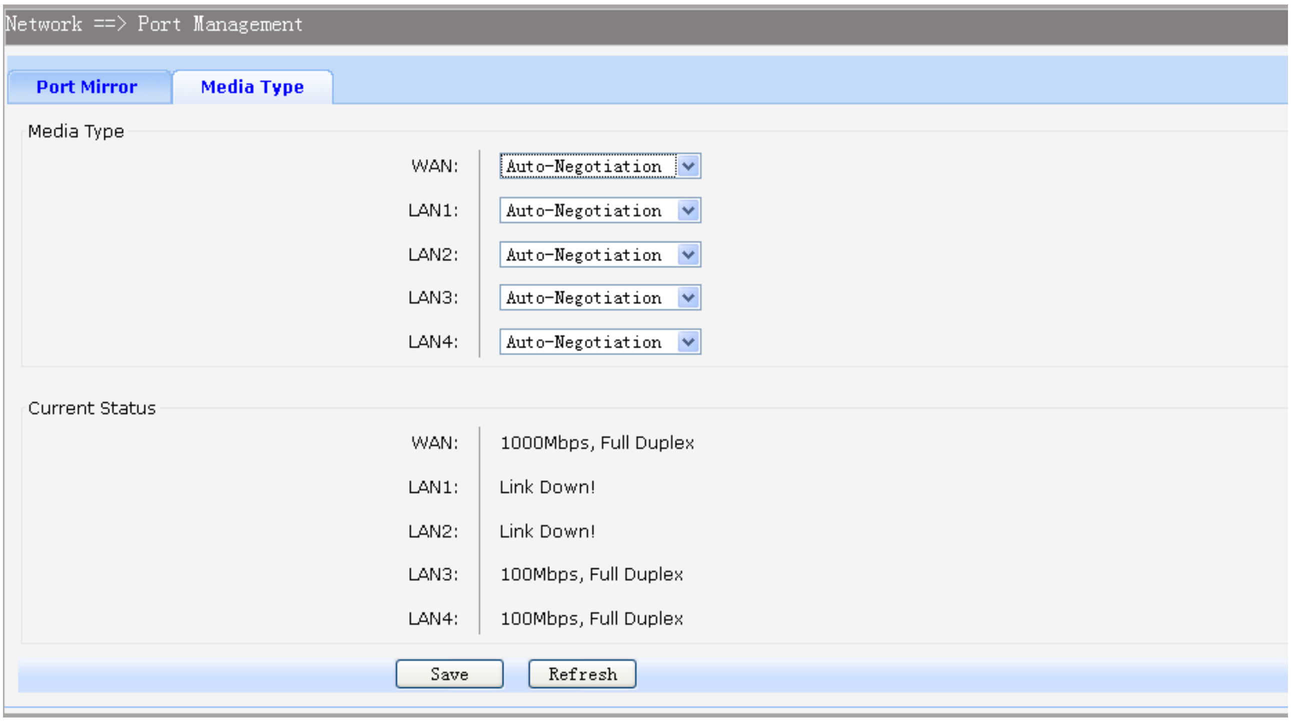
Figure 3-27 Port Mirror

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.



Network ==> Port Management

Media Type

WAN:	Auto-Negotiation
LAN1:	Auto-Negotiation
LAN2:	Auto-Negotiation
LAN3:	Auto-Negotiation
LAN4:	Auto-Negotiation

Current Status

WAN:	1000Mbps, Full Duplex
LAN1:	Link Down!
LAN2:	Link Down!
LAN3:	100Mbps, Full Duplex
LAN4:	100Mbps, Full Duplex

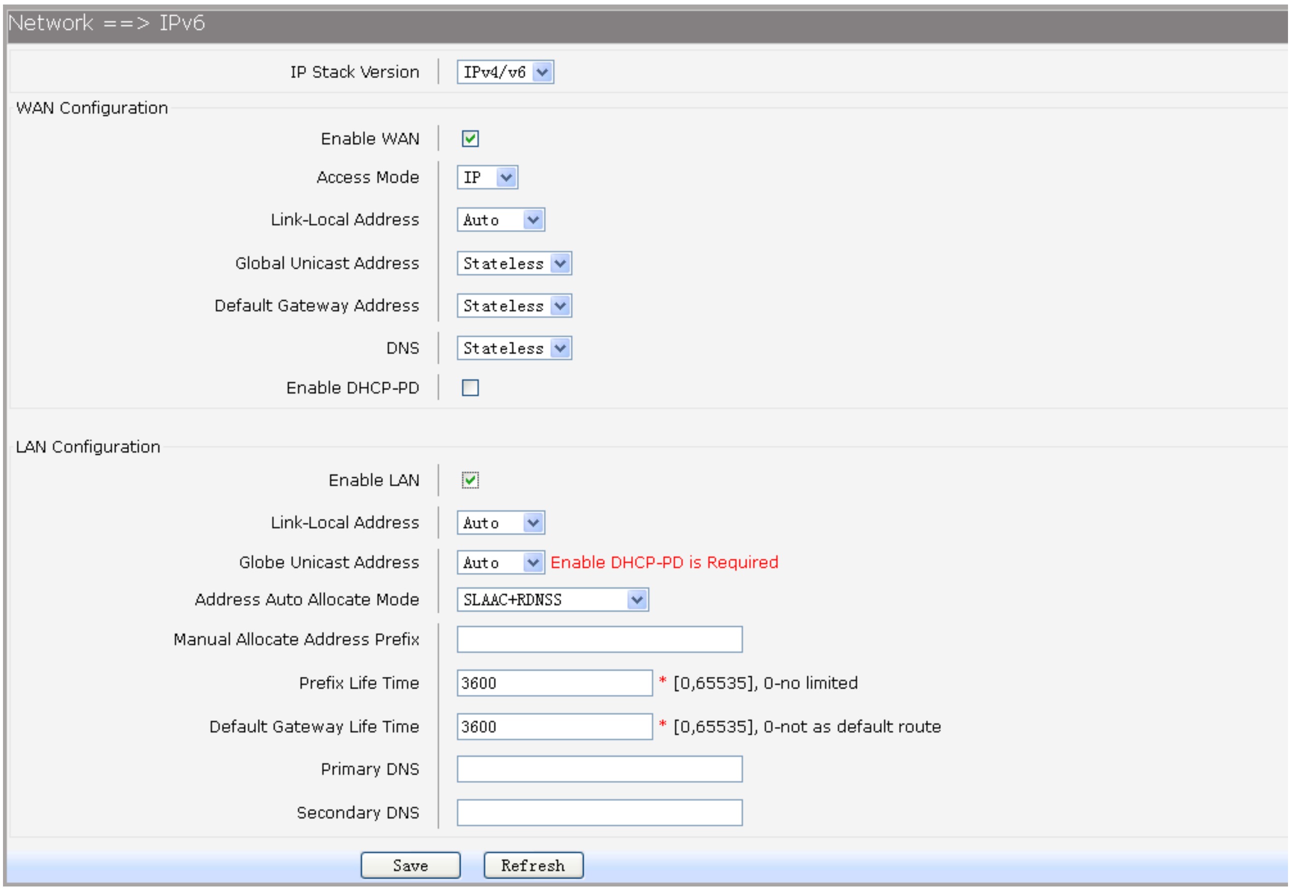
Figure 3-28 Media Type

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.



Network ==> IPv6

IP Stack Version: IPv4/v6

WAN Configuration

Enable WAN: ☑
Access Mode: IP
Link-Local Address: Auto
Global Unicast Address: Stateless
Default Gateway Address: Stateless
DNS: Stateless
Enable DHCP-PD: □

LAN Configuration

Enable LAN: ☑
Link-Local Address: Auto
Globe Unicast Address: Auto Enable DHCP-PD is Required
Address Auto Allocate Mode: SLAAC+RDNSS
Manual Allocate Address Prefix:
Prefix Life Time: 3600 * [0,65535], 0-no limited
Default Gateway Life Time: 3600 * [0,65535], 0-not as default route
Primary DNS:
Secondary DNS:

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

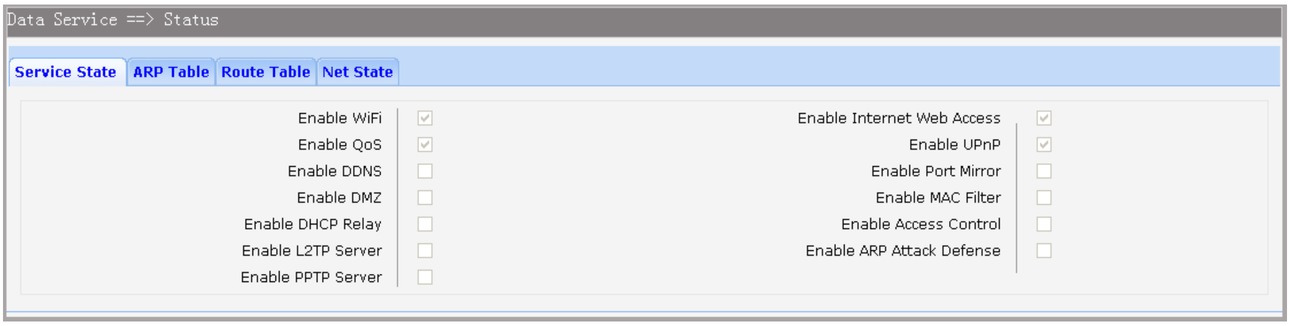
3.4.1 Status

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.



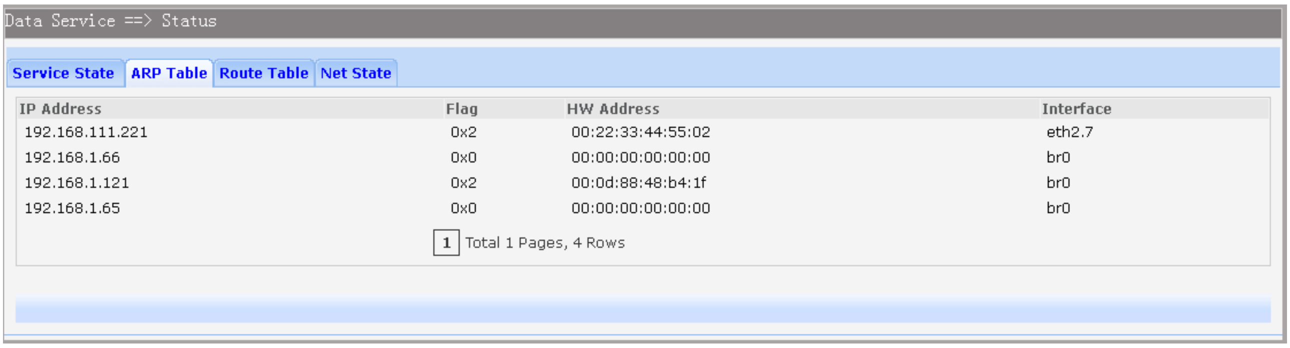
Enable WiFi	☑	Enable Internet Web Access	☑
Enable QoS	☑	Enable UPnP	☑
Enable DDNS	□	Enable Port Mirror	□
Enable DMZ	□	Enable MAC Filter	□
Enable DHCP Relay	□	Enable Access Control	□
Enable L2TP Server	□	Enable ARP Attack Defense	□
Enable PPTP Server	□		

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.



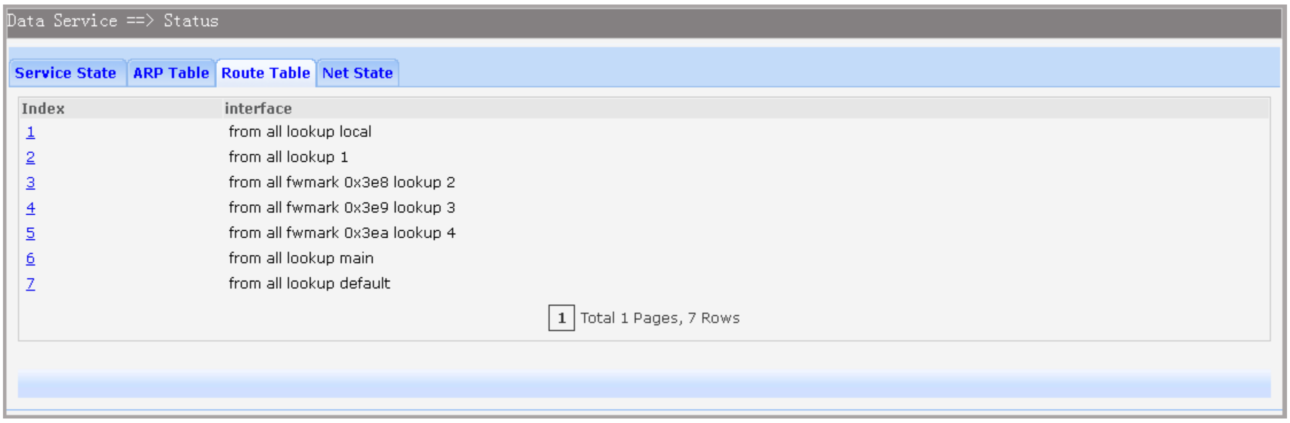
IP Address	Flag	HW Address	Interface
192.168.111.221	0x2	00:22:33:44:55:02	eth2.7
192.168.1.66	0x0	00:00:00:00:00:00	br0
192.168.1.121	0x2	00:0d:88:48:b4:1f	br0
192.168.1.65	0x0	00:00:00:00:00:00	br0

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.



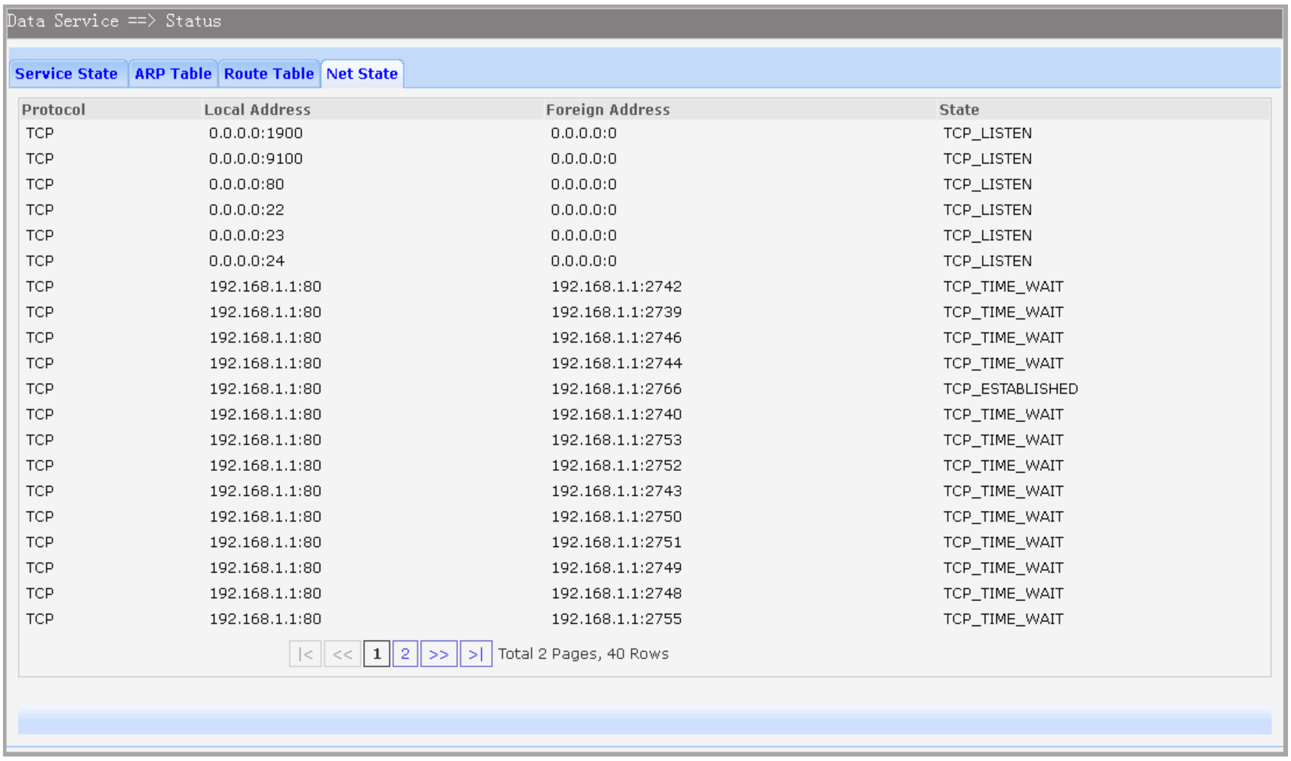
Index	interface
1	from all lookup local
2	from all lookup 1
3	from all fwmark 0x3e8 lookup 2
4	from all fwmark 0x3e9 lookup 3
5	from all fwmark 0x3ea lookup 4
6	from all lookup main
7	from all lookup default

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.



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

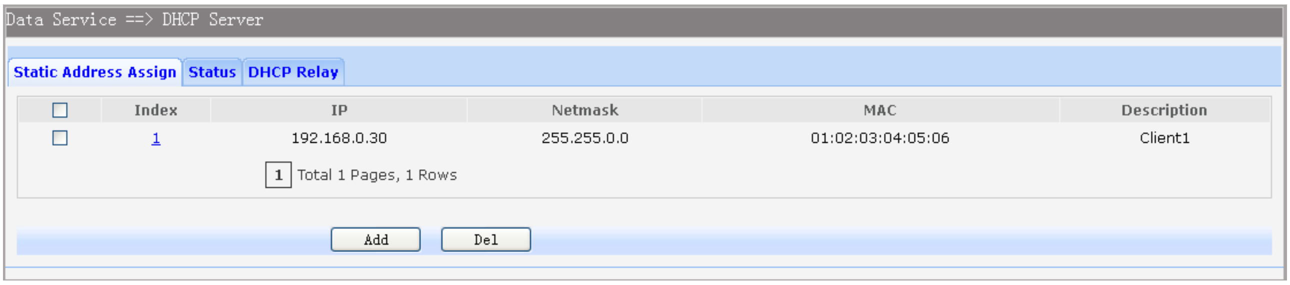
|< << 1 2 >> >| Total 2 Pages, 40 Rows

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.

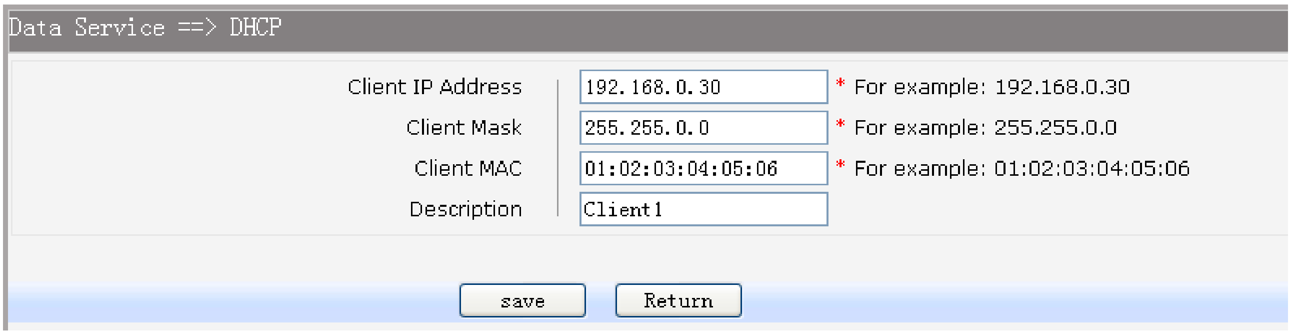


□	Index	IP	Netmask	MAC	Description
□	1	192.168.0.30	255.255.0.0	01:02:03:04:05:06	Client1

1 Total 1 Pages, 1 Rows

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.



Client IP Address: 192.168.0.30 * For example: 192.168.0.30

Client Mask: 255.255.0.0 * For example: 255.255.0.0

Client MAC: 01:02:03:04:05:06 * For example: 01:02:03:04:05:06

Description: Client1

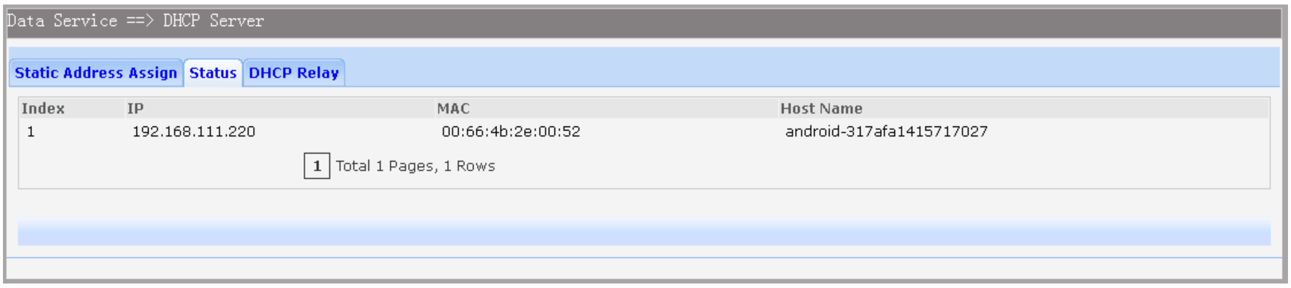
Figure 3-35 Add or Modify An Static Address Assign Entry

The following items are displayed on this screen:

- ► **Client IP Addres:** 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.



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.

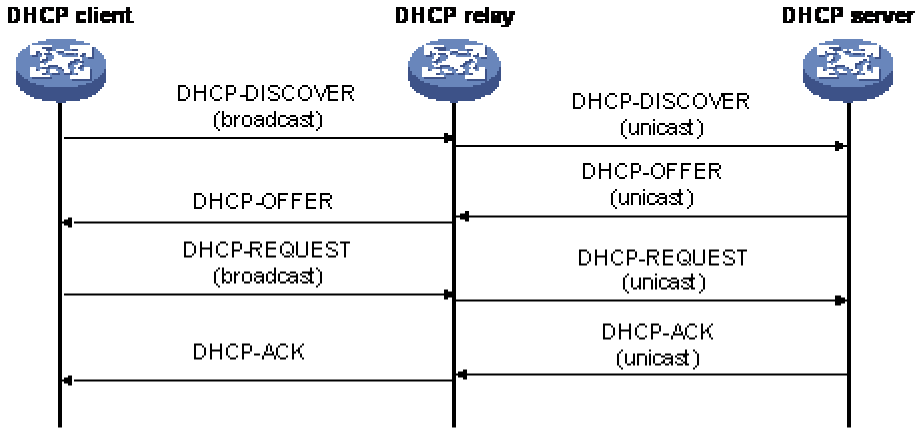
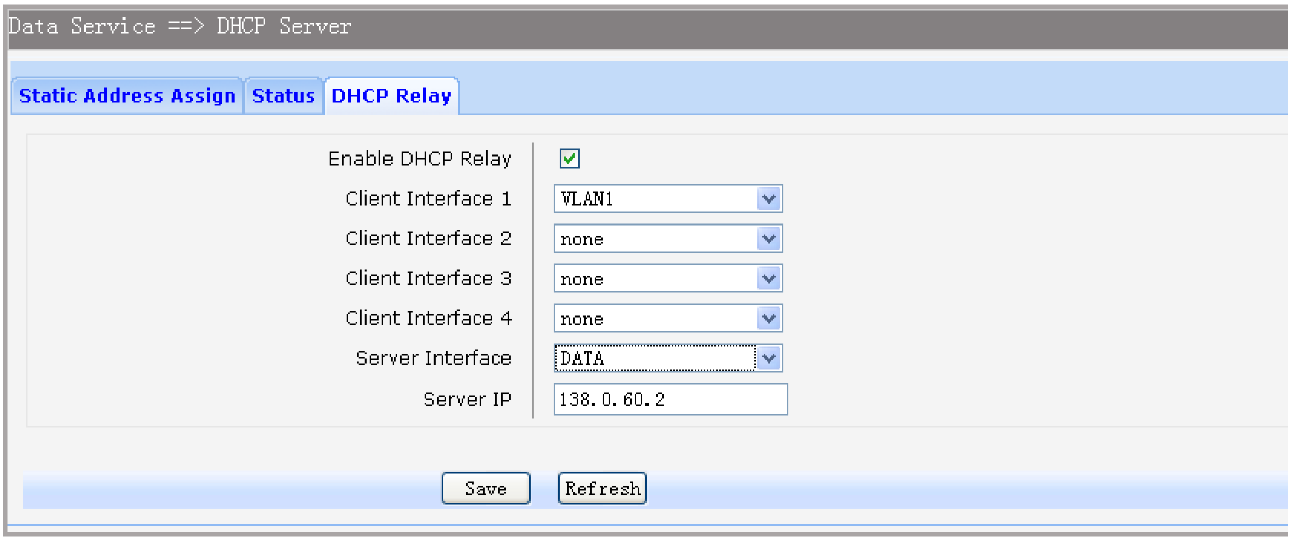


Figure 3-37 DHCP Relay Overview

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


Data Service ==> DHCP Server

Enable DHCP Relay	☑
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

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.

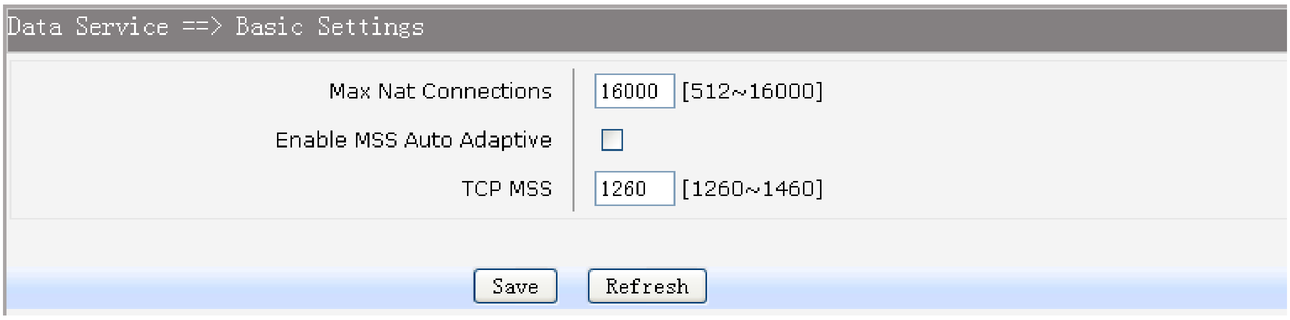
► **Server IP:** Configure the DHCP server IP address.

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	16000 [512~16000]
Enable MSS Auto Adaptive	□
TCP MSS	1260 [1260~1460]

Figure 3-39 Basic Settings

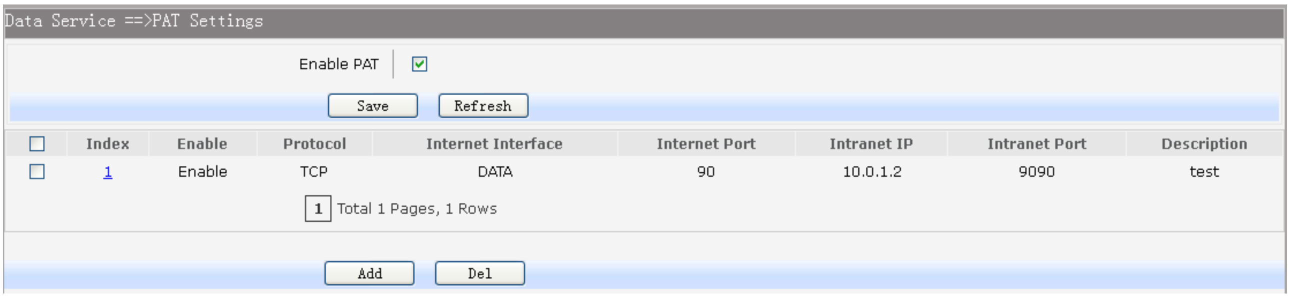
The following items are displayed on this screen:

- ► **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 ☑

□	Index	Enable	Protocol	Internet Interface	Internet Port	Intranet IP	Intranet Port	Description
□	1	Enable	TCP	DATA	90	10.0.1.2	9090	test

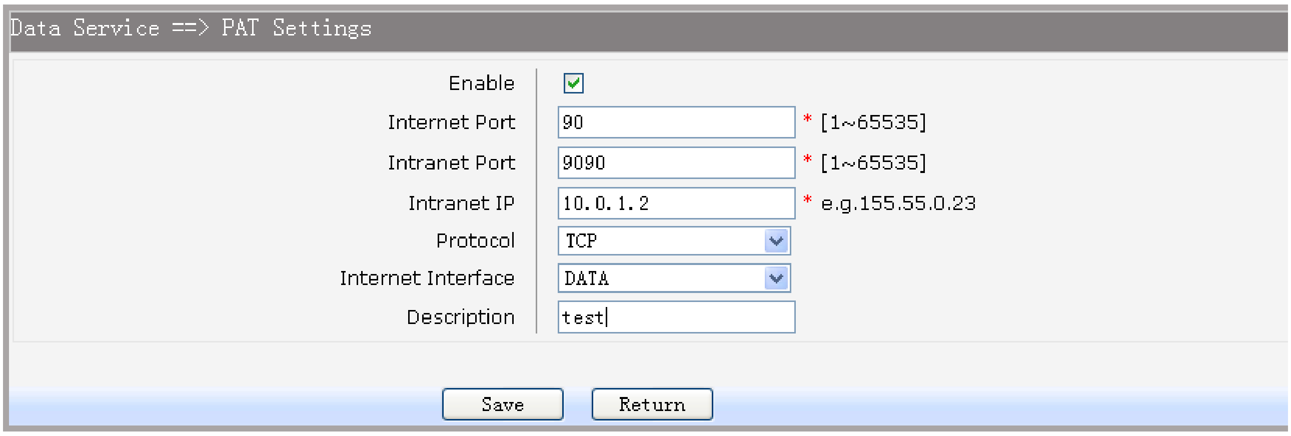
1 Total 1 Pages, 1 Rows

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	☑
Internet Port	90 * [1~65535]
Intranet Port	9090 * [1~65535]
Intranet IP	10. 0. 1. 2 * e.g.155.55.0.23
Protocol	TCP
Internet Interface	DATA
Description	test

Figure 3-41 Add or Modify PAT Entry

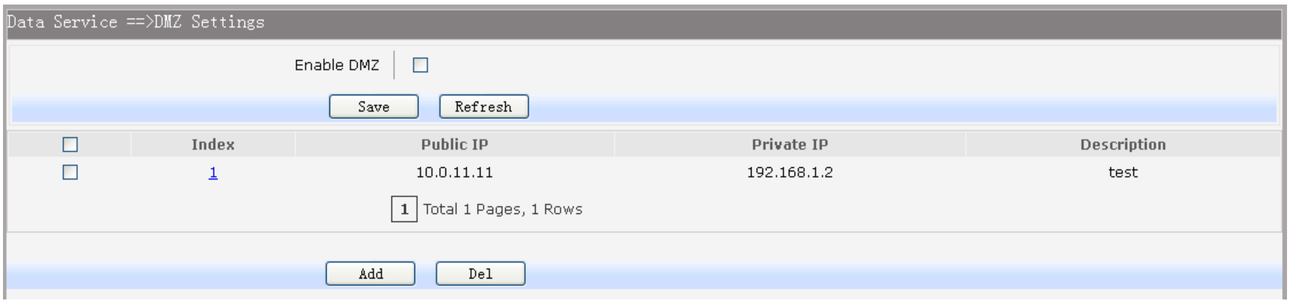
The following items are displayed on this screen:

- ► **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.



Data Service ==>DMZ Settings

Enable DMZ □

□	Index	Public IP	Private IP	Description
□	1	10.0.11.11	192.168.1.2	test

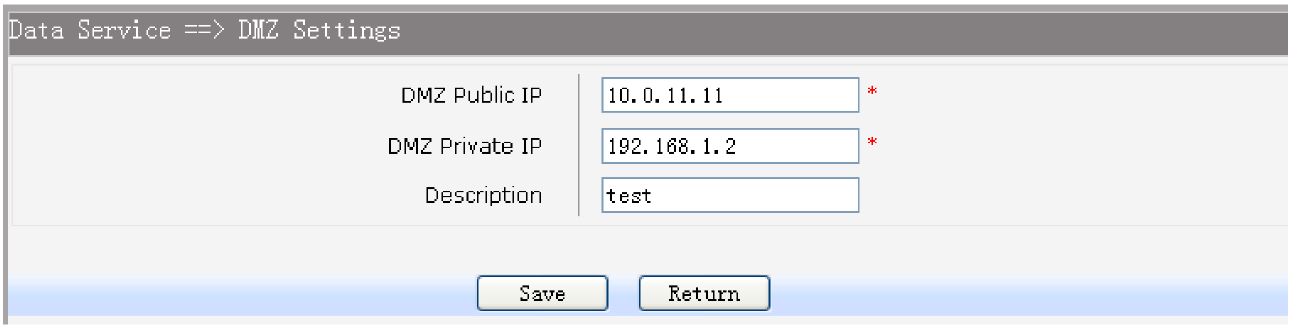
1 Total 1 Pages, 1 Rows

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.



Data Service ==> DMZ Settings

DMZ Public IP	10.0.11.11 *
DMZ Private IP	192.168.1.2 *
Description	test

Figure 3-43 Add or Modify DMZ Entry

The following items are displayed on this screen:

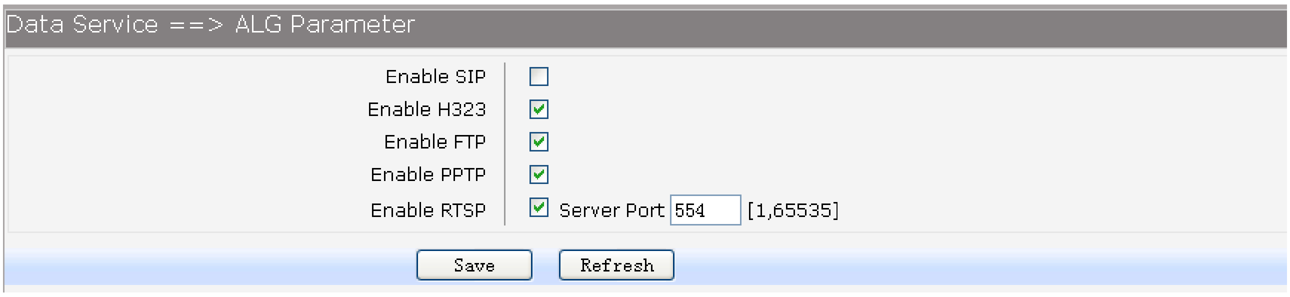
- ► **DMZ Public IP:** The public IP address for this DMZ entry.

- ► **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	□
Enable H323	☑
Enable FTP	☑
Enable PPTP	☑
Enable RTSP	☑ Server Port 554 [1,65535]

Figure 3-44 ALG Settings

The following items are displayed on this screen:

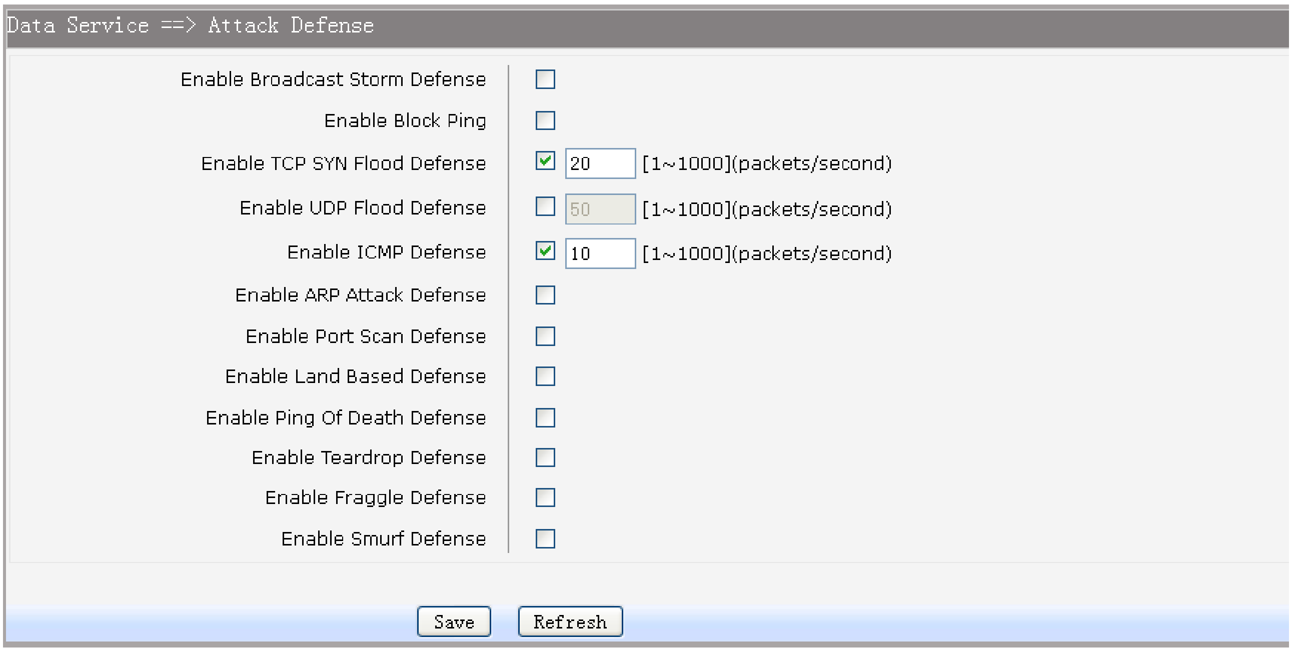
- ► **Enable SIP:** Enable or disable SIP ALG.
- ► **Enable H323:** Allow Microsoft NetMeeting clients to communicate across NAT if selected.
- ► **Enable FTP:** Allow FTP clients and servers to transfer data across NAT if selected.
- ► **Enable PPTP:** Enable or disable PPTP ALG.
- ► **Enable RTSP:** 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	□
Enable Block Ping	□
Enable TCP SYN Flood Defense	☑ 20 [1~1000](packets/second)
Enable UDP Flood Defense	□ 50 [1~1000](packets/second)
Enable ICMP Defense	☑ 10 [1~1000](packets/second)
Enable ARP Attack Defense	□
Enable Port Scan Defense	□
Enable Land Based Defense	□
Enable Ping Of Death Defense	□
Enable Teardrop Defense	□
Enable Fraggle Defense	□
Enable Smurf Defense	□

Figure 3-45 Attack Defense

The following items are displayed on this screen:

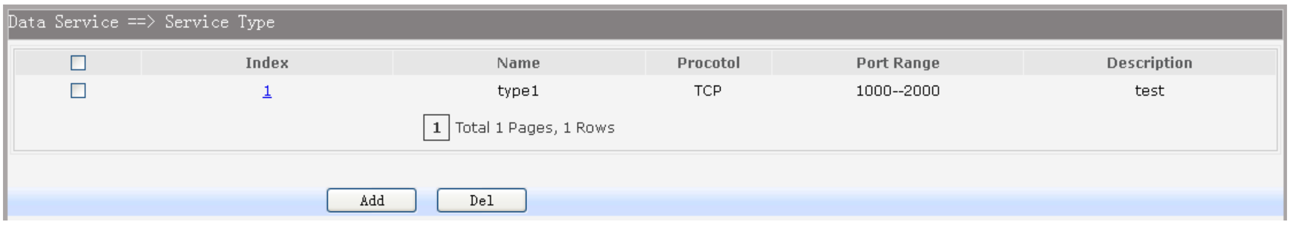
- **Enable Broadcast Storm Defense:** Enable or disable **Broadcast Storm Defense**.
- **Enable Block Ping:** Enable or disable **Block Ping** function.
- **Enable TCP SYN Flood Defense:** Enable or disable **TCP SYN Flood Defense**.
- **Enable UDP Flood Defense:** Enable or disable **UDP Flood Defense**.
- **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

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**.

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.



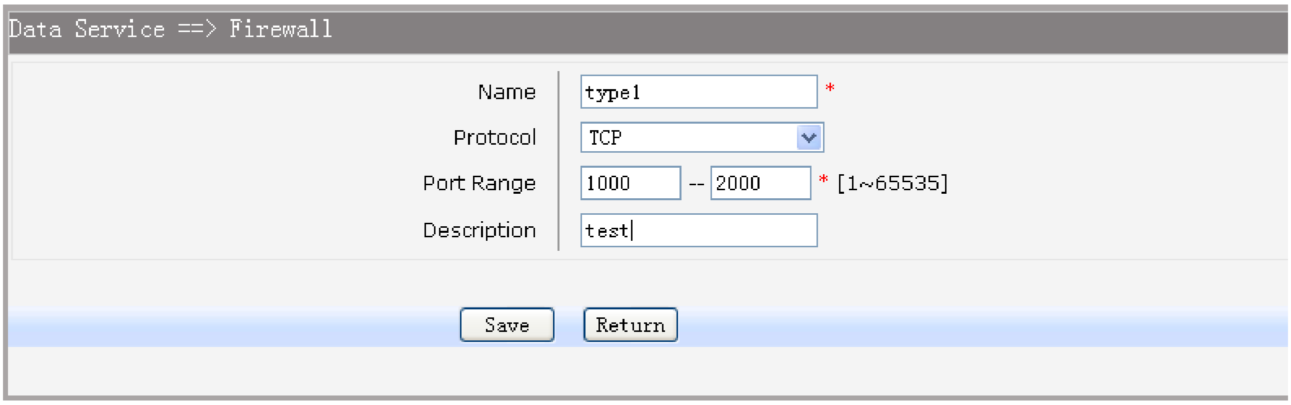
Data Service ==> Service Type

□	Index	Name	Procotol	Port Range	Description
□	1	type1	TCP	1000--2000	test

1 Total 1 Pages, 1 Rows

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

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

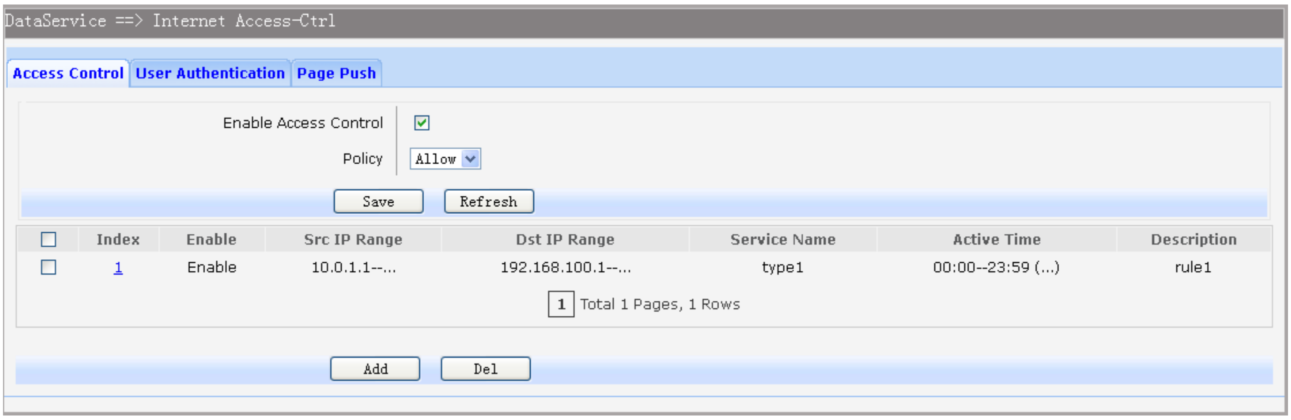
3.4.4.3 Internet Access-Ctrl

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

Enable Access Control ☑

Policy Allow

☐	Index	Enable	Src IP Range	Dst IP Range	Service Name	Active Time	Description
☐	1	Enable	10.0.1.1--...	192.168.100.1--...	type1	00:00--23:59 (...)	rule1

1 Total 1 Pages, 1 Rows

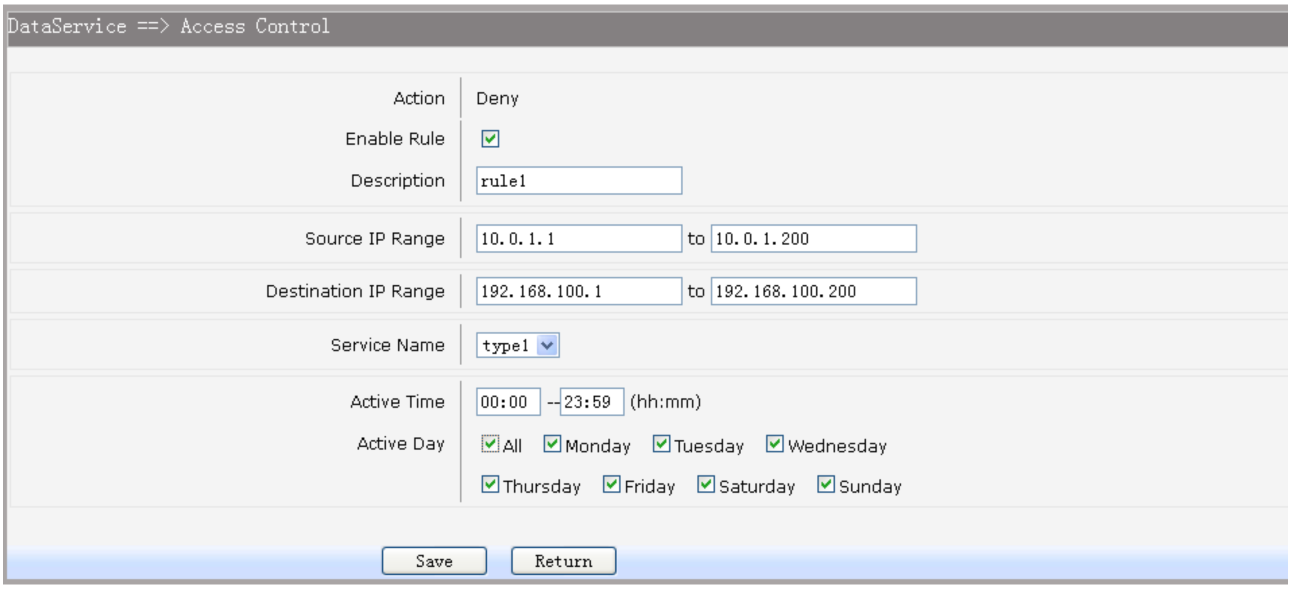
Figure 3-48 View Access Control Entry

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

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.

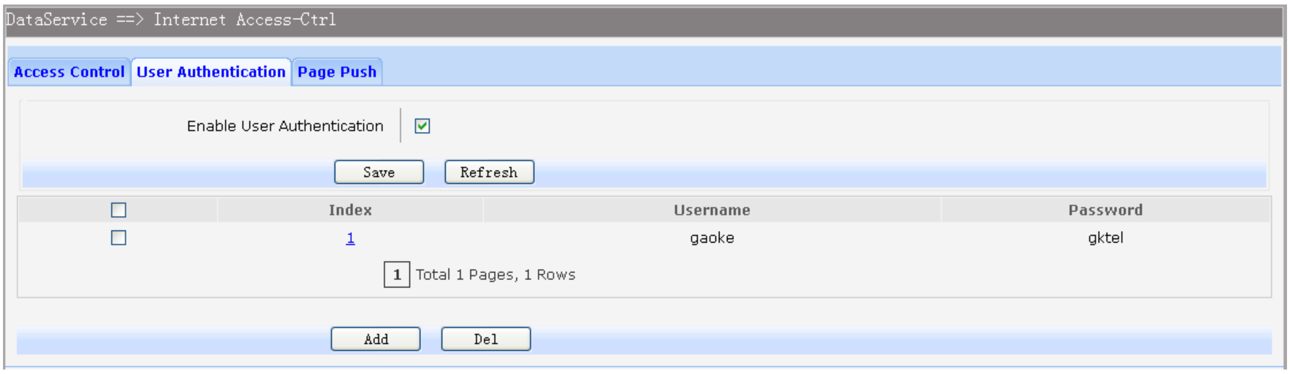
► **Active Time:** Specify the time range for the entry to take effect.

► **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.



DataService ==> Internet Access-Ctrl

Enable User Authentication ☑

□	Index	Username	Password
□	1	gaoke	gktel

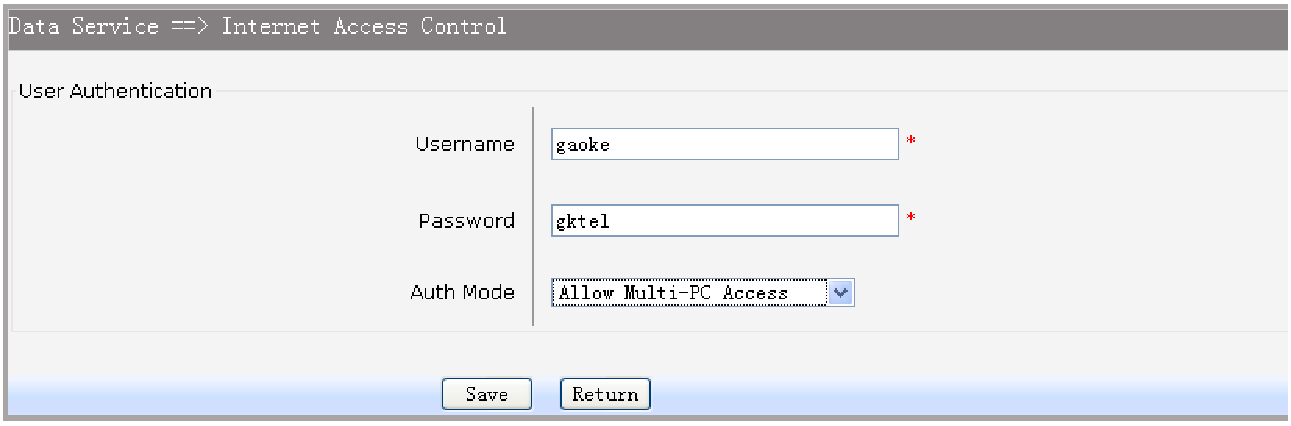
1 Total 1 Pages, 1 Rows

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.



Data Service ==> Internet Access Control

User Authentication

Username: gaoke *

Password: gktel *

Auth Mode: Allow Multi-PC Access

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.

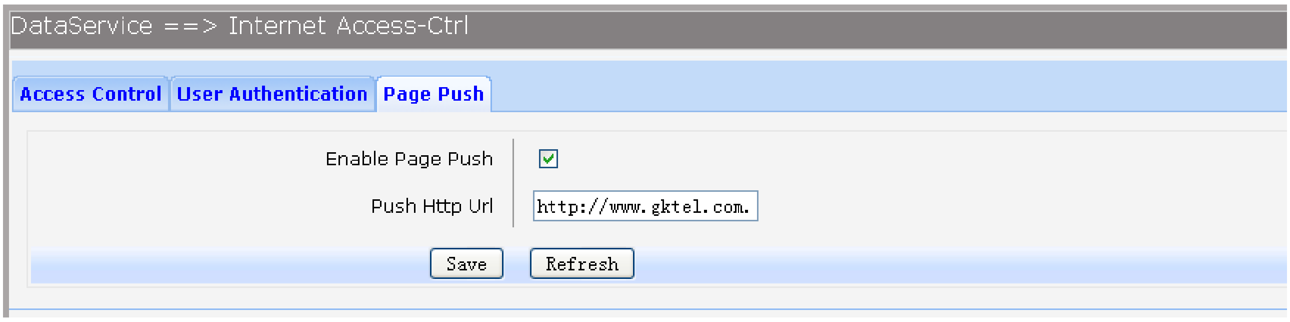
Allow Special IP Access: Allowing only specified IP computer uses this account to access the Internet.

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.



Enable Page Push ☑

Push Http Url http://www.gktel.com.

Figure 3-52 Configure Page Push

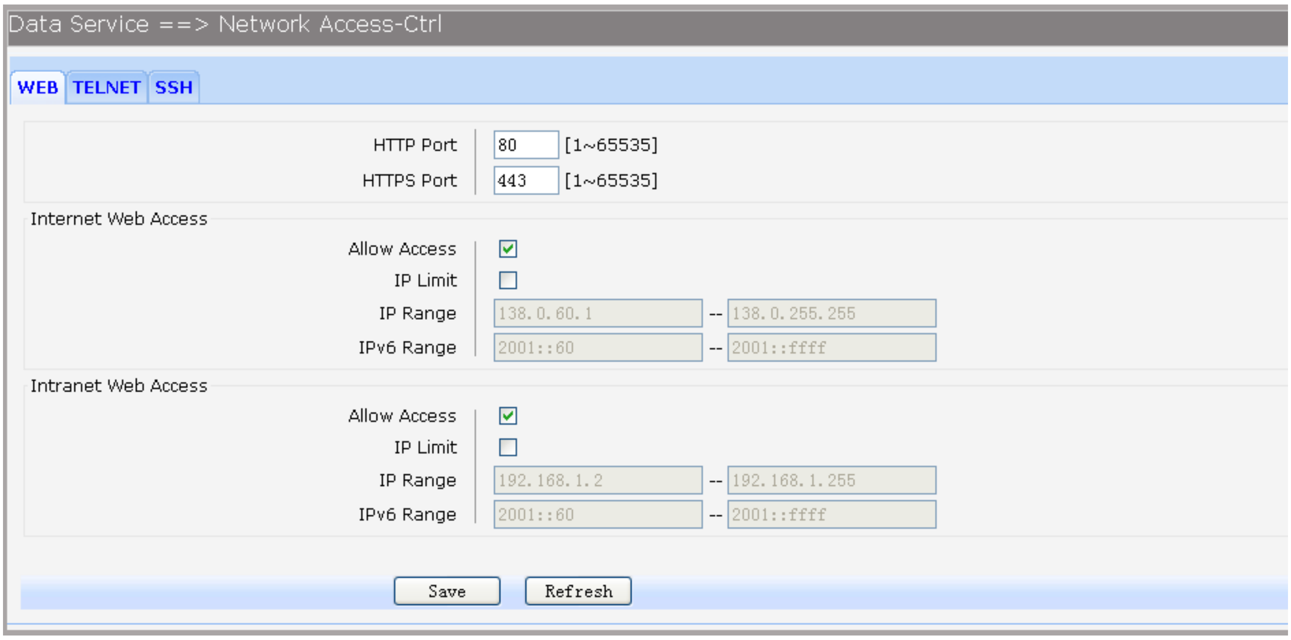
The following items are displayed on this screen:

- **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→Netword Access-Ctrl→WEB** to load the following page.



HTTP Port 80 [1~65535]

HTTPS Port 443 [1~65535]

Internet Web Access

Allow Access ☑

IP Limit □

IP Range 138.0.60.1 -- 138.0.255.255

IPv6 Range 2001::60 -- 2001::ffff

Intranet Web Access

Allow Access ☑

IP Limit □

IP Range 192.168.1.2 -- 192.168.1.255

IPv6 Range 2001::60 -- 2001::ffff

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.

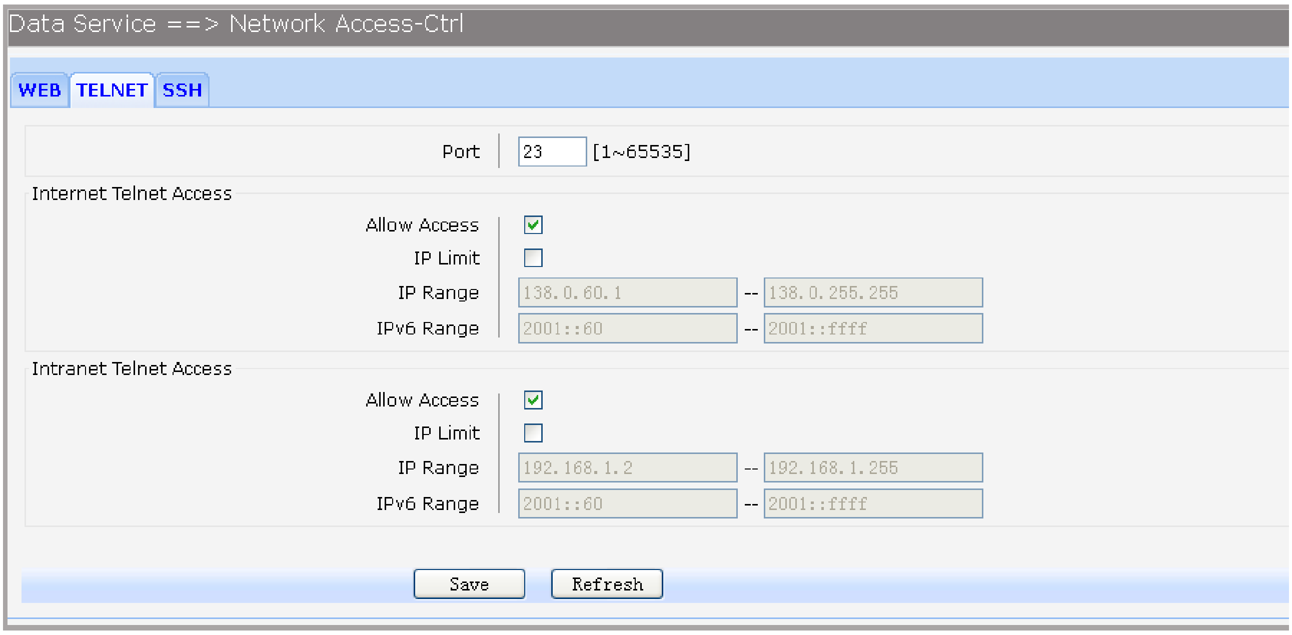
► **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via WEB.

► **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→Netword Access-Ctrl→TELNET** to load the following page.



Data Service ==> Network Access-Ctrl

Port 23 [1~65535]

Internet Telnet Access

Allow Access ☑

IP Limit □

IP Range 138.0.60.1 -- 138.0.255.255

IPv6 Range 2001::60 -- 2001::ffff

Intranet Telnet Access

Allow Access ☑

IP Limit □

IP Range 192.168.1.2 -- 192.168.1.255

IPv6 Range 2001::60 -- 2001::ffff

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.

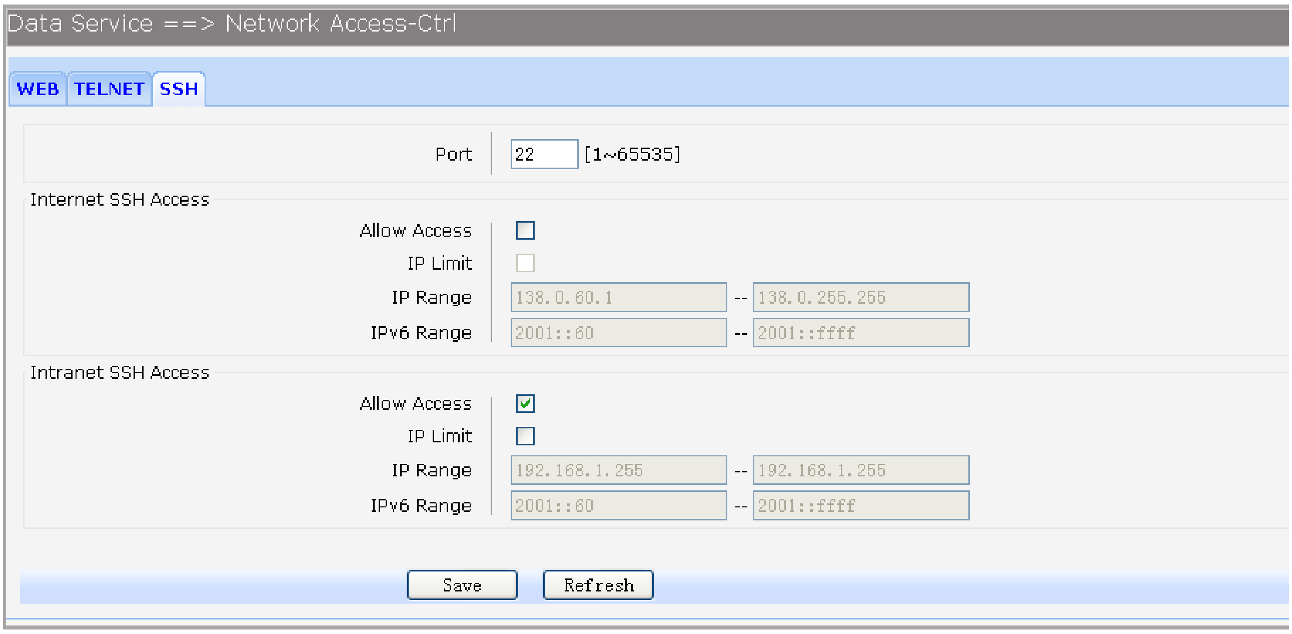
► **IP Limit:** If enabled, allow only specific IP range to access the device from the Intranet via telnet

► **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→Netword Access-Ctrl→SSH** to load the following page.



Data Service ==> Network Access-Ctrl

WEB | TELNET | SSH

Port: 22 [1~65535]

Internet SSH Access

Allow Access □
IP Limit □
IP Range 138.0.60.1 -- 138.0.255.255
IPv6 Range 2001::60 -- 2001::ffff

Intranet SSH Access

Allow Access ☑
IP Limit □
IP Range 192.168.1.255 -- 192.168.1.255
IPv6 Range 2001::60 -- 2001::ffff

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.

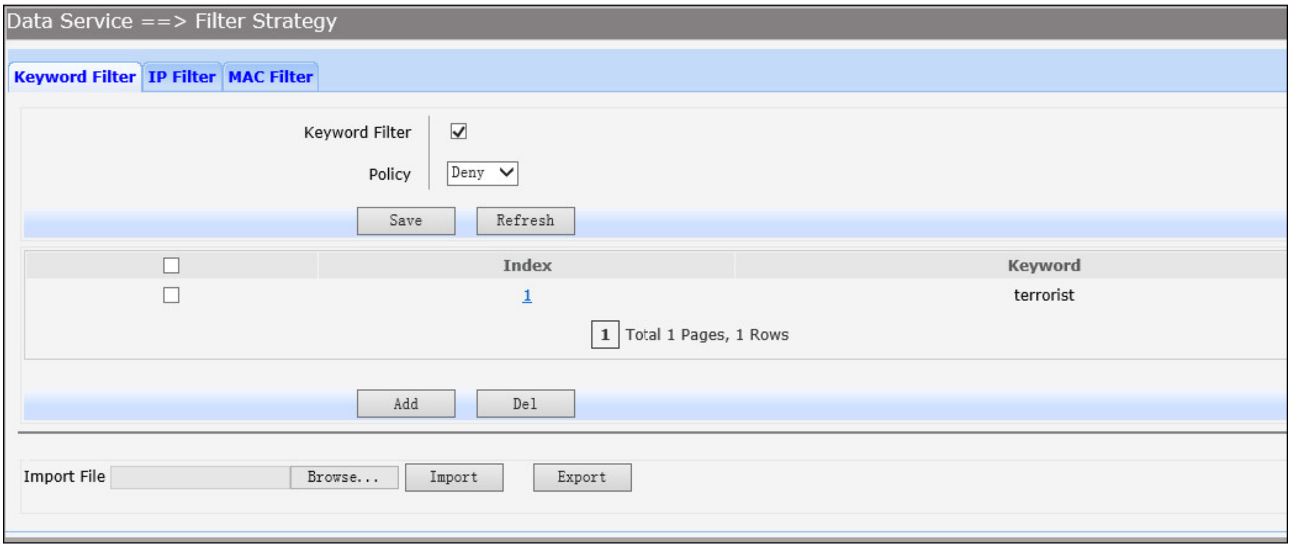
3.4.4.5 Filter Strategy

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 ☑

Policy Deny

☐	Index	Keyword
☐	1	terrorist

1 Total 1 Pages, 1 Rows

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.

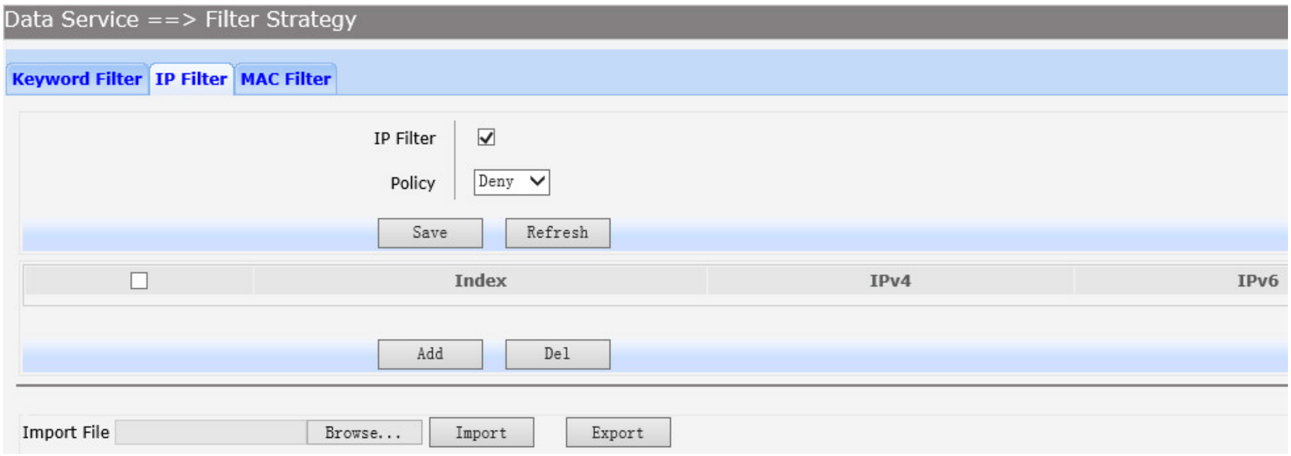
You can export all the keywords as a file. Of course, you can also import a file.

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

IP Filter ☑

Policy Deny

□	Index	IPv4	IPv6

Import File

Figure 3-57 Configure IP Filter

The following items are displayed on this screen:

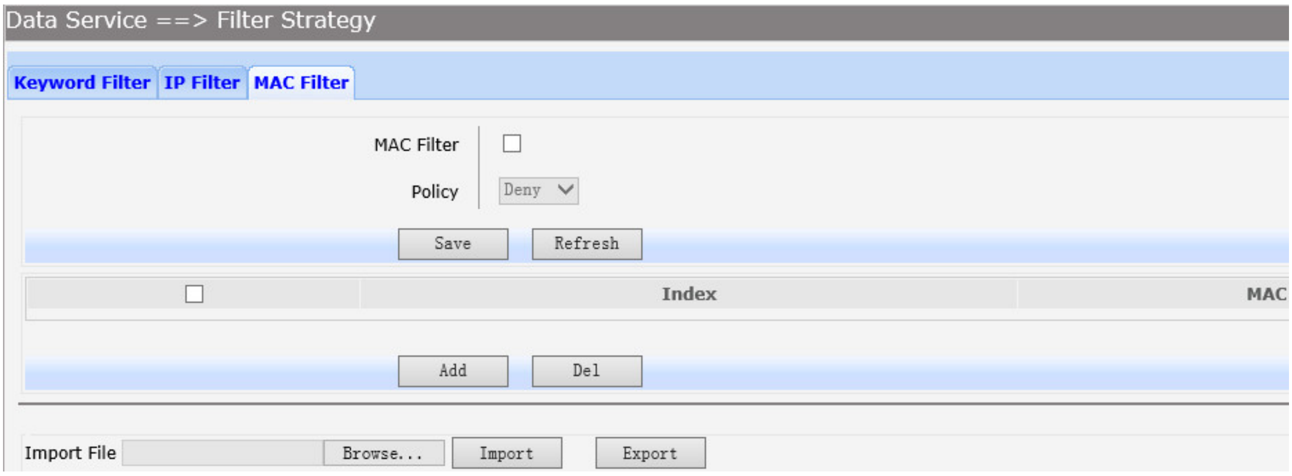
► **IP Filter:** If enabled, packet filtering is enabled by IP address.

► **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

MAC Filter □

Policy Deny

□	Index	MAC

Import File

Figure 3-58 Configure MAC Filter

The following items are displayed on this screen:

► **IP Filter:** If enabled, packet filtering is enabled by MAC.

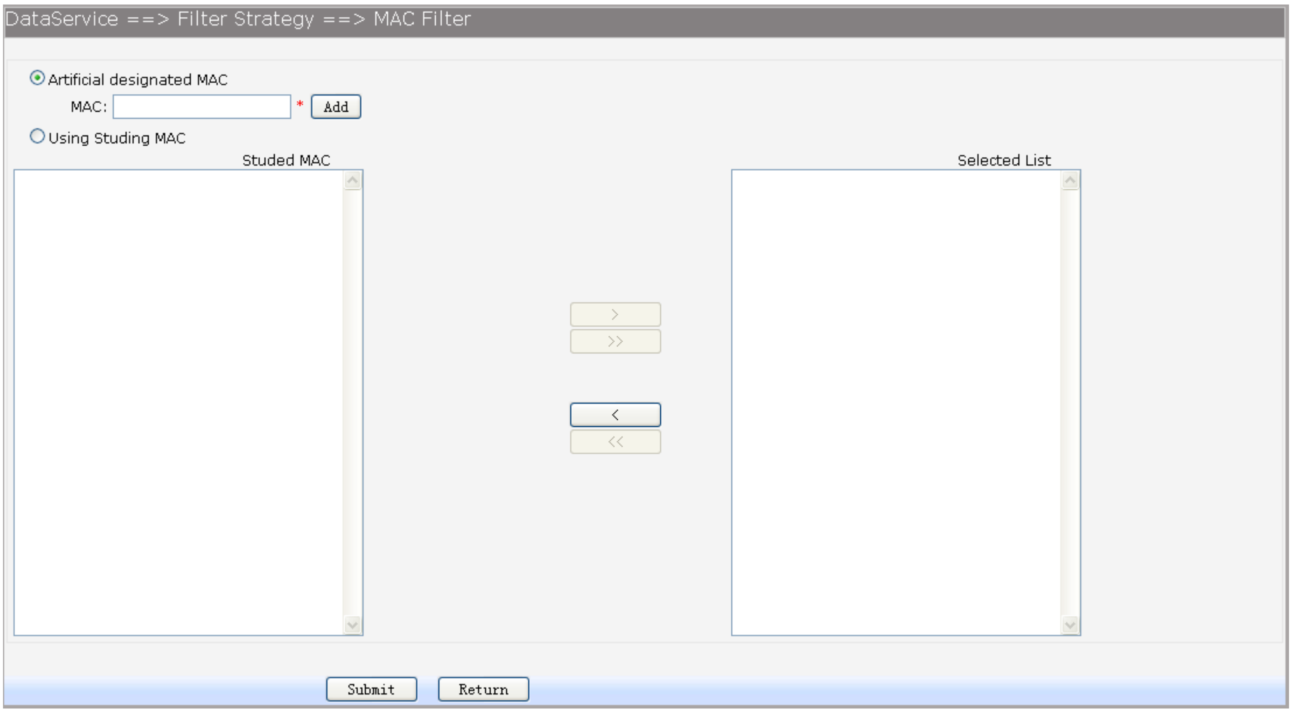
► **Policy:** The policy for MAC list. Deny and Allow.

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.

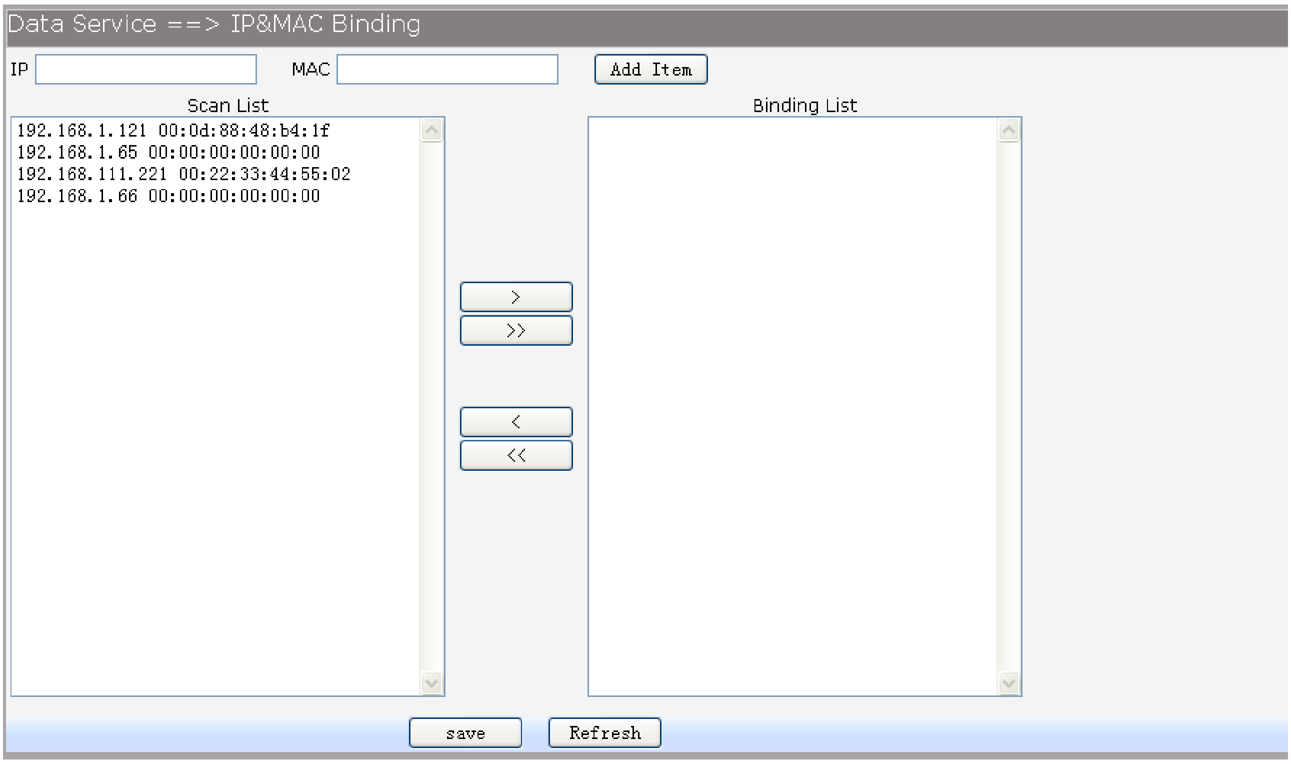


DataService ==> Filter Strategy ==> MAC Filter
● Artificial designated MAC
MAC: *
Add
○ Using Studing MAC
Studed MAC
Selected List
>
>>
<
<<
Submit
Return

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.



```
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
```

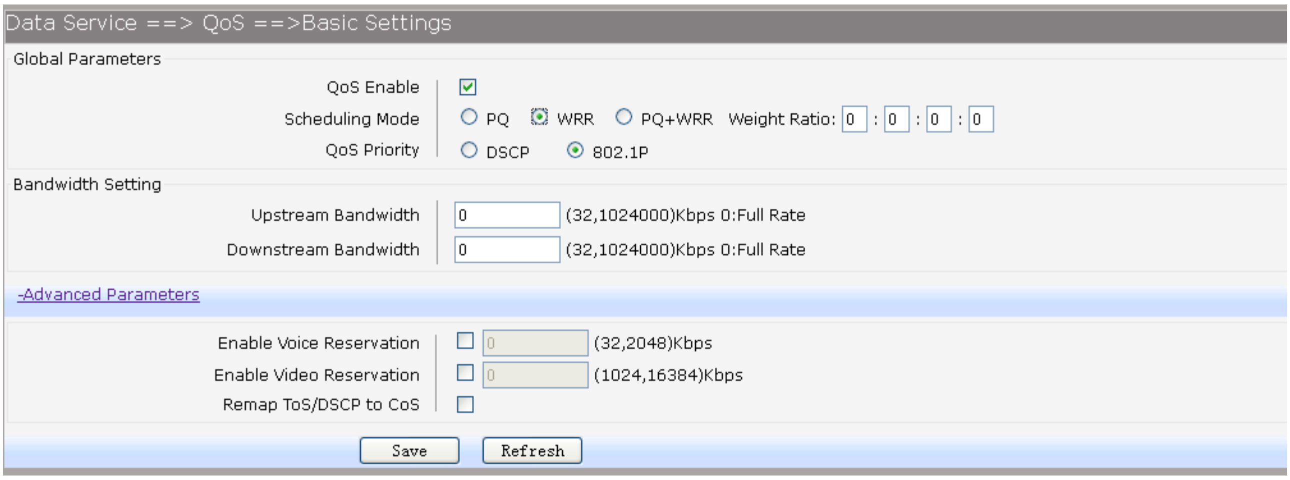
Figure 3-60 Configure IP&MAC Binding

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.



Data Service ==> QoS ==>Basic Settings

Global Parameters

QoS Enable ☑

Scheduling Mode ○ PQ ● WRR ○ PQ+WRR Weight Ratio: 0 : 0 : 0 : 0

QoS Priority ○ DSCP ● 802.1P

Bandwidth Setting

Upstream Bandwidth 0 (32,1024000)Kbps 0:Full Rate

Downstream Bandwidth 0 (32,1024000)Kbps 0:Full Rate

-Advanced Parameters

Enable Voice Reservation □ 0 (32,2048)Kbps

Enable Video Reservation □ 0 (1024,16384)Kbps

Remap ToS/DSCP to CoS □

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

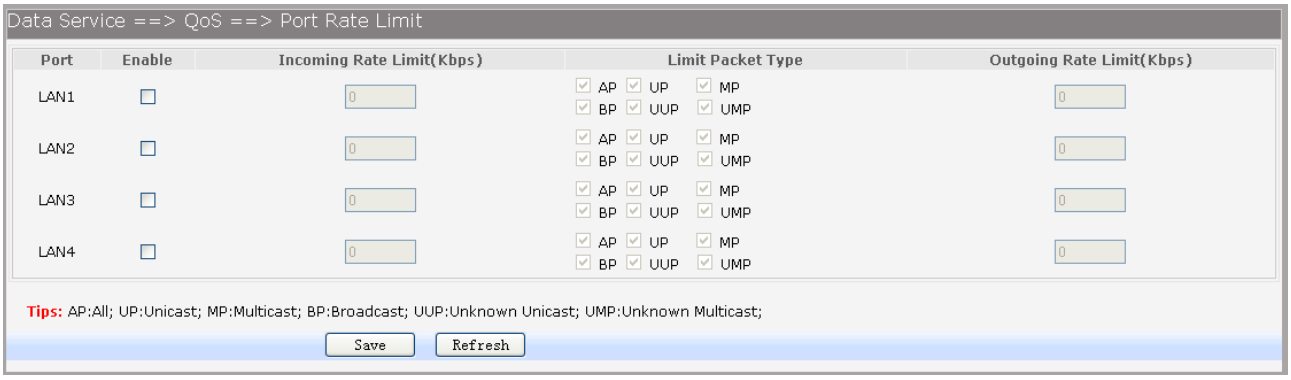
► **Remap Tos/DSCP to CoS:** Check the box that the system will remark 802.1P value with TOS/DSCP of upstream packets, the mapping relationship is as follows:

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	□	0	☑ AP ☑ UP ☑ MP ☑ BP ☑ UUP ☑ UMP	0
LAN2	□	0	☑ AP ☑ UP ☑ MP ☑ BP ☑ UUP ☑ UMP	0
LAN3	□	0	☑ AP ☑ UP ☑ MP ☑ BP ☑ UUP ☑ UMP	0
LAN4	□	0	☑ AP ☑ UP ☑ MP ☑ BP ☑ UUP ☑ UMP	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.

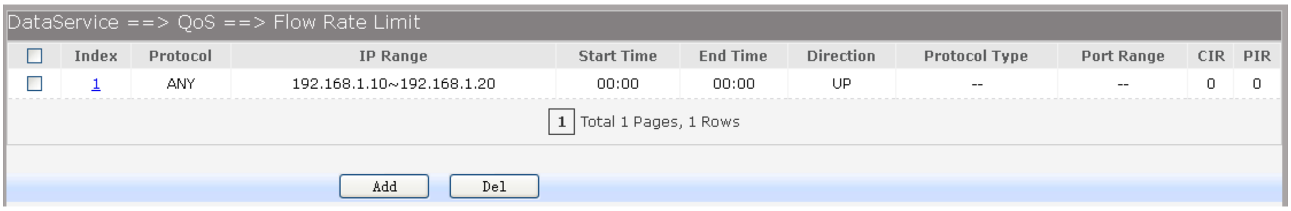
► **Incoming Rate Limit:** Enter incoming maximum rate, which must is times of 32Kbsp.

► **Limit Packet Type:** Select the packet type which is limited rate.

► **Outgoing Rate Limit:** Enter Outgoing maximum rate, which must is times of 32Kbsp.

3.4.5.3 Flow Rate Limit

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



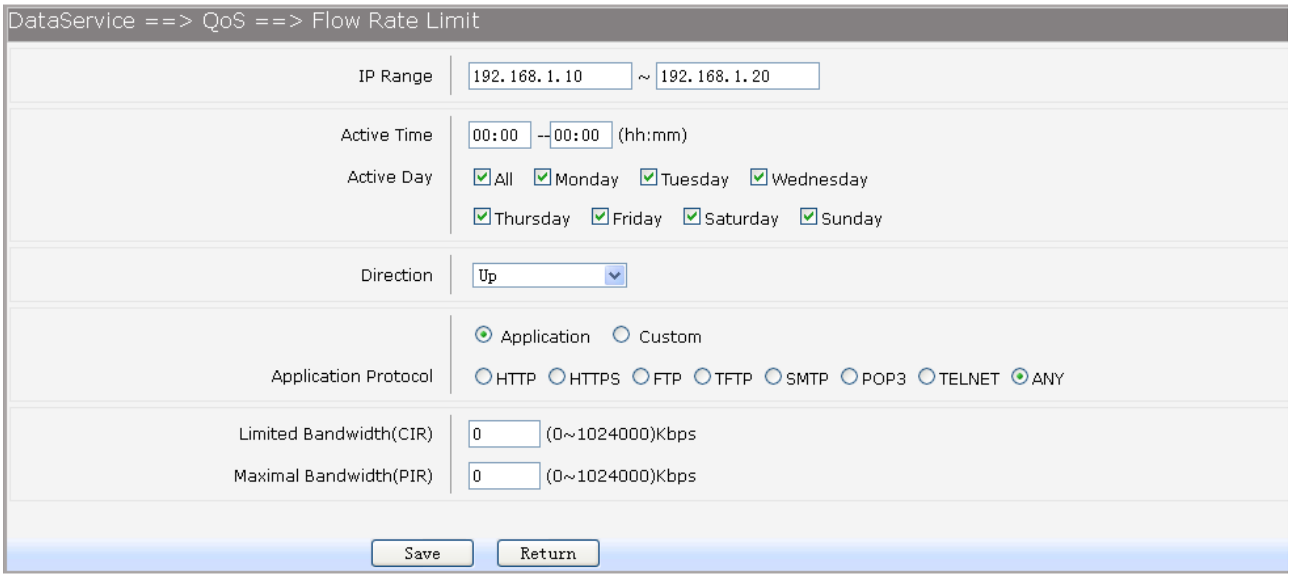
DataService ==> QoS ==> Flow Rate Limit

□	Index	Protocol	IP Range	Start Time	End Time	Direction	Protocol Type	Port Range	CIR	PIR
□	1	ANY	192.168.1.10~192.168.1.20	00:00	00:00	UP	--	--	0	0

1 Total 1 Pages, 1 Rows

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	☑ All ☑ Monday ☑ Tuesday ☑ Wednesday ☑ Thursday ☑ Friday ☑ Saturday ☑ Sunday
Direction	Up
	● Application ○ Custom
Application Protocol	○ HTTP ○ HTTPS ○ FTP ○ TFTP ○ SMTP ○ POP3 ○ TELNET ● ANY
Limited Bandwidth(CIR)	0 (0~1024000)Kbps
Maximal Bandwidth(PIR)	0 (0~1024000)Kbps

Figure 3-64 Configure Qos Flow Rate Limit

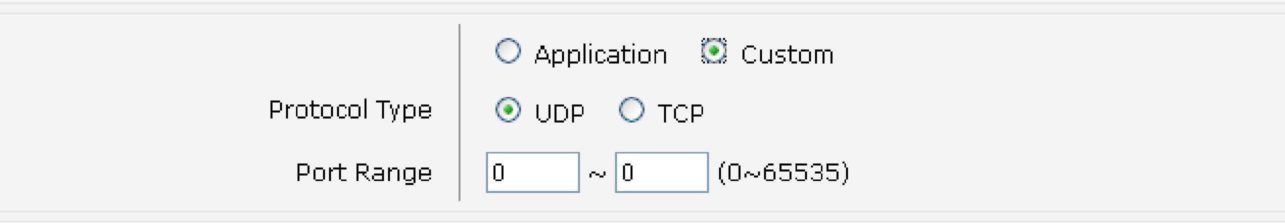
The following items are displayed on this screen:

- ► **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:



	○ Application ● Custom
Protocol Type	● UDP ○ TCP
Port Range	0 ~ 0 (0~65535)

Figure 3-65 Configure Custom of Qos Flow Rate Limit

The following items are displayed on this screen:

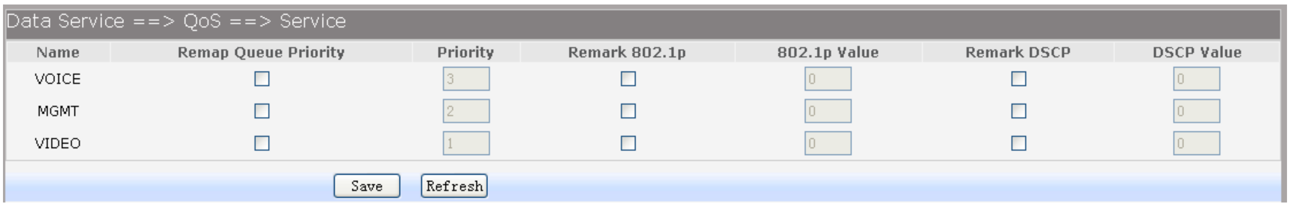
► **Protocol Type:** Custom protocol type, UDP or TCP.

► **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	□	3	□	0	□	0
MGMT	□	2	□	0	□	0
VIDEO	□	1	□	0	□	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.

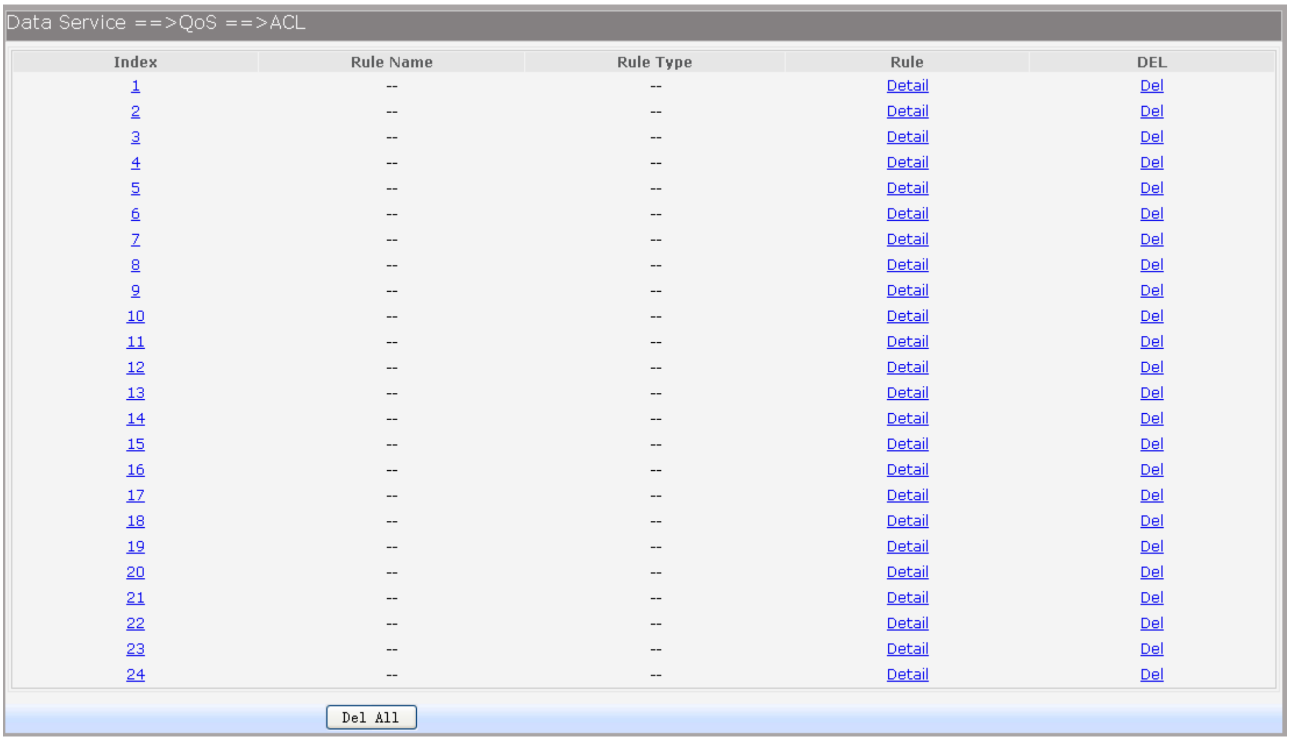
► **802.1p Value:** The value of remarking 802.1P.

► **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.



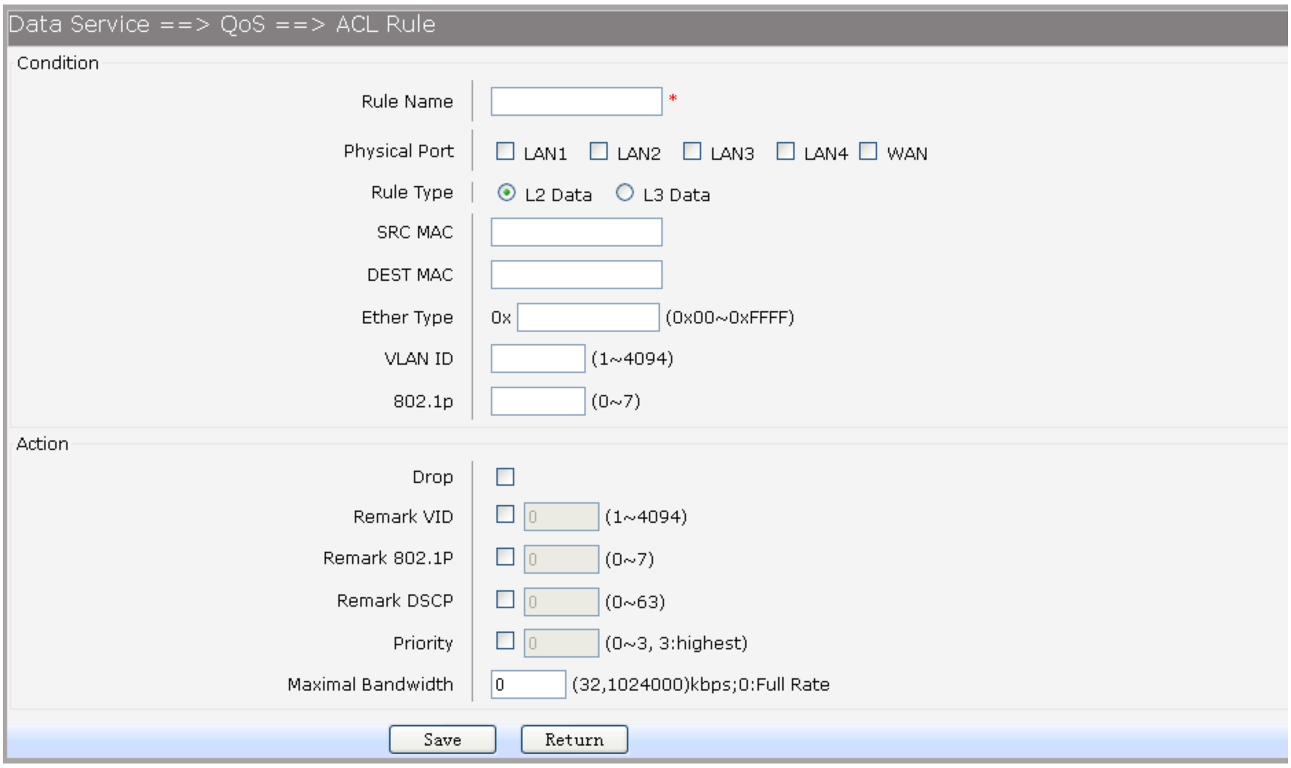
Data Service ==>QoS ==>ACL

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

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	*
Physical Port	□ LAN1 □ LAN2 □ LAN3 □ LAN4 □ WAN
Rule Type	● L2 Data ○ L3 Data
SRC MAC	
DEST MAC	
Ether Type	0x (0x00~0xFFFF)
VLAN ID	(1~4094)
802.1p	(0~7)

Action

Drop	□
Remark VID	□ 0 (1~4094)
Remark 802.1P	□ 0 (0~7)
Remark DSCP	□ 0 (0~63)
Priority	□ 0 (0~3, 3:highest)
Maximal Bandwidth	0 (32,1024000)kbps;0:Full Rate

Figure 3-68 Modify Qos ACL

The following items are display on this page:

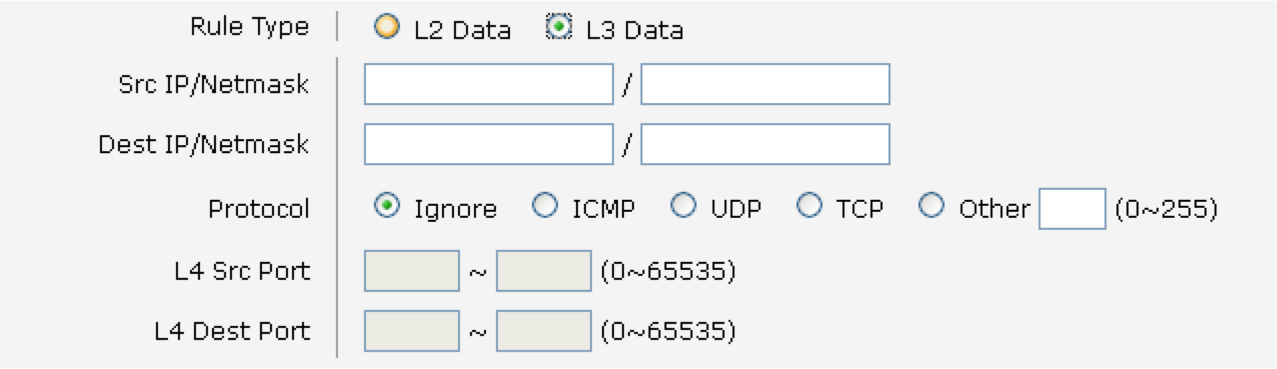
Condition:

► **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	○ L2 Data ● L3 Data
Src IP/Netmask	/
Dest IP/Netmask	/
Protocol	● Ignore ○ ICMP ○ UDP ○ TCP ○ Other (0~255)
L4 Src Port	~ (0~65535)
L4 Dest Port	~ (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.

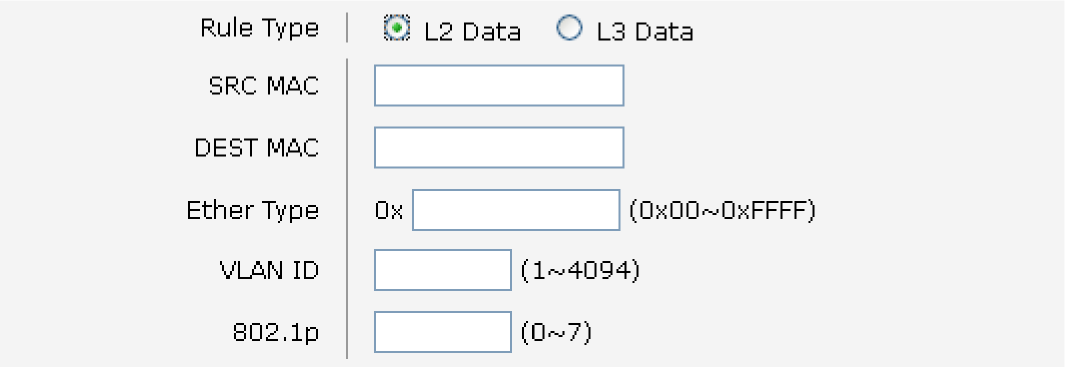
► **Dest IP/Netmask:** The destination IP address and netmask of packets.

► **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	● L2 Data ○ L3 Data
SRC MAC	
DEST MAC	
Ether Type	0x (0x00~0xFFFF)
VLAN ID	(1~4094)
802.1p	(0~7)

Figure 3-70 L2 Data Rule Type

The following items are display on this page:

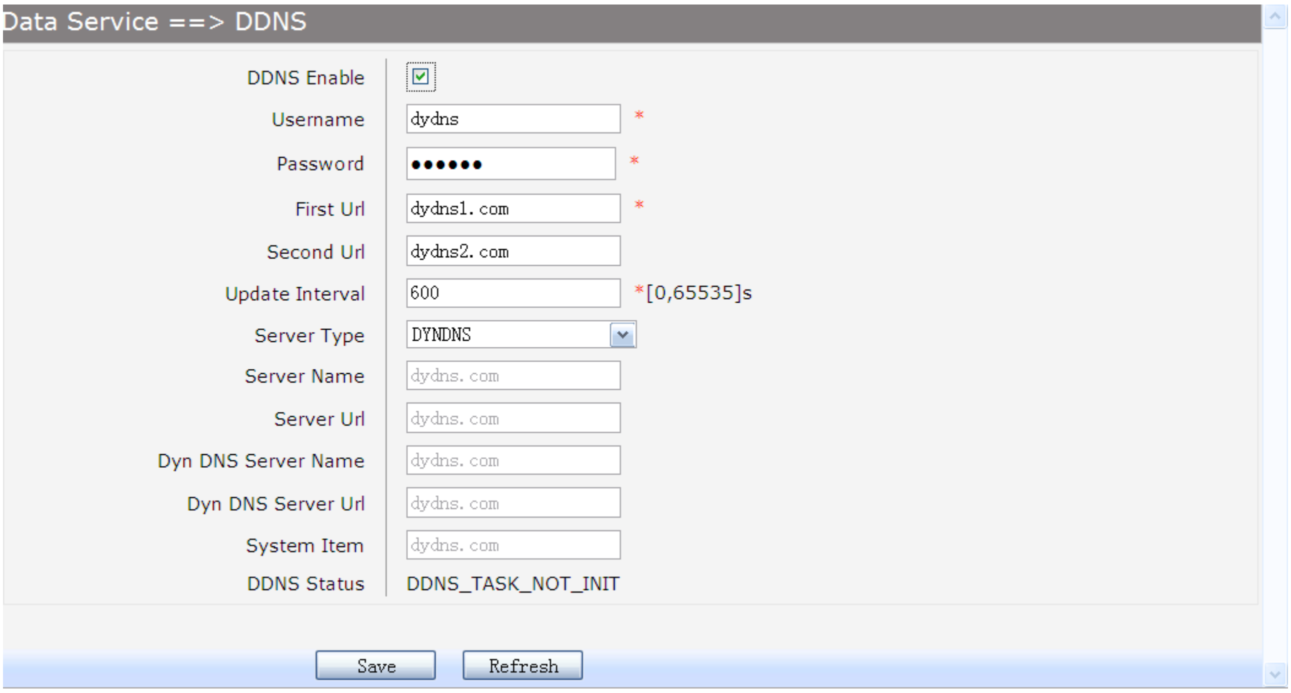
- ► **SRC MAC:** Source MAC address of packets.
- ► **DEST MAC:** Destination MAC address of packets.
- ► **Ether Type:** The ether type of packets.
- ► **VLAN ID:** The VLAN id of packets.
- ► **802.1p:** The VLAN priority of packets.

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.



Data Service ==> DDNS

DDNS Enable	☑
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

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.

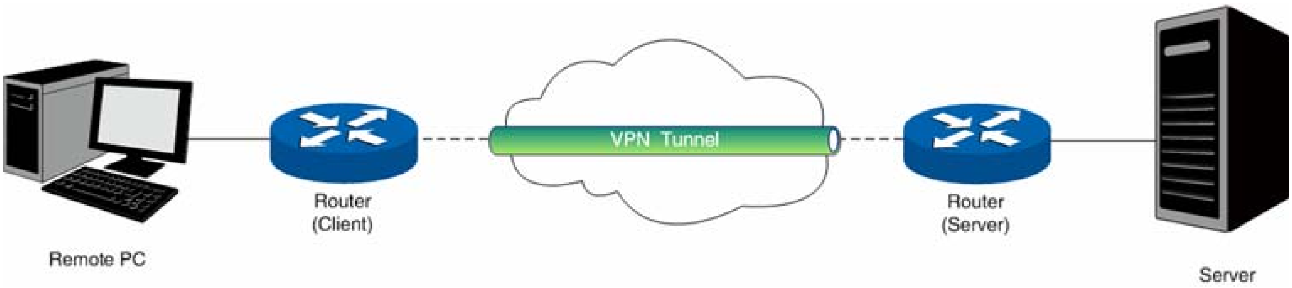


Figure 3-72 VPN – Network Topology

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

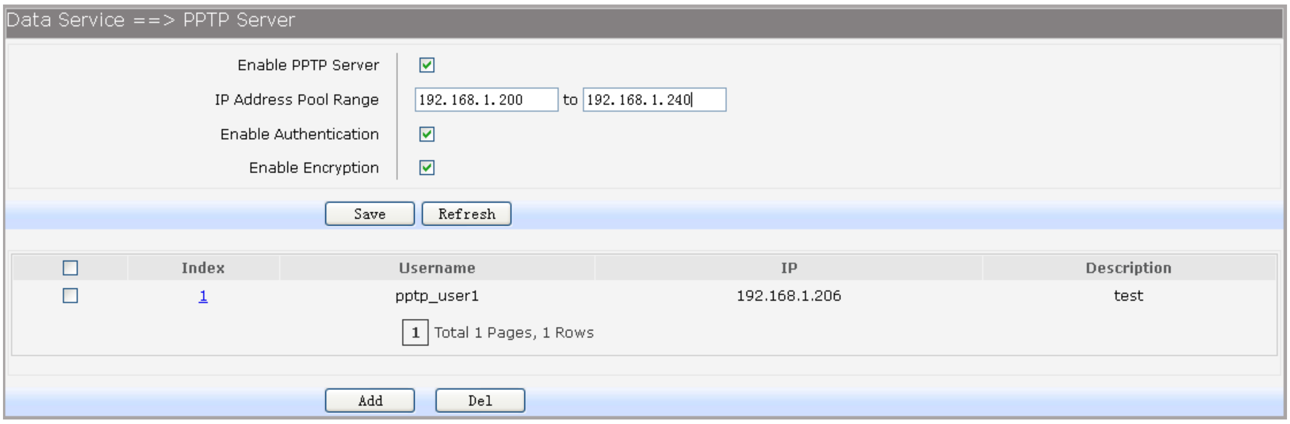
Layer 2 VPN tunneling protocol consists of L2TP (Layer 2 Tunneling Protocol) and PPTP (Point to Point Tunneling Protocol).Both L2TP and PPTP encapsulate packet and add extra header to the packet by using PPP (Point to Point Protocol).

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	192. 168. 1. 200 to 192. 168. 1. 240
Enable Authentication	☑
Enable Encryption	☑

□	Index	Username	IP	Description
□	1	pptp_user1	192.168.1.206	test

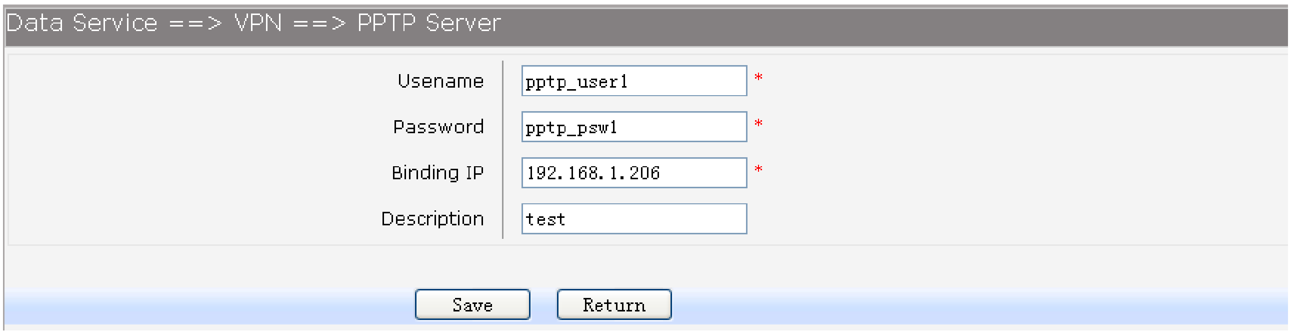
1 Total 1 Pages, 1 Rows

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

Usename	pptp_user1 *
Password	pptp_psw1 *
Binding IP	192. 168. 1. 206 *
Description	test

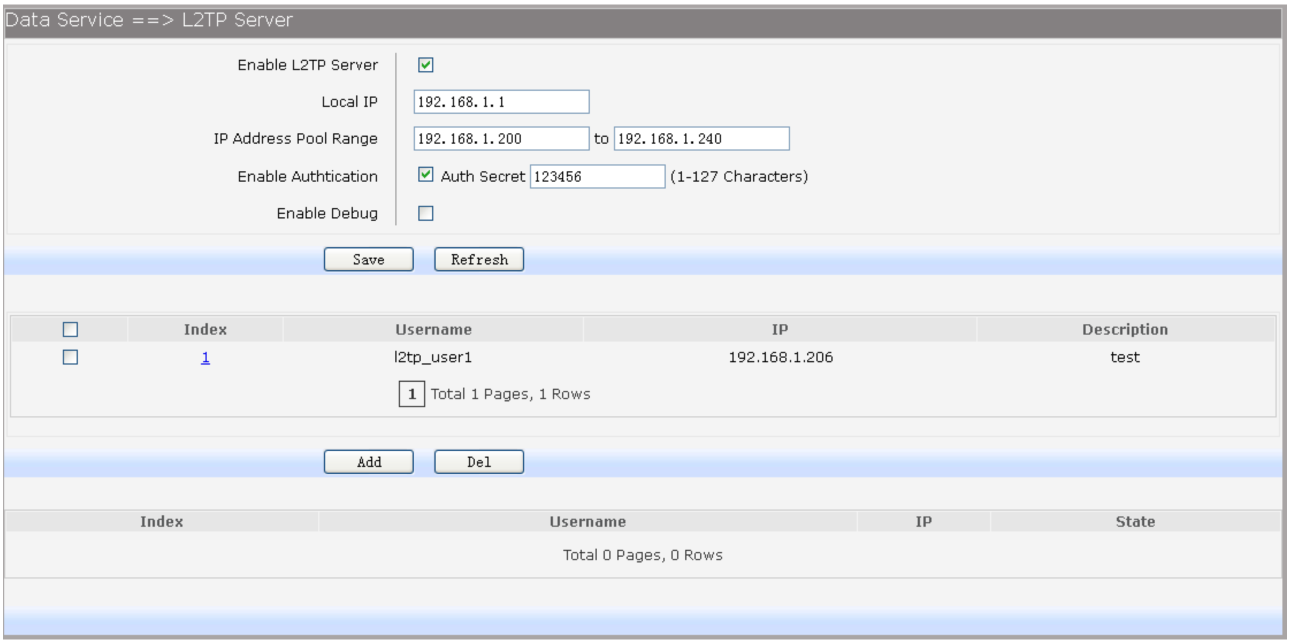
Figure 3-75 Add or Modify PPTP Client Entry

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	192. 168. 1. 1
IP Address Pool Range	192. 168. 1. 200 to 192. 168. 1. 240
Enable Authtication	☑ Auth Secret 123456 (1-127 Characters)
Enable Debug	□

□	Index	Username	IP	Description
□	1	l2tp_user1	192.168.1.206	test

1 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.

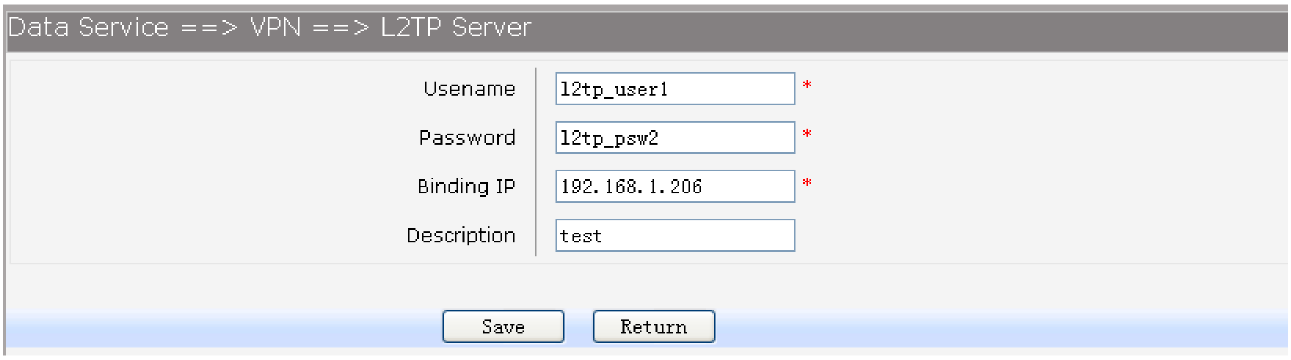
► **Local IP:** Enter the local IP address of L2TP server.

► **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

Usename	l2tp_user1 *
Password	l2tp_psw2 *
Binding IP	192. 168. 1. 206 *
Description	test

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

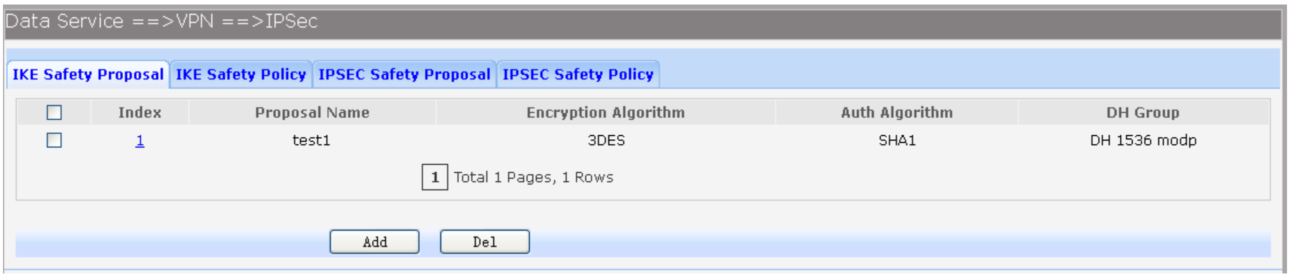
IPSEC (IP Security) is a set of services and protocols defined by IETF (Internet Engineering Task Force) to provide high security for IP packets and prevent attacks. To ensure a secured communication, the two IPSEC peers use IPSEC protocol to negotiate the data encryption algorithm and the security protocols 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.



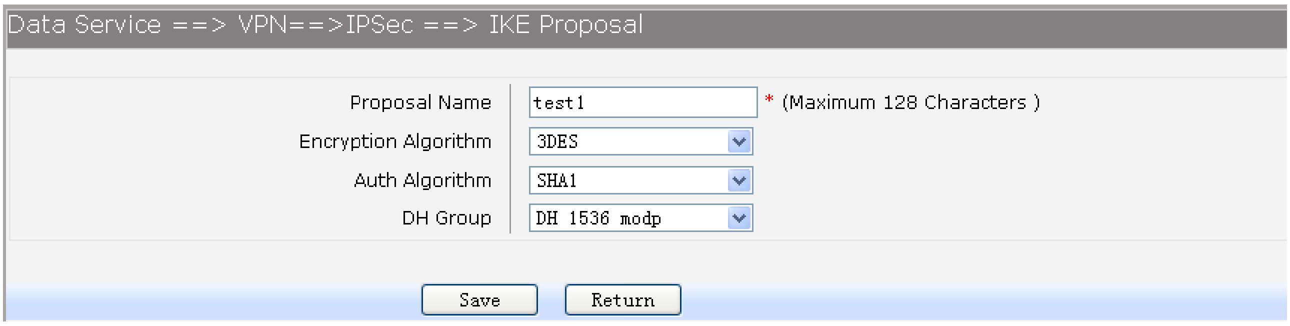
Data Service ==>VPN ==>IPSec

□	Index	Proposal Name	Encryption Algorithm	Auth Algorithm	DH Group
□	1	test1	3DES	SHA1	DH 1536 modp

1 Total 1 Pages, 1 Rows

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	test1 * (Maximum 128 Characters)
Encryption Algorithm	3DES
Auth Algorithm	SHA1
DH Group	DH 1536 modp

Figure 3-79 Add or Modify IKE Safety Proposal Entry

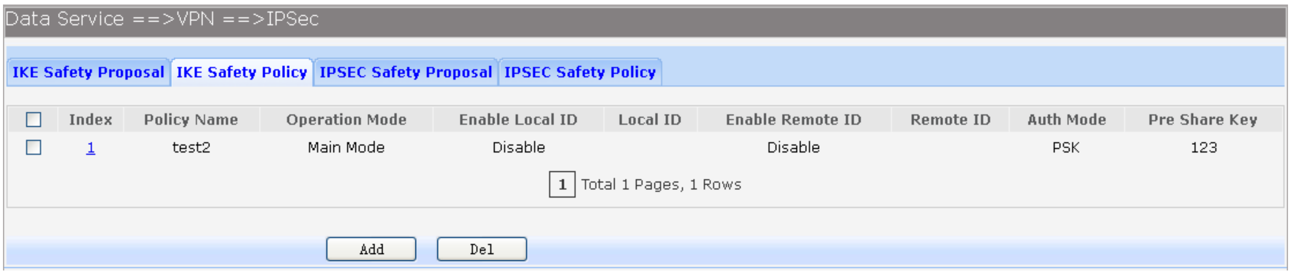
The following items are displayed on this screen:

- ► **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.



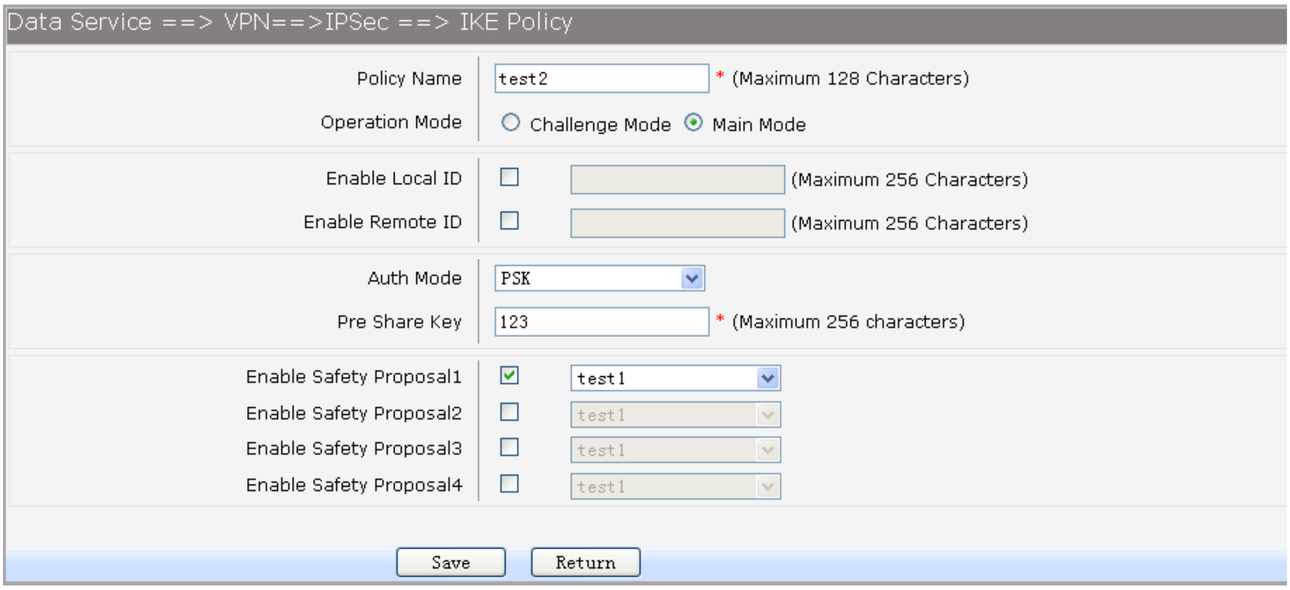
Data Service ==>VPN ==>IPSec

□	Index	Policy Name	Operation Mode	Enable Local ID	Local ID	Enable Remote ID	Remote ID	Auth Mode	Pre Share Key
□	1	test2	Main Mode	Disable		Disable		PSK	123

1 Total 1 Pages, 1 Rows

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	test2	* (Maximum 128 Characters)
Operation Mode	○ Challenge Mode ● Main Mode	
Enable Local ID	□	(Maximum 256 Characters)
Enable Remote ID	□	(Maximum 256 Characters)
Auth Mode	PSK	
Pre Share Key	123	* (Maximum 256 characters)
Enable Safety Proposal1	☑	test1
Enable Safety Proposal2	□	test1
Enable Safety Proposal3	□	test1
Enable Safety Proposal4	□	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:

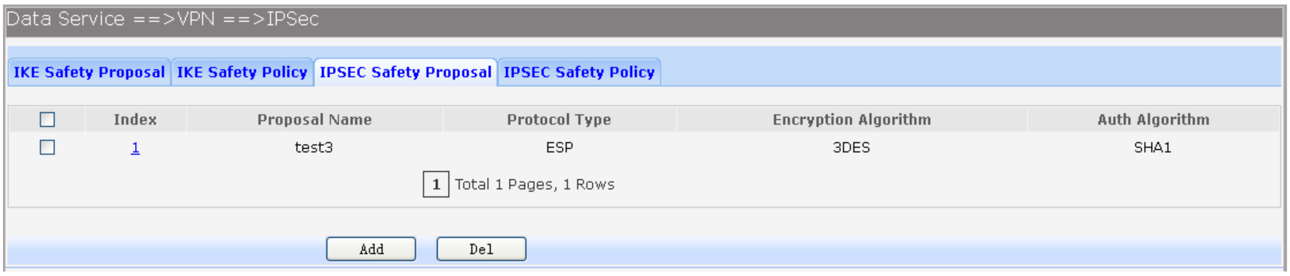
► **Pre Share Key:** Enter the Pre-shared Key for IKE authentication, and ensure both the two peers use the same key. The key should consist of visible characters without blank space.

► **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.

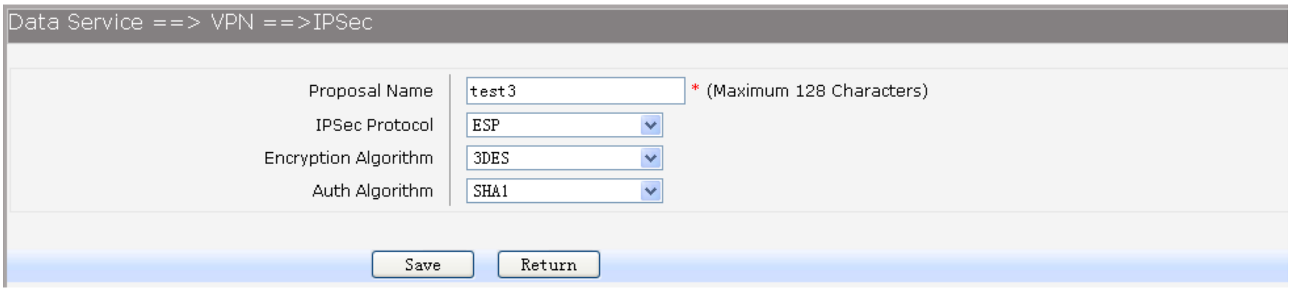

Data Service ==>VPN ==>IPSec

□	Index	Proposal Name	Protocol Type	Encryption Algorithm	Auth Algorithm
□	1	test3	ESP	3DES	SHA1

1 Total 1 Pages, 1 Rows

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

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:

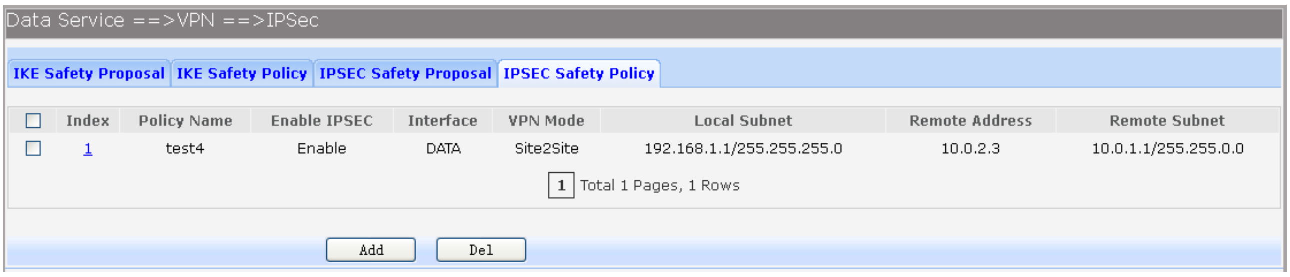
  MD5: MD5 (Message Digest Algorithm) takes a message of arbitrary length and generates a 128-bit message digest.

  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.



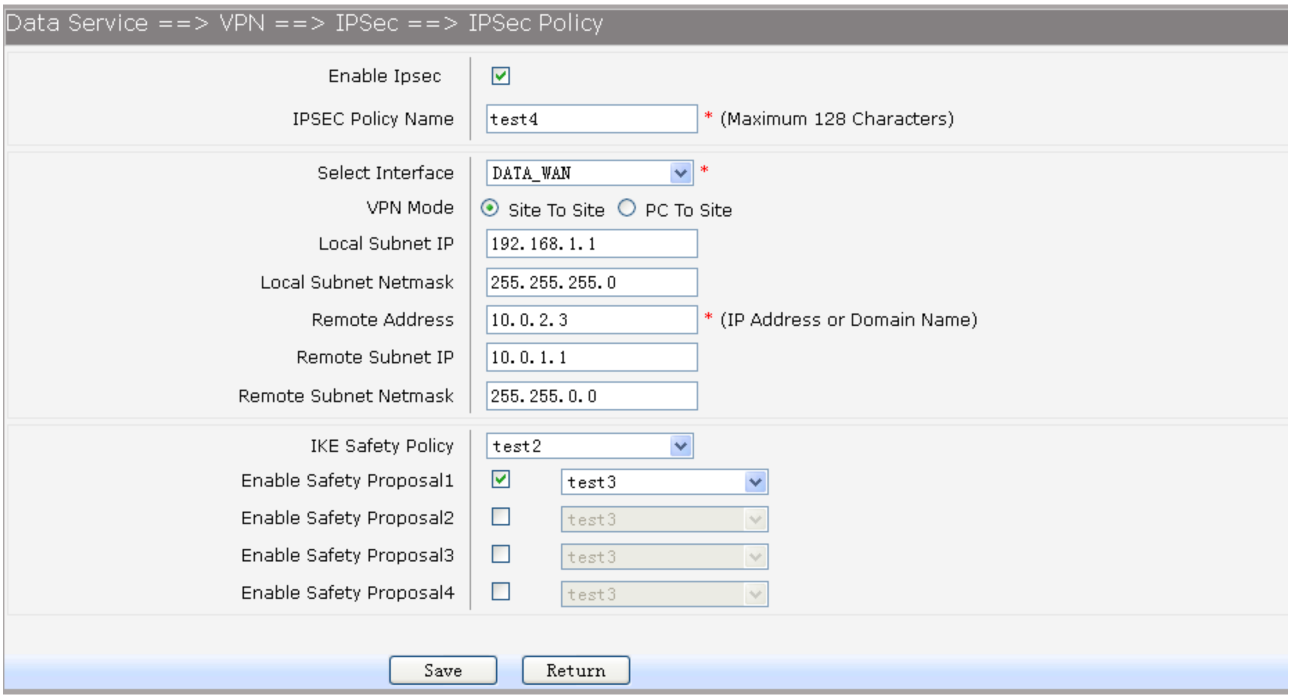
Data Service ==>VPN ==>IPSec

□	Index	Policy Name	Enable IPSEC	Interface	VPN Mode	Local Subnet	Remote Address	Remote Subnet
□	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

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 Ipsec	☑
IPSEC Policy Name	test4 * (Maximum 128 Characters)
Select Interface	DATA_WAN *
VPN Mode	● Site To Site ○ 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	☑ test3
Enable Safety Proposal2	□ test3
Enable Safety Proposal3	□ test3
Enable Safety Proposal4	□ test3

Figure 3-85 Add or Modify IPSEC Safety Policy Entry

The following items are displayed on this screen:

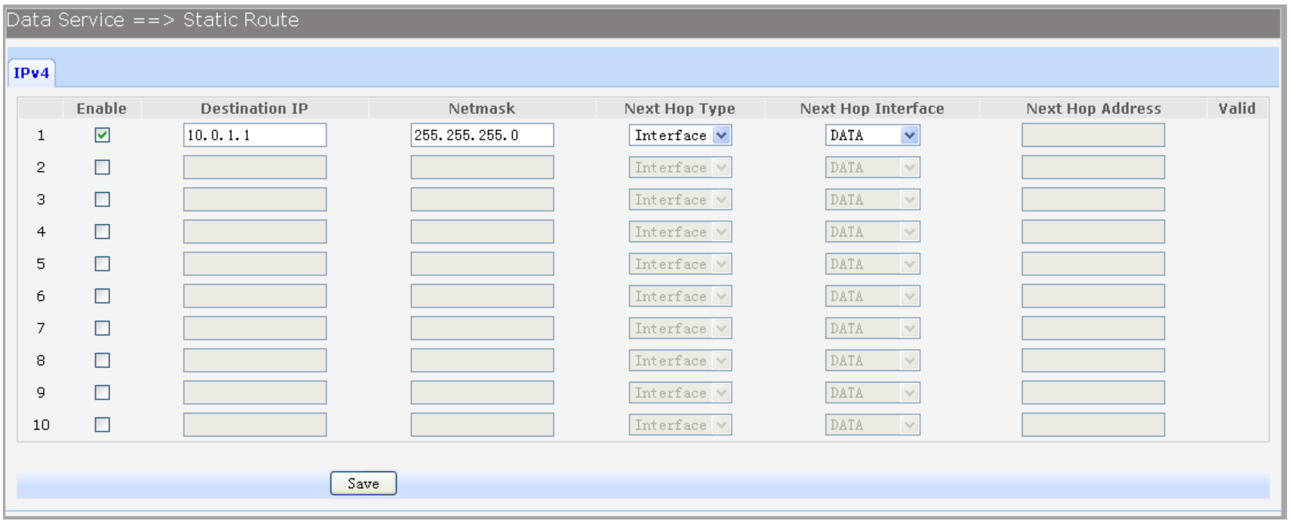
- **Enable Ipsec:** Enable or disable this IPSEC entry.
- **IPSEC Policy Name:** Specify a unique name to the IPSEC policy.
- **Select Interface:** Specify the local WAN port for this Policy.
- **VPN Mode:** Select the network mode for IPSEC policy. Options include:
  Site To Site: Select this option 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. 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.



Data Service ==> Static Route

	Enable	Destination IP	Netmask	Next Hop Type	Next Hop Interface	Next Hop Address	Valid
1	☑	10.0.1.1	255.255.255.0	Interface	DATA		
2	☐			Interface	DATA		
3	☐			Interface	DATA		
4	☐			Interface	DATA		
5	☐			Interface	DATA		
6	☐			Interface	DATA		
7	☐			Interface	DATA		
8	☐			Interface	DATA		
9	☐			Interface	DATA		
10	☐			Interface	DATA		

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

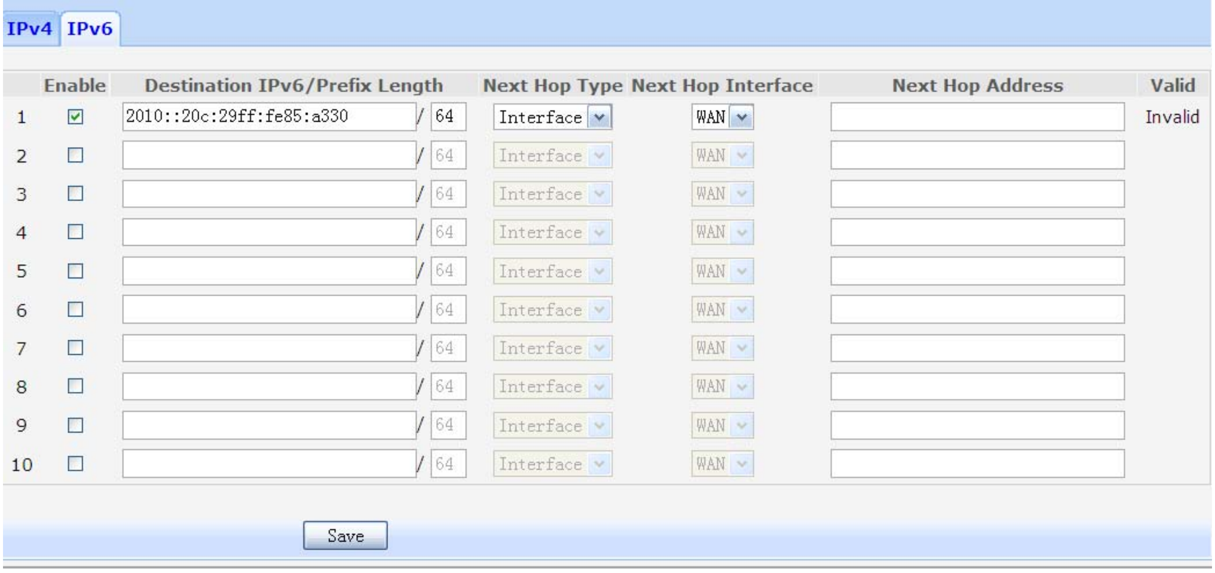
► **Next Hop Address:** Specify the address of next hop for current route

► **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.



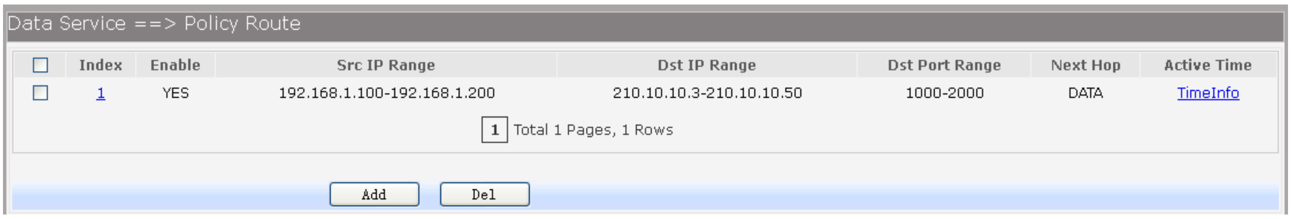
	Enable	Destination IPv6/Prefix Length		Next Hop Type	Next Hop Interface	Next Hop Address	Valid
1	☑	2010::20c:29ff:fe85:a330	/ 64	Interface	WAN		Invalid
2	☐		/ 64	Interface	WAN		
3	☐		/ 64	Interface	WAN		
4	☐		/ 64	Interface	WAN		
5	☐		/ 64	Interface	WAN		
6	☐		/ 64	Interface	WAN		
7	☐		/ 64	Interface	WAN		
8	☐		/ 64	Interface	WAN		
9	☐		/ 64	Interface	WAN		
10	☐		/ 64	Interface	WAN		

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.



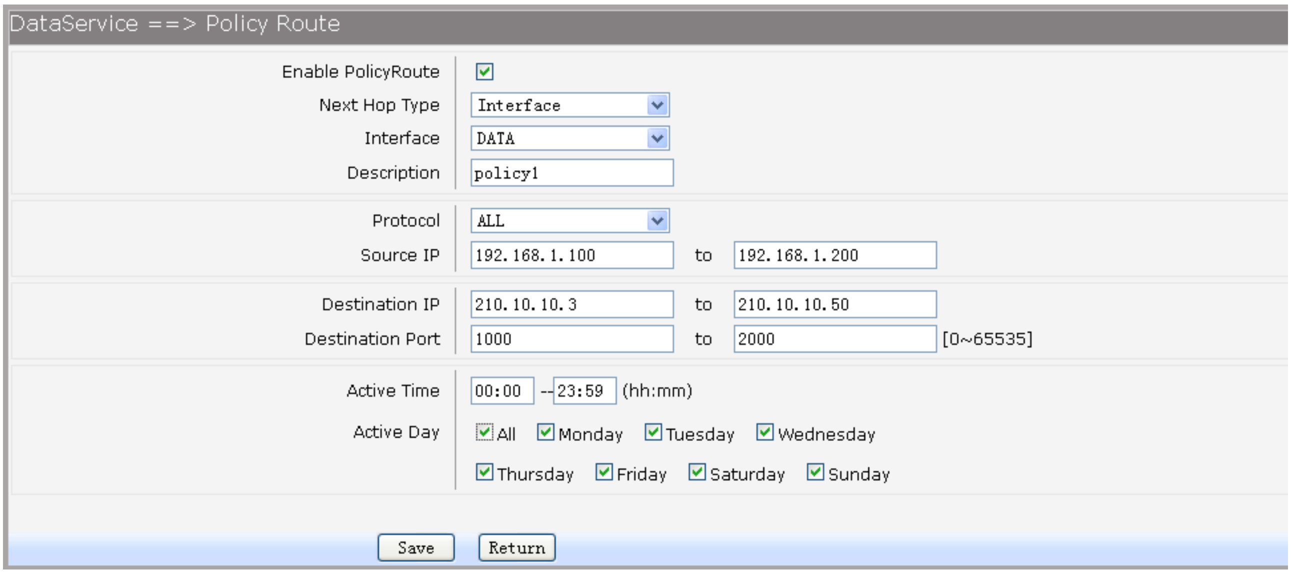
Data Service ==> Policy Route

□	Index	Enable	Src IP Range	Dst IP Range	Dst Port Range	Next Hop	Active Time
□	1	YES	192.168.1.100-192.168.1.200	210.10.10.3-210.10.10.50	1000-2000	DATA	TimeInfo

1 Total 1 Pages, 1 Rows

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

Figure 3-89 Add or Modify Policy Route

The following items are displayed on this page:

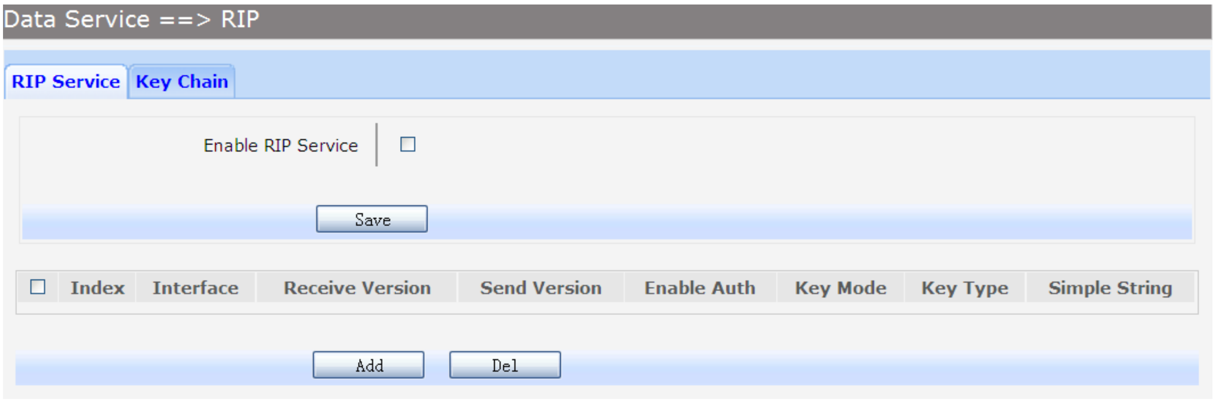
- **Enable PoliceRoute:** Enable or disable the entry
- **Next Hop Type:** Select from pull-down list: **Interface, Address.**
- **Interface:** Specify the interface of next hop for the entry.
- **Address:** Specify the address of next hop for the entry.
- **Description:** Give description for the entry.
- **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.



Data Service ==> RIP

Enable RIP Service | □

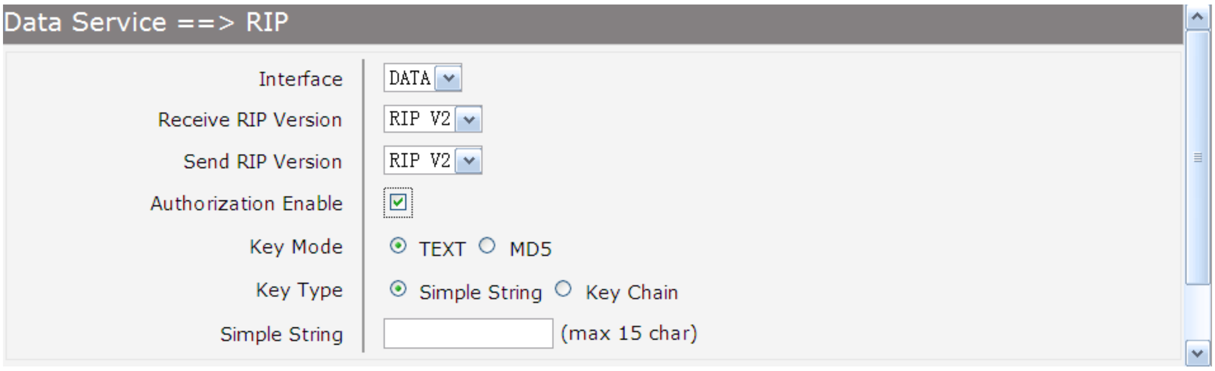
□	Index	Interface	Receive Version	Send Version	Enable Auth	Key Mode	Key Type	Simple String

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.



Data Service ==> RIP

Interface	DATA
Receive RIP Version	RIP V2
Send RIP Version	RIP V2
Authorization Enable	☑
Key Mode	● TEXT ○ MD5
Key Type	● Simple String ○ Key Chain
Simple String	(max 15 char)

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).

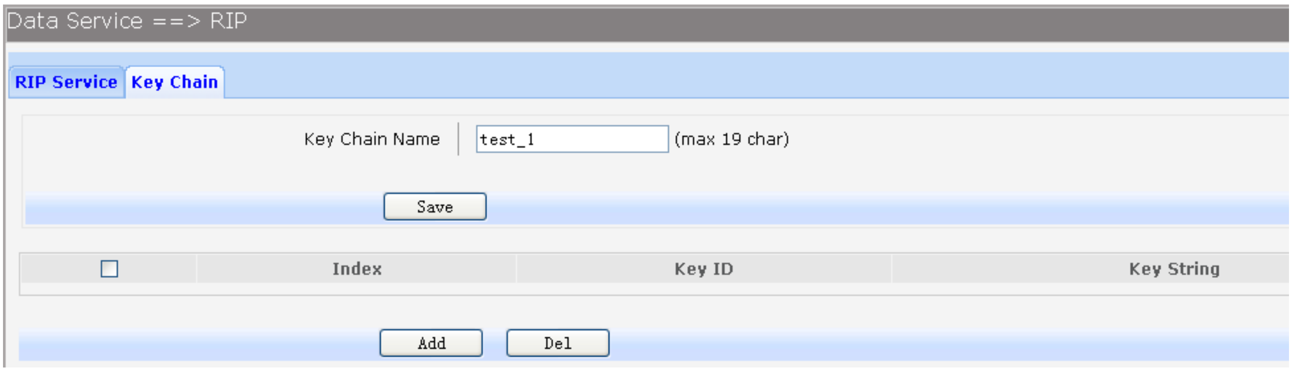
► **Key Type:** Specify the key from **Simple String** or **Key Chain**.

► **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

□	Index	Key ID	Key String

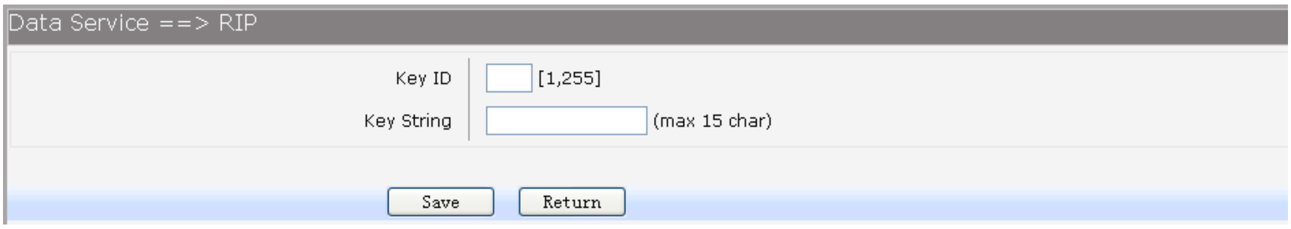
Add Del

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

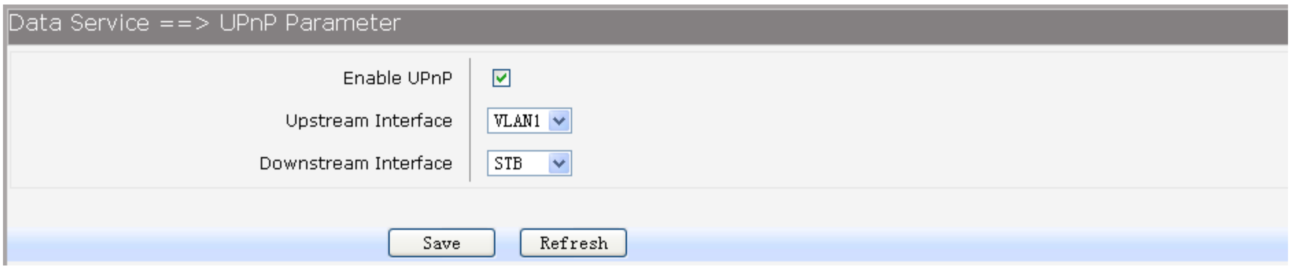
The Universal Plug and Play (UPnP) technology is enabling a world in which music and other digital entertainment content is accessible from various devices in the home without regard for where the media is stored. Using UPnP devices the whole family can share in the fun together whether it's:

- 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.



Data Service ==> UPnP Parameter

Enable UPnP ☑

Upstream Interface: VLAN1

Downstream Interface: STB

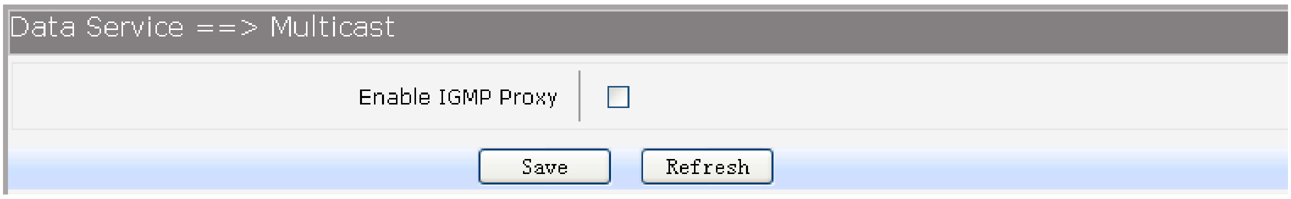
Figure 3-94 Configure UPnp

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.



Data Service ==> Multicast

Enable IGMP Proxy □

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.

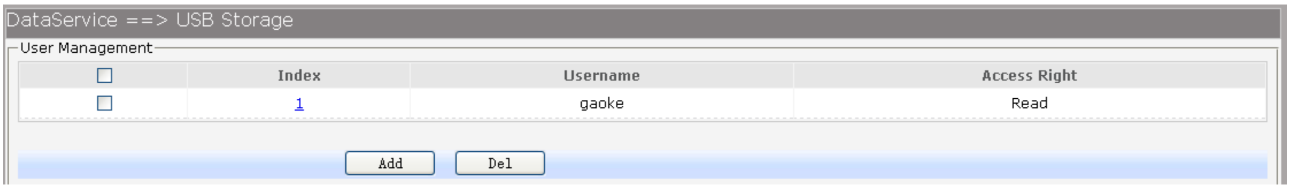
3.4.11 USB Storage

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.



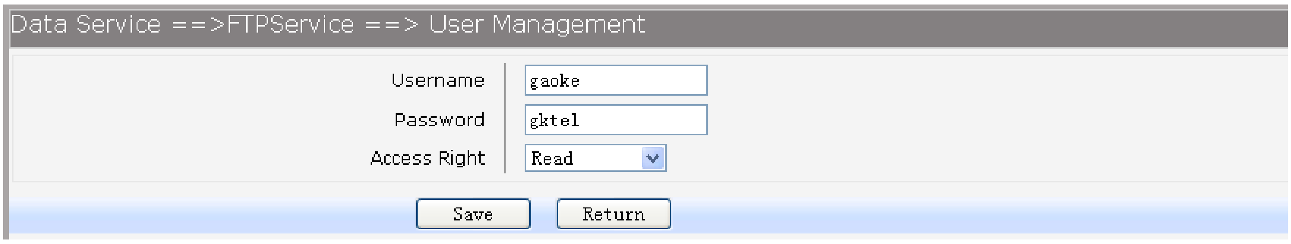
DataService ==> USB Storage

User Management

□	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.



Data Service ==>FTPService ==> User Management

Username: gaoke

Password: gktel

Access Right: Read

Figure 3-97 Add or Modify User Management Entry

The following items are displayed on this screen:

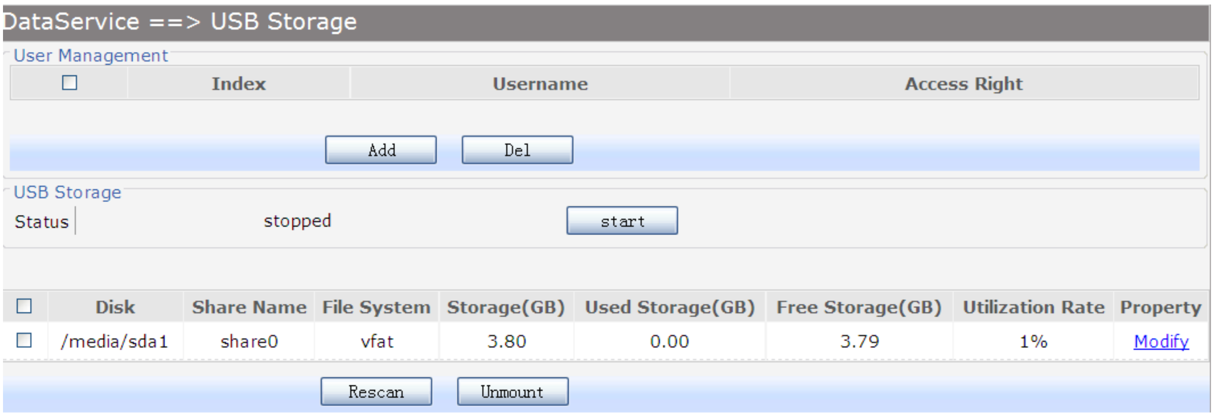
► **Username:** Enter user name of this entry.

► **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.



DataService ==> USB Storage

User Management

□	Index	Username	Access Right

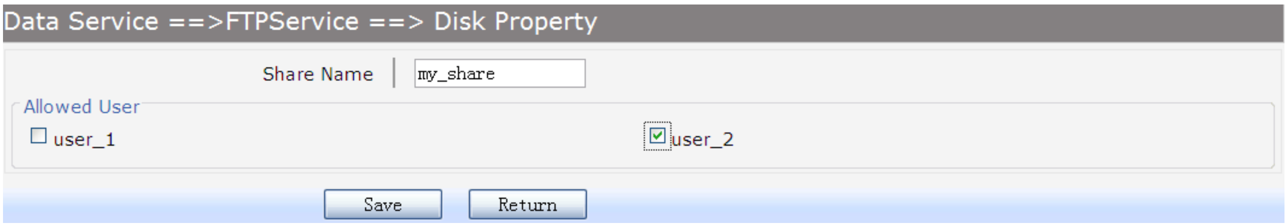
USB Storage

Status: stopped

□	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%	Modify

Figure 3-98 View USB Storage

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



Data Service ==>FTPService ==> Disk Property

Share Name: my_share

Allowed User

□ user_1 ☑ user_2

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 SIP Trunk Configuration

3.5.1 SIP

A IP Trunk is primarily a concurrent call that is routed over the IP backbone of a carrier using VoIP technology, the most popular protocol is Session Initiation Protocol(SIP). SIP trunk is a VoIP service based on the SIP by which Internet telephony service providers (ITSPs) deliver telephone services and unified communication to customers equipped with private branch exchange (IP-PBX) facilities.

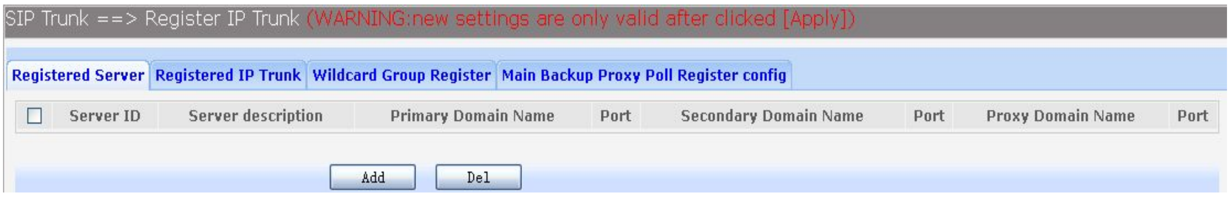
3.5.2 Introduction about SIP

- SIP
  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.
- IMS
  IMS widely known as IP Multimedia Subsystem is an IP multimedia and telephony core network that is defined by 3GPP and 3GPP2 standards and organizations based on IETF Internet protocols. IMS is a set of specifications that describes the Next Generation Networking (NGN) architecture for implementing IP based telephony and multimedia services. It defines a complete architecture and framework that enables the integration of voice, video, data and mobile network technology over an IP-based infrastructure.
- Related Parameters
  - IP Trunk Group: Each account is required to specify a SIP trunk group number which will be used in the call route.
  - Phone Number: Used to bind SIP account with subscriber. The subscriber which configured this number as caller number will select this account to callout, and the subscriber which configured this number as external called number will ring when call in from this account.
  - Authentication User Name: The user name for SIP authentication. The user account will be used for authentication if this parameter leaves blank.

3.5.3 Registered Server

More IP trunk accounts can be configured in device, and each account can be registered to different SIP server.

Choose the menu **SIP Trunk→Register IP Trunk→Registered Server** to load the following page.

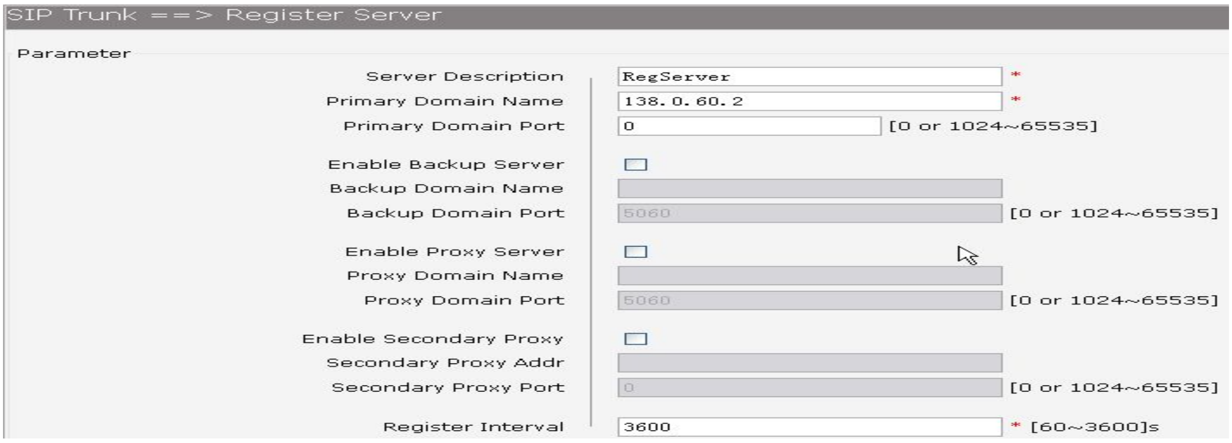


SIP Trunk ==> Register IP Trunk (WARNING:new settings are only valid after clicked [Apply])

□	Server ID	Server description	Primary Domain Name	Port	Secondary Domain Name	Port	Proxy Domain Name	Port

Figure 3-100 Registered Server List

On click **Add** button to load the following page.



SIP Trunk ==> Register Server

Parameter

Server Description	RegServer	*
Primary Domain Name	138. 0. 60. 2	*
Primary Domain Port	0	[0 or 1024~65535]
Enable Backup Server	□	
Backup Domain Name		
Backup Domain Port	5060	[0 or 1024~65535]
Enable Proxy Server	□	
Proxy Domain Name		
Proxy Domain Port	5060	[0 or 1024~65535]
Enable Secondary Proxy	□	
Secondary Proxy Addr		
Secondary Proxy Port	0	[0 or 1024~65535]
Register Interval	3600	* [60~3600]s

Figure 3-101 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.

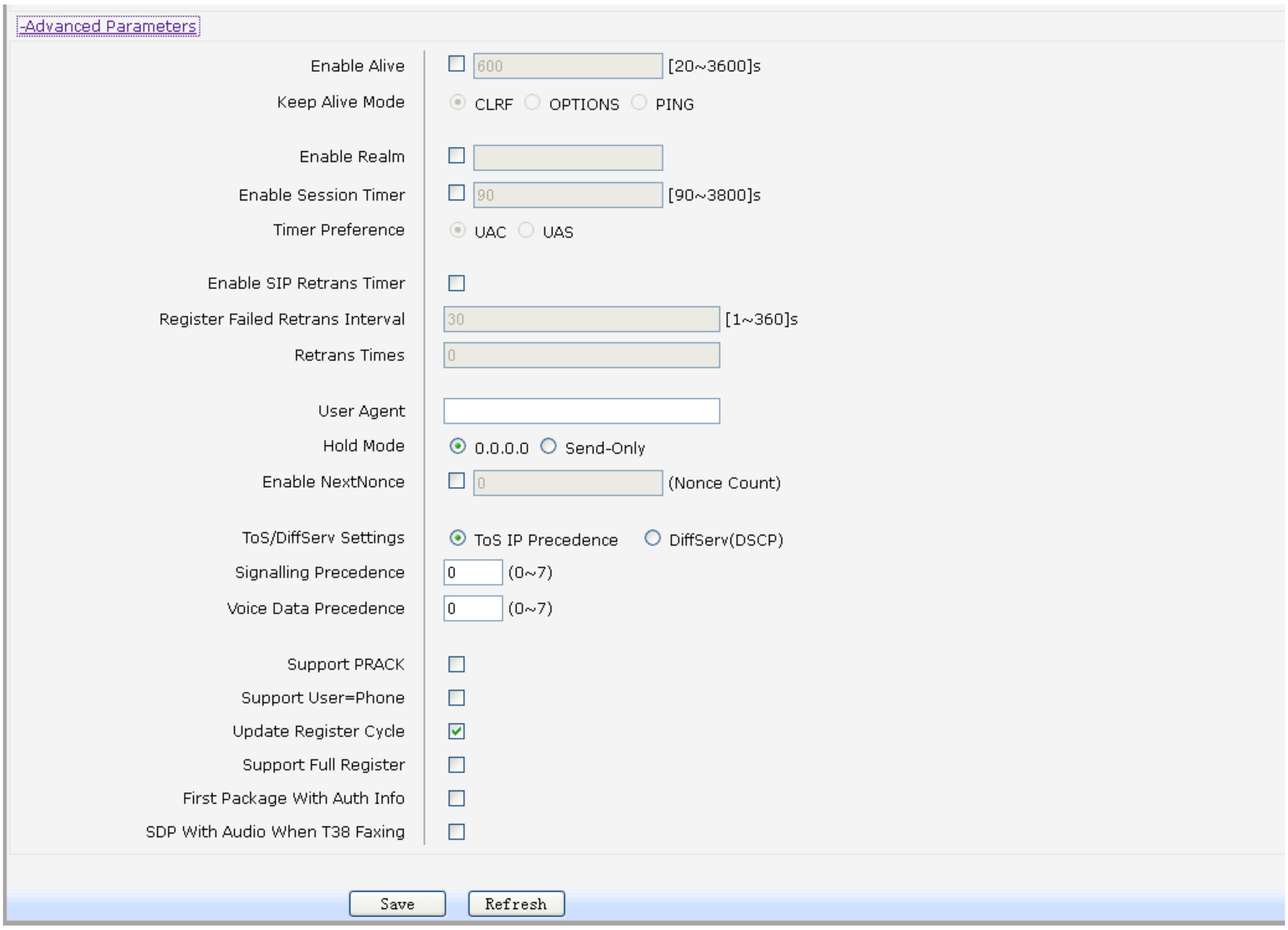
► **Enable Secondary Proxy:** Enable or disable backup proxy server.

► **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 in which sip UA will send register message.

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



-Advanced Parameters

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

Figure 3-102 Advanced Parameters of SIP Service

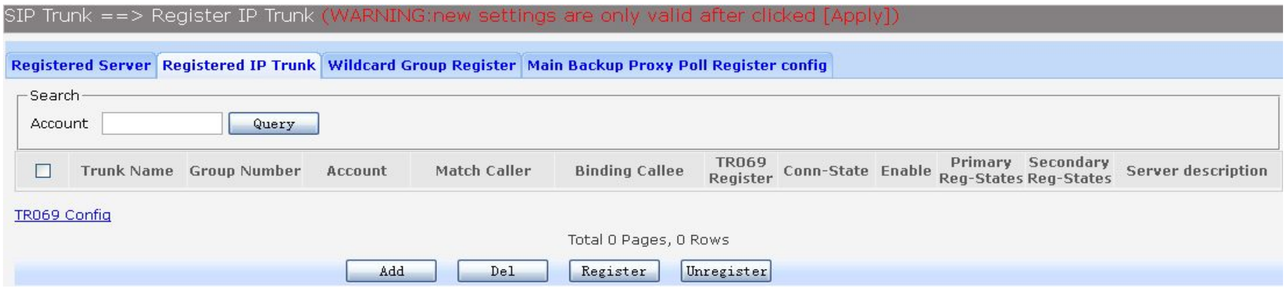
The following items are displayed on this screen:

- ► **Enable Alive:** After successful registration, whether or not 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 or not 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 or not SIP signaling packets with User = Phone field information.
- ► **Update Register Cycle:** Based on server response to update registering period.
- ► **Support Full Register:** Each registering 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.

3.5.4 Register IP Trunk

Add SIP account, the most important parameters are SIP account, password, SIP Server, IP trunk group, binding callee and matched caller.

Choose the menu **SIP Trunk→Register IP Trunk→Registered IP Trunk** to load the following page.


SIP Trunk ==> Register IP Trunk (WARNING:new settings are only valid after clicked [Apply])

Search

Account [ ] Query

□	Trunk Name	Group Number	Account	Match Caller	Binding Callee	TR069 Register	Conn-State	Enable	Primary Reg-States	Secondary Reg-States	Server description

TR069 Config

Total 0 Pages, 0 Rows

Figure 3-103 Registered IP Trunk List

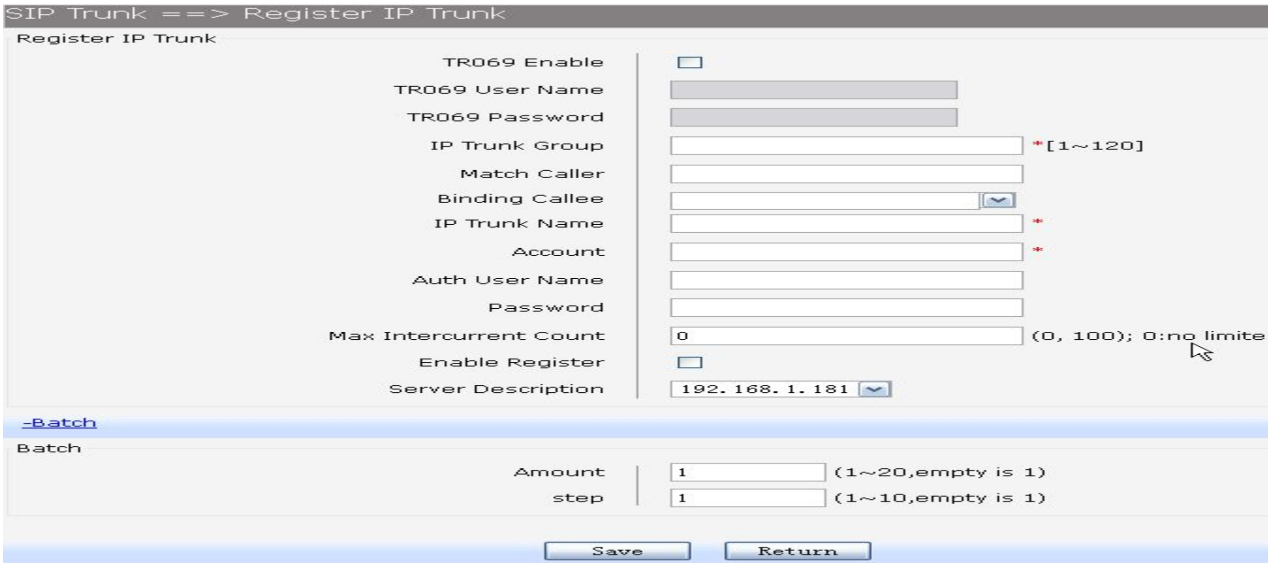
The following items are displayed on this screen:

► **Query:** Filtering out the specified accounts.

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

► **Unregister:** Click the **Unregister** button to end the registering to the SIP server.

On click **Add** button to load following page.


SIP Trunk ==> Register IP Trunk

Register IP Trunk

TR069 Enable	□
TR069 User Name	
TR069 Password	
IP Trunk Group	*[1~120]
Match Caller	
Binding Callee	
IP Trunk Name	*
Account	*
Auth User Name	
Password	
Max Intercurrent Count	0 (0, 100); 0:no limite
Enable Register	□
Server Description	192.168.1.181

-Batch

Batch

Amount	1 (1~20,empty is 1)
step	1 (1~10,empty is 1)

Figure 3-104 Parameters of Registered IP Trunk

The following items are displayed on this screen:

► **IP Trunk Group**: Each account is required to specify one SIP trunk group number which will be used in the call routing.

► **Match Caller:** When caller number match the number in whole or in part, then call out with this IP trunk account.

► **Binding Callee**: When one incoming call arrives, the called number of all the account will be matched and routed.

► **IP Trunk Name**: The description of IP Trunk.

► **Account**: The registering account provided by SS Platform.

► **Auth User Name**: The user name for SIP authentication. The user account will be used for authentication if this parameter leave blank.

► **Password**: Authentication password.

► **Max Intercurrent Count**: The maximum of concurrent calls in the same time for the account.

► **Enable Register**: Enable or disable registering.

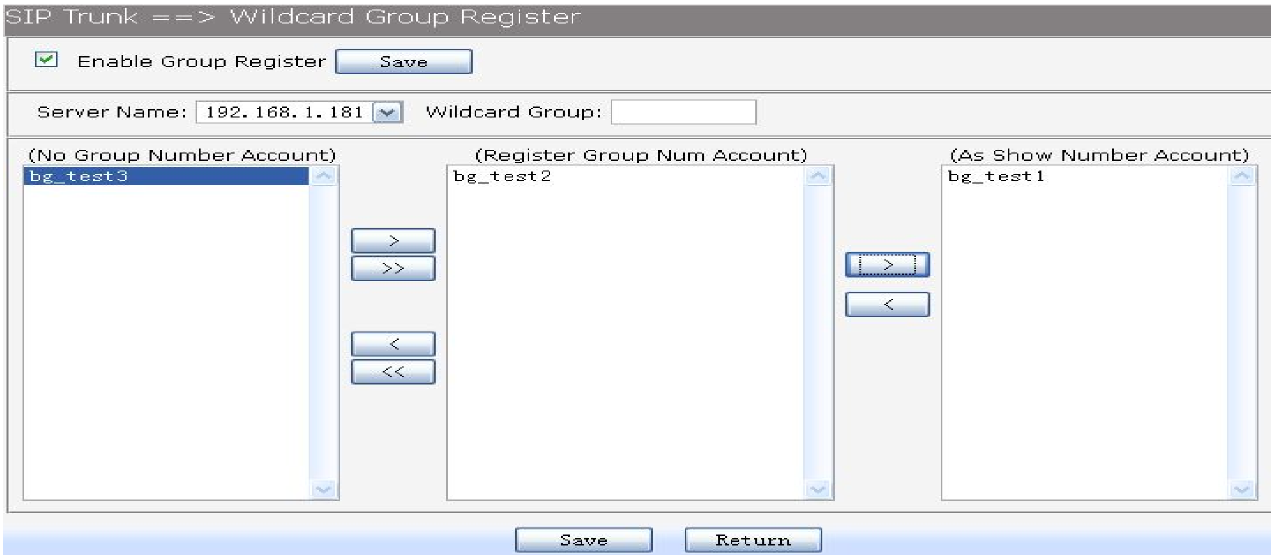
► **Server Description**: Server IP or domain.

►**Batch**: Increase in bulk registered IP trunk account, account name and authentication name.

3.5.5 Wildcard Group Register

This function must be supported by SIP server or IMS platform, in order to reduce the number of registering packets. Registered IP trunk accounts are divided into groups. Each group only one account registers to the server. If this account is registered, then all accounts are registered in this group.

Choose the menu **SIP Trunk→Register IP Trunk→Wildcard Group Register** to load the following page.



SIP Trunk ==> Wildcard Group Register

☑ Enable Group Register

Server Name: 192.168.1.181 Wildcard Group:

(No Group Number Account) bg_test3

(Register Group Num Account) bg_test2

(As Show Number Account) bg_test1

Figure 3-105 Parameters of Wildcard Group Register

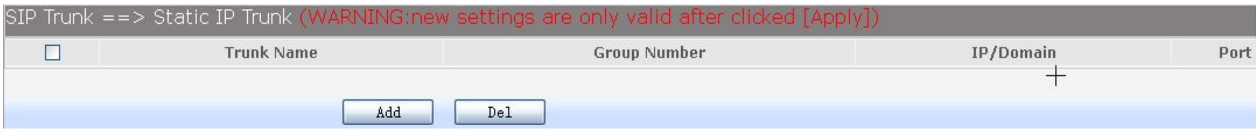
► **Enable Group Register**: Whether or not to enable the group registering.

3.5.6 Static IP Trunk

Static IP trunk is used for peer-to-peer connecting with other media gateway.

3.5.6.1 Configuration instructions

Choose the menu **SIP Trunk→Static IP Trunk** to load the following page.

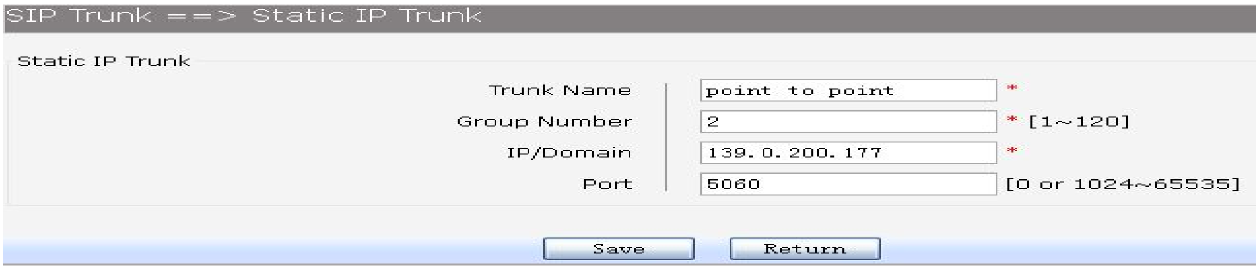


SIP Trunk ==> Static IP Trunk (WARNING:new settings are only valid after clicked [Apply])

□	Trunk Name	Group Number	IP/Domain	Port

Figure 3-106 Static IP Trunk List

On click **Add** button to load the following page.



SIP Trunk ==> Static IP Trunk

Static IP Trunk

Trunk Name	point to point	*
Group Number	2	* [1~120]
IP/Domain	139.0.200.177	*
Port	5060	[0 or 1024~65535]

Figure 3-107 Parameters of Static IP Trunk

The following items are displayed on this screen:

► **Trunk Name**: The description of the trunk.

► **Group Number**: Each static IP trunk is required to specify a SIP trunk group number which will be used in the call routing.

► **IP/Domain**: IP address or domain of remote device.

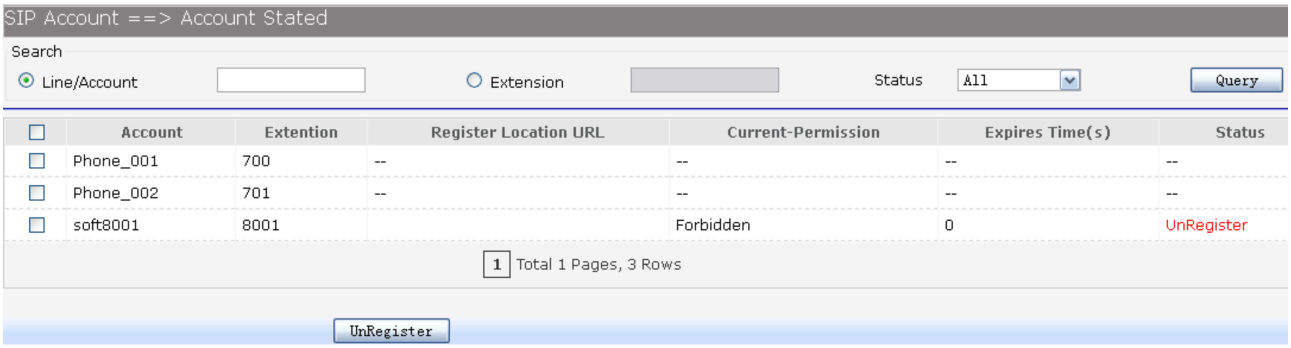
► **Port**: Service port of remote device.

3.6 SIP Account Configuration

3.6.1 SIP Account Status

As a sip server, it can provide registered authentication service for each account.

Choose the menu **SIP Account→SIP Account Status** to load the following page.



SIP Account ==> Account Stated

Search

● Line/Account ○ Extension Status All Query

□	Account	Extention	Register Location URL	Current-Permission	Expires Time(s)	Status
□	Phone_001	700	--	--	--	--
□	Phone_002	701	--	--	--	--
□	soft8001	8001		Forbidden	0	UnRegister

1 Total 1 Pages, 3 Rows

Figure 3-108 Account Status List

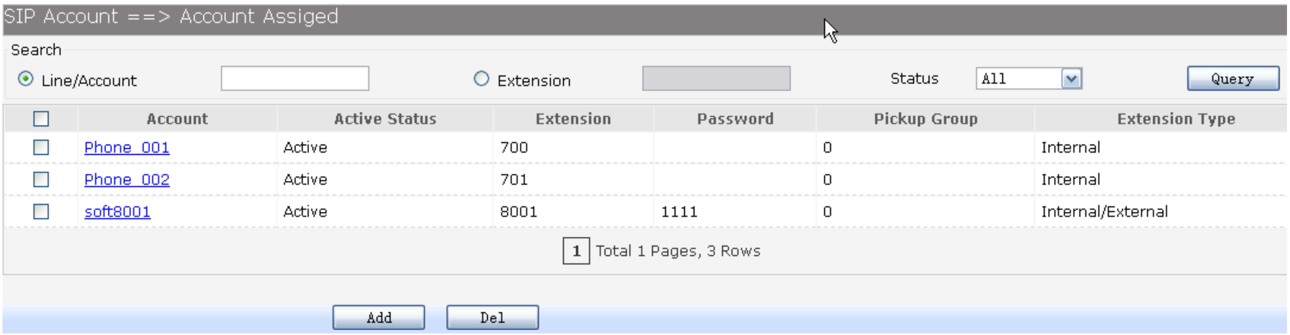
The following items are displayed on this screen:

►**Query**: Search the interested accounts, which can be based on the account name, extension number and registering status.

►**UnRegister**: Force to change registering status to unregistered status for selected accounts.

3.6.2 SIP Account Assign

User can add, delete and modify accounts in this page. Choose the menu **SIP Account→SIP Account Status** to load the following page.



SIP Account ==> Account Assiged

Search

● Line/Account ○ Extension Status All Query

□	Account	Active Status	Extension	Password	Pickup Group	Extension Type
□	Phone_001	Active	700		0	Internal
□	Phone_002	Active	701		0	Internal
□	soft8001	Active	8001	1111	0	Internal/External

1 Total 1 Pages, 3 Rows

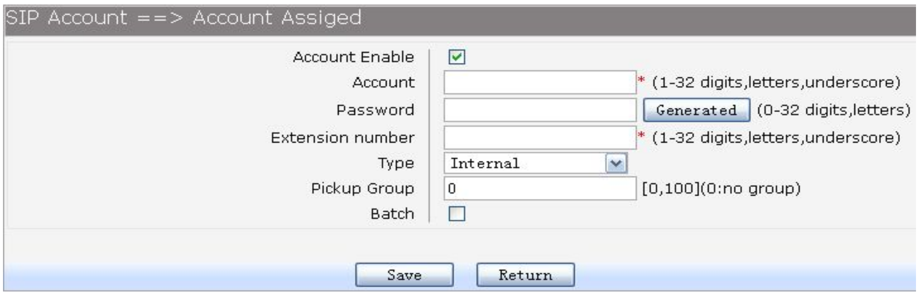
Figure 3-109 Account Assign

The following items are displayed on this screen:

►**Query**: Search the interested accounts, which can be based on the account name, extension number, registering status.

►**Del**: Delete the selected accounts.

►**Add**: On click **Add** button to load the following page.



SIP Account ==> Account Assiged

Account Enable	☑	
Account		* (1-32 digits,letters,underscore)
Password	Generated	(0-32 digits,letters)
Extension number		* (1-32 digits,letters,underscore)
Type	Internal	
Pickup Group	0	[0,100](0:no group)
Batch	□	

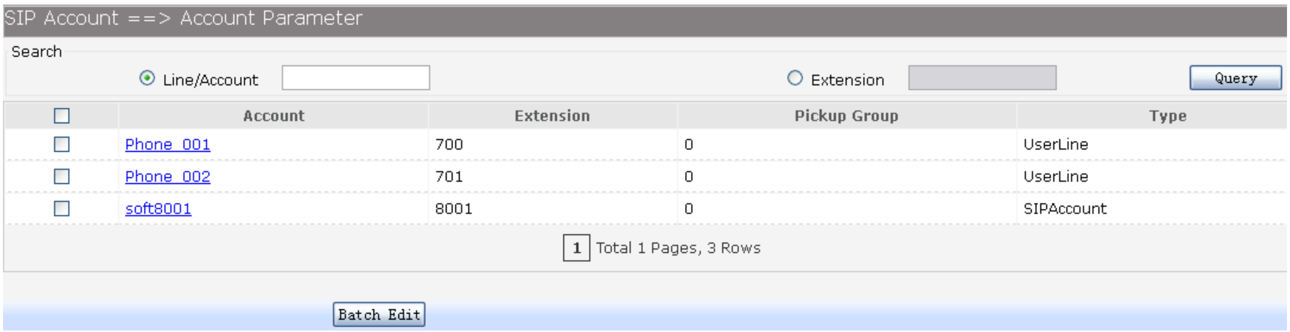
Figure 3-110 Parameters of SIP Account

►**Generated**: Generate a random password.

►**Batch**: Increase in batch SIP account, account name and password.

3.6.3 Account Parameter

Choose the menu **SIP Account→Account Parameter** to load the following page.



SIP Account ==> Account Parameter

Search

● Line/Account ○ Extension

□	Account	Extension	Pickup Group	Type
□	Phone_001	700	0	UserLine
□	Phone_002	701	0	UserLine
□	soft8001	8001	0	SIPAccount

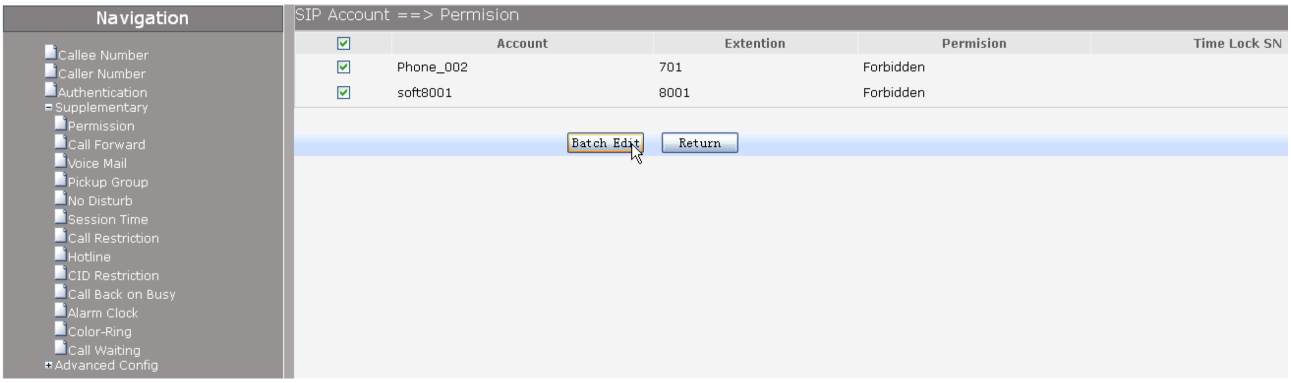
1 Total 1 Pages, 3 Rows

Figure 3-111 Account List

The following items are displayed on this screen:

►**Query**: Search the interested accounts, which can be based on the account name, extension number, registering status.

►**Batch Edit**: Configure multiple accounts at once for the same parameters. Select accounts, on click **Batch Edit** button to load the following page.



SIP Account ==> Permision

☑	Account	Extention	Permision	Time Lock SN
☑	Phone_002	701	Forbidden	
☑	soft8001	8001	Forbidden	

Figure 3-112 Menu List of Batch Edit

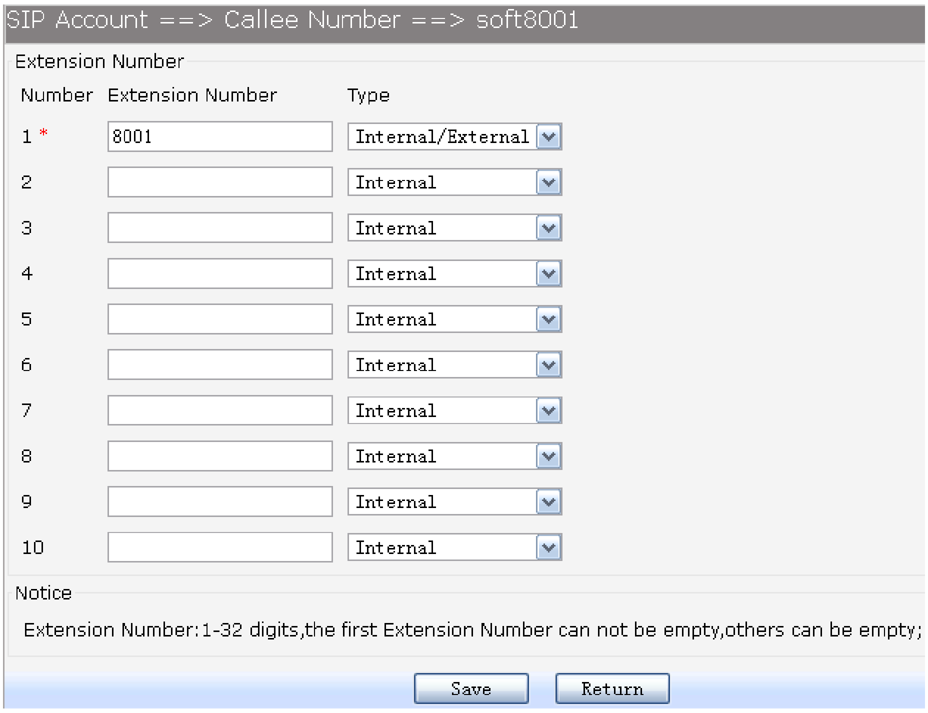
Note：

This document don't introduce to modify parameter in batch, Because a single account configuration will be referred。

3.6.3.2 Called Number

Called number is just the phone number. The device defines two types of called number, internal called number and external called number. The internal called number is only use for internal calls, the external called number is use for Direct Inward Dialing (DID). The device supports up to 10 called numbers, the first called number, also named extension number, should be unique in order to distinguish each extension.

Choose the menu **SIP Account→Account Parameter→Callee Number** to load the following page.



SIP Account ==> Callee Number ==> soft8001

Extension Number

Number	Extension Number	Type
1 *	8001	Internal/External
2		Internal
3		Internal
4		Internal
5		Internal
6		Internal
7		Internal
8		Internal
9		Internal
10		Internal

Notice

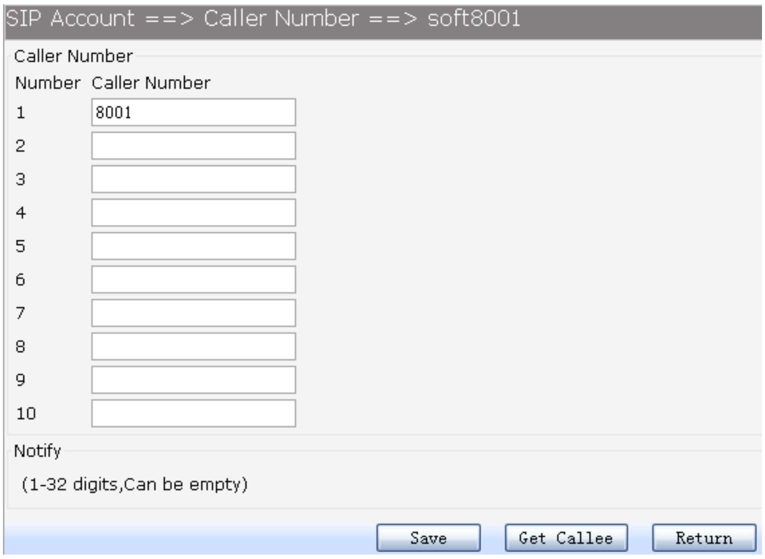
Extension Number:1-32 digits,the first Extension Number can not be empty,others can be empty;

Figure 3-113 Called Number

3.6.3.3 Caller Number

Caller number is usually used for caller identifier display (CID). The device supports up to 10 caller number, you can select different caller number when you call out from different trunk. The first group of caller number is used for internal calls. You can select the group number of outbound calls when configuring the call routing.

Choose the menu **SIP Account→Account Parameter→Caller Number** to load the following page.



SIP Account ==> Caller Number ==> soft8001

Caller Number

Number	Caller Number
1	8001
2	
3	
4	
5	
6	
7	
8	
9	
10	

Notify

(1-32 digits,Can be empty)

Figure 3-114 Caller Number

►**Get Callee**: Get called number and configure to Caller ID.

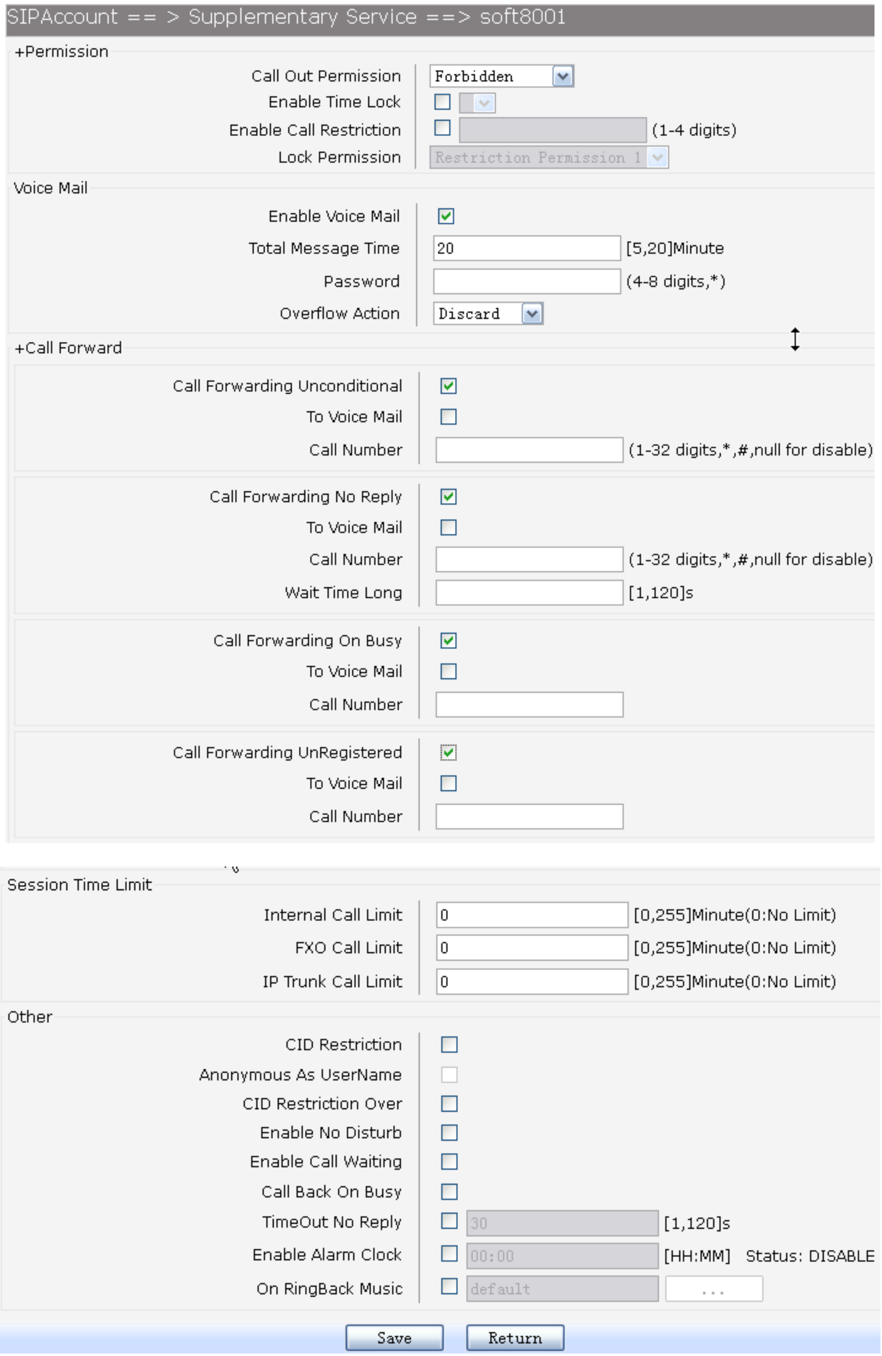
Note：

When calling out from registered IP trunk, Caller number must partially or completely match outgoing caller of registered IP trunk account.

3.6.3.4 Supplementary service

Improvements and additions to the basic services, it can not be alone provided, and must be provided with basic services.

Choose the menu **SIP Account→Account Parameter→Supplementary** to load the following page.



SIPAccount == > Supplementary Service ==> soft8001

+Permission

Call Out Permission	Forbidden	
Enable Time Lock	□	
Enable Call Restriction	□	(1-4 digits)
Lock Permission	Restriction Permission 1	

Voice Mail

Enable Voice Mail	☑	
Total Message Time	20	[5,20]Minute
Password		(4-8 digits,*)
Overflow Action	Discard	

+Call Forward

Call Forwarding Unconditional	☑	
To Voice Mail	□	
Call Number		(1-32 digits,*,#,null for disable)
Call Forwarding No Reply	☑	
To Voice Mail	□	
Call Number		(1-32 digits,*,#,null for disable)
Wait Time Long		[1,120]s
Call Forwarding On Busy	☑	
To Voice Mail	□	
Call Number		
Call Forwarding UnRegistered	☑	
To Voice Mail	□	
Call Number		

Session Time Limit

Internal Call Limit	0	[0,255]Minute(0:No Limit)
FXO Call Limit	0	[0,255]Minute(0:No Limit)
IP Trunk Call Limit	0	[0,255]Minute(0:No Limit)

Other

CID Restriction	□		
Anonymous As UserName	□		
CID Restriction Over	□		
Enable No Disturb	□		
Enable Call Waiting	□		
Call Back On Busy	□		
TimeOut No Reply	□	30	[1,120]s
Enable Alarm Clock	□	00:00	[HH:MM] Status: DISABLE
On RingBack Music	□	default	...

Figure 3-115 Parameter of Supplementary

The following items are displayed on this screen:

►**Call Out Permission**: Call permission is used to control whether or not you can dial some phone numbers, such as long distance call, international long distance call. The device has 5 levels of call permission by default. Web configuration index: **Voice Service→Permission Definition**.

►**Time Lock**: Time Lock is just time-based call restriction. Call permission can be changed automatically for different time period. For example, the extension has permission for local call at working period, and has permission only for internal call at off-duty time.

►**Call Restriction**: Call Restriction enables you to restrict or bar certain or all types of calls to your phone, i.e. long distance calls, international calls. Dialing supplementary services function key can be opened and canceled. Web configuration index:

Voice Service→Advance config→Supplementary.

►**Voice mail**: Voicemail is used to convey a caller's recorded audio message when you can not answer the phone. It contains a user interface to select, play and manage messages.

►**Total Message Time**：The total time length is for all voice messages.

►**Password:** When using to extract messages, you must input password.

►**Action**: When the total time length has been reached, then if new voice message comes, it will be discarded or overwritten.

►**Call Forwarding Unconditional**: If you enter a number for this parameter, any call to your extension will be forwarding to that number, unconditional.

►**Call Forwarding No Reply**: If you enter a number for this parameter, any call to your extension will be forwarding to that number when you don't reply the call.

►**Call Forwarding On Busy**: If you enter a number for this parameter, any call to your extension will be forwarding to that number, on busy.

►**Call Forwarding UnRegistered**: If you enter a number for this parameter, any call to your extension will be forwarding to that number when the registering of extension fails.

►**Hot line**: Immediately hotline or delay hotline. Time 0 indicates immediate hotline, otherwise indicates delay hotline. If corresponding function key of supplementary services is enabled, then dial function key to configure the number, but note, can't use immediately hotline.

►**Session Time Limit**: The functionality will disconnect the call automatically when the call time reached the specified value.

►**CID Restriction**: Enable or disable CID Restriction. If CID Restriction is enabled, the display name content in sip package is anonymous. If **Anonymous As UserName** is chosen, that user name content is anonymous also.

►**CID Restriction Over**: This function is only valid for the call between two internal externsions.

►**Enable No Disturb**: Allows you to totally block incoming calls at any time. If corresponding function key of supplementary services is enabled, then dial function key to configure.

►**Enable Call Waiting**: When talking, a third party phone comes in and you can hear the beep tone. If corresponding function key of supplementary services is enabled, then dial function key to configure.

►**Call Back On Busy**: When talking, a third party phone comes in and dial 1 after the prompt tone. When you hang up, the system will call you and third party.

►**Alarm Clock**: Alarm Clock lets the phone ring at a specified time for alerting.

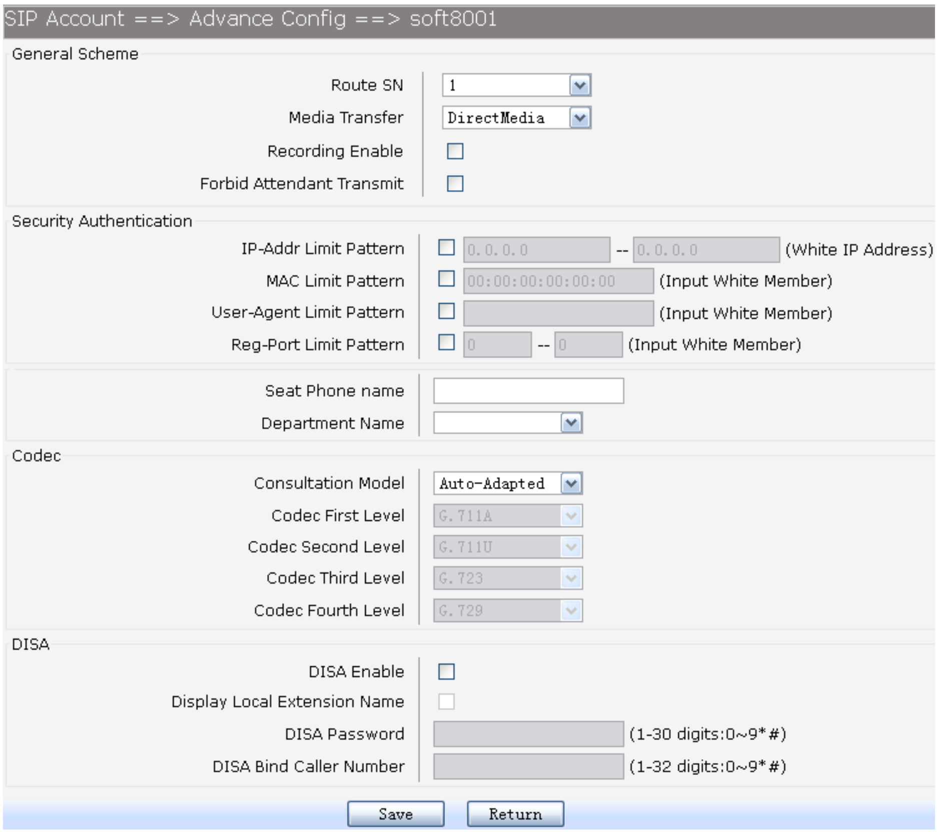
Note：

Call waiting is only valid for FXS。

3.6.3.5 Advanced configuration

The following parameters can be configured in this page, like DISA, Route number, Fax model, Media Transfer, Recording, Codec and Security Authentication.

Choose the menu **SIP Account→Account Parameter→Advance Config** to load the following page.



SIP Account ==> Advance Config ==> soft8001

General Scheme

Route SN	1
Media Transfer	DirectMedia
Recording Enable	□
Forbid Attendant Transmit	□

Security Authentication

IP-Addr Limit Pattern	□ 0.0.0.0 -- 0.0.0.0 (White IP Address)
MAC Limit Pattern	□ 00:00:00:00:00:00 (Input White Member)
User-Agent Limit Pattern	□ (Input White Member)
Reg-Port Limit Pattern	□ 0 -- 0 (Input White Member)
Seat Phone name	
Department Name	

Codec

Consultation Model	Auto-Adapted
Codec First Level	G.711A
Codec Second Level	G.711U
Codec Third Level	G.723
Codec Fourth Level	G.729

DISA

DISA Enable	□
Display Local Extension Name	□
DISA Password	(1-30 digits:0~9*#)
DISA Bind Caller Number	(1-32 digits:0~9*#)

Figure 3-116 Advanced Parameters of Account

The following items are displayed on this screen:

►**Route SN**: The system supports up to ten call route tables. The parameter is the index of call routing table.

►**Media Transfer**: RTP media stream to go directly between the caller and the callee.

►**Fax Mode**: Transparent, T38, VBD.

►**Recording**: Enable or disable call recording function for the user.

►**Forbid Attendant Transmit**: Check the box to permit whether of not the attendant can transfer call to this user.

►**Security Authentication**: To prevent from attacking, only allow qualified SIP account to register.

►**Seat Phone name**: The value is used for Caller ID Name Display.

►**Department Name**: Department attribution division, which is used in billing statistics.

►**Codec**: Negotiation mode of voice capabilities.

Auto-Adapted: The system forwards codec capability priority.

Priority-Level: The system rearranges codec capability before sending.

►**DISA**: Enable or disable DISA (Direct Inward System Access).

DISA Password: The password for authentication.

DISA Bind Caller Number: The caller from this number does not need to authentication.

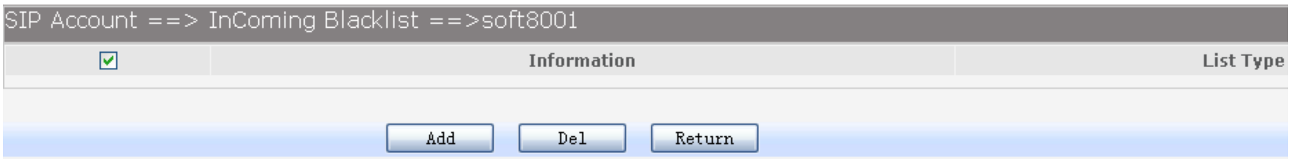
3.6.3.6 Incoming Black&White List

Blacklist & Whitelist is one function which detects incoming calls and rejects unwanted callers which are in the blacklist and allows only whitelist numbers to come through.

If blacklist is enabled, you can only configure blacklist, otherwise, you can configure a whitelist. In order to enable the blacklist or whitelist, choose the menu **Voice Service→Advance Config→SIP**

Service Control.

Choose the menu **SIP Account→Account Parameter→Incoming Black&White List** to load the following page.

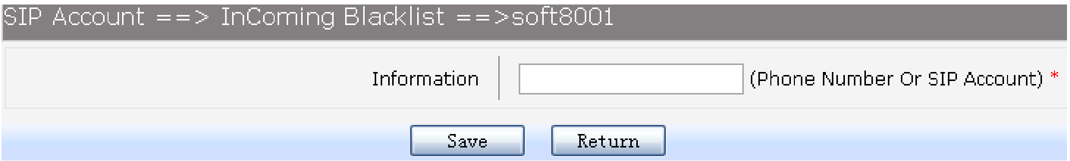


SIP Account ==> InComing Blacklist ==>soft8001

☑	Information	List Type

Figure 3-117 Incoming Black&White List

On click **Add** button to load the following page.



SIP Account ==> InComing Blacklist ==>soft8001

Information (Phone Number Or SIP Account) *

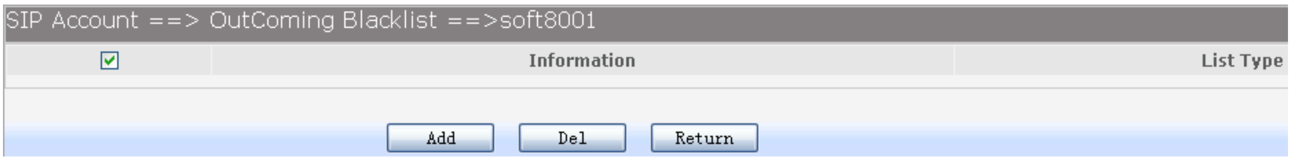
Figure 3-118 Parameters of Black&White List

3.6.3.7 Outgoing Black&White List

Blacklist & Whitelist is one function which permits to call the numbers in the whitelist for outgoing calls.

If the blacklist is enabled, you can only configure blacklist. Otherwise, you can configure a whitelist. In order to enable the blacklist or whitelist, choose the menu **Voice Service→Advance Config→SIP Service Control.**

Choose the menu **SIP Account→Account Parameter→OutGoing Black&White List** to load the following page.

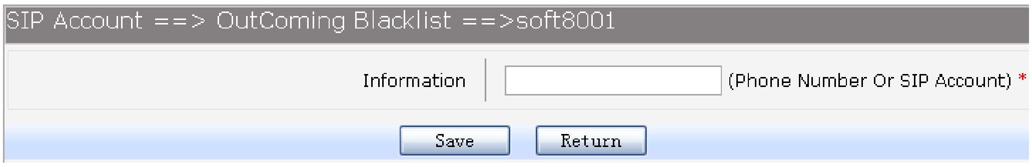


SIP Account ==> OutComing Blacklist ==>soft8001

☑	Information	List Type

Figure 3-119 OutGoing Black&White List

On click **Add** button to load the following page.



SIP Account ==> OutComing Blacklist ==>soft8001

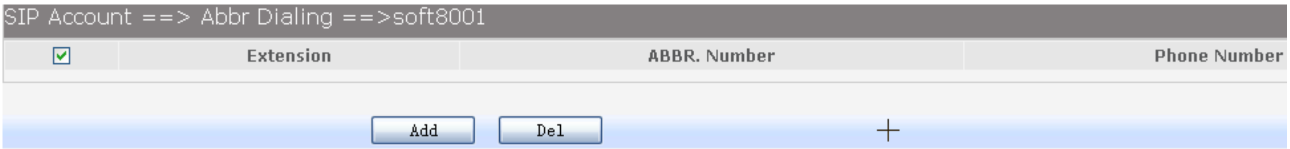
Information (Phone Number Or SIP Account) *

Figure 3-120 Parameters of Black&White List

3.6.3.8 Abbreviated Dialing

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

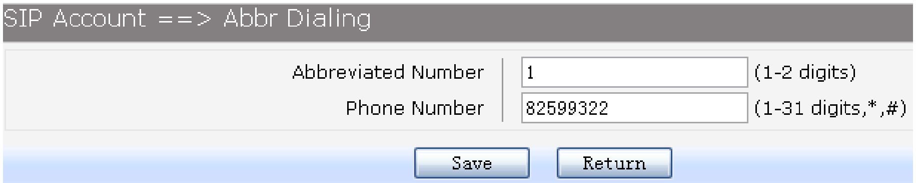
Choose the menu **SIP Account→Account Parameter→Abbreviated Dialing** to load the following page.



☑	Extension	ABBR. Number	Phone Number

Figure 3-121 Abbreviated Dialing List

On click **Add** button to load the following page.



Abbreviated Number	1	(1-2 digits)
Phone Number	82599322	(1-31 digits,*,#)

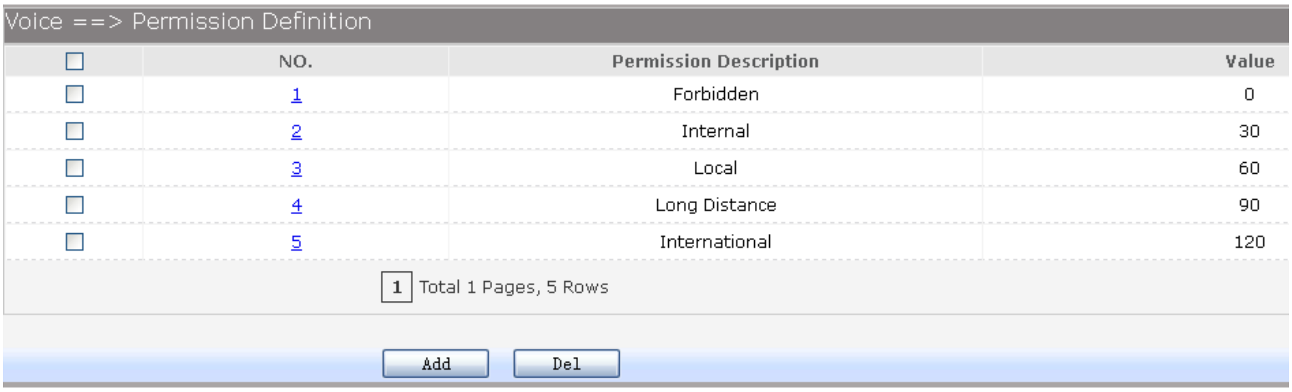
Figure 3-122 Parameters of Abbreviated Dialing

3.7 Voice Service Configuration

3.7.1 Permission Definition

Permissions define the meaning and weight, Call route and user need to configure permission.

Choose the menu **Voice Service→Permission Definition** to load the following page.

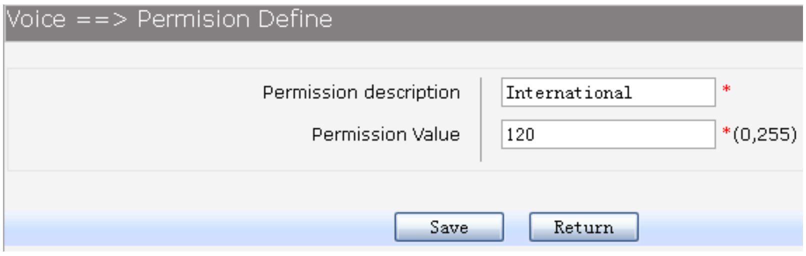


□	NO.	Permission Description	Value
□	1	Forbidden	0
□	2	Internal	30
□	3	Local	60
□	4	Long Distance	90
□	5	International	120

1 Total 1 Pages, 5 Rows

Figure 3-123 Permission Define List

On click **Add** button to load the following page.



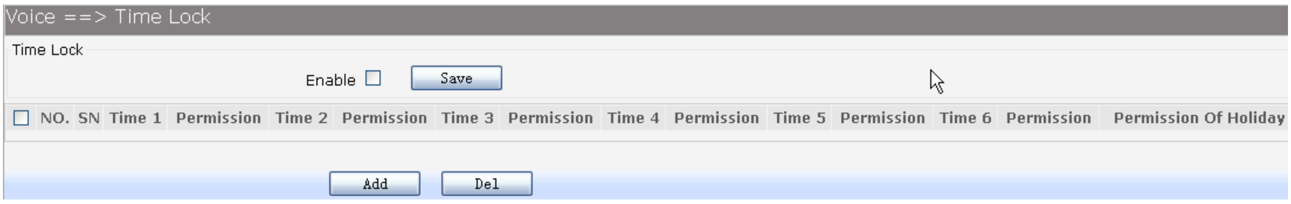
Permission description	International	*
Permission Value	120	*(0,255)

Figure 3-124 Parameter of Permission Definition

3.7.2 Time Lock

Time Lock is just time-based call restriction. Call permission can be changed automatically for different time period. For example, the extension has permission for local call at working time, and has permission only for internal call at off-duty time. The device supports up to 100 time lock items. Each time lock has 6 time period settings and a holiday setting. Holidays can be configured to any day you need. If you want to active all rules, you must enable time lock firstly.

Choose the menu **Voice Service→Time Lock** to load the following page.



Voice ==> Time Lock

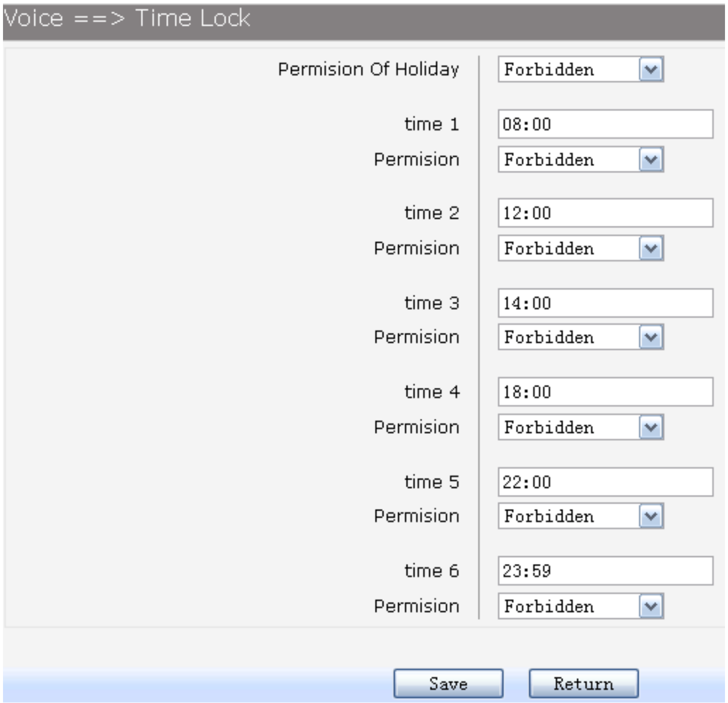
Time Lock

Enable □ Save

□	NO.	SN	Time 1	Permission	Time 2	Permission	Time 3	Permission	Time 4	Permission	Time 5	Permission	Time 6	Permission	Permission Of Holiday

Figure 3-125 Time Lock List

On click **Add** button to load the following page.



Voice ==> Time Lock

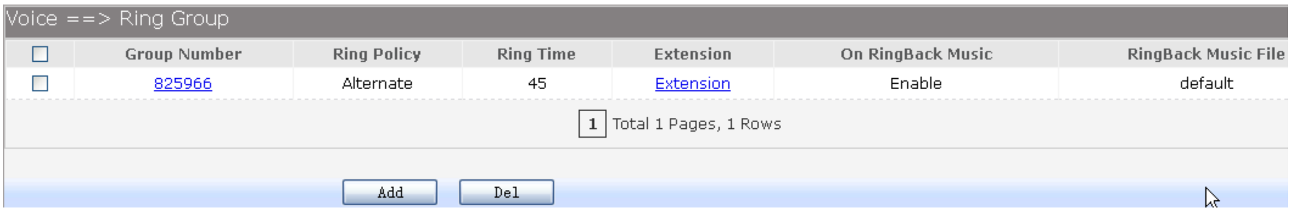
Permision Of Holiday	Forbidden
time 1	08:00
Permision	Forbidden
time 2	12:00
Permision	Forbidden
time 3	14:00
Permision	Forbidden
time 4	18:00
Permision	Forbidden
time 5	22:00
Permision	Forbidden
time 6	23:59
Permision	Forbidden

Figure 3-126 Parameters of Time Lock

3.7.3 Ring Group

A hunt group is a collection of extensions that ring in a particular order when the hunt group number is dialed. Hunt group usually have a phone number associated with them, which is 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.

Choose the menu **Voice Service→Ring Group** to load the following page.



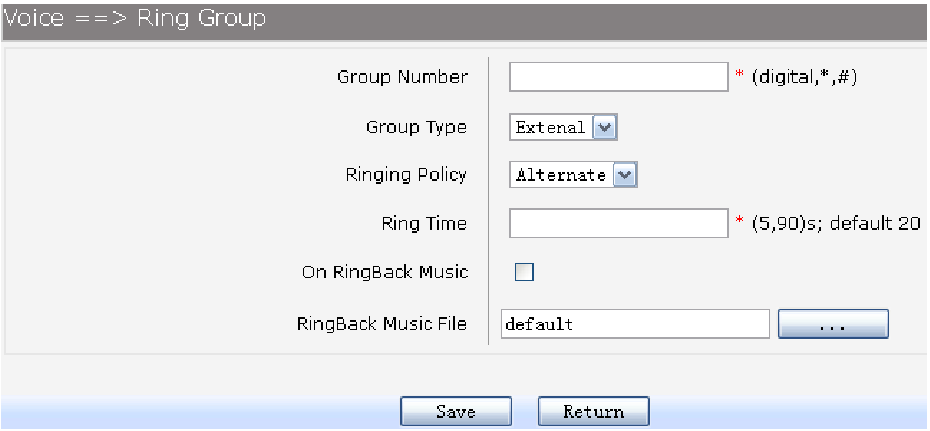
Voice ==> Ring Group

□	Group Number	Ring Policy	Ring Time	Extension	On RingBack Music	RingBack Music File
□	825966	Alternate	45	Extension	Enable	default

1 Total 1 Pages, 1 Rows

Figure 3-127 Ring Group List

On click **Add** button to load the following page.



Voice ==> Ring Group

Group Number	* (digital,*,#)
Group Type	Extenal
Ringing Policy	Alternate
Ring Time	* (5,90)s; default 20
On RingBack Music	□
RingBack Music File	default ...

Figure 3-128 Parameters of Ring Group

The following items are displayed on this screen:

►**Group Number:** The group number which can be called.

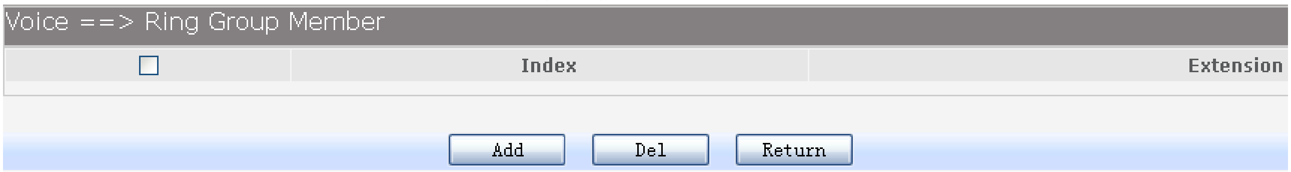
►**Group Type**: Internal number or external number.

►**Ringing Policy**: Include Alternate, Ordinal, Parallel.

►**Ring Time**: The timeout period of ringing

►**On RingBack Music**: When you call group number, you will hear a ringback tone or color ring music. You can update the music file of ringback.

On click **Save** button, then load the following page.

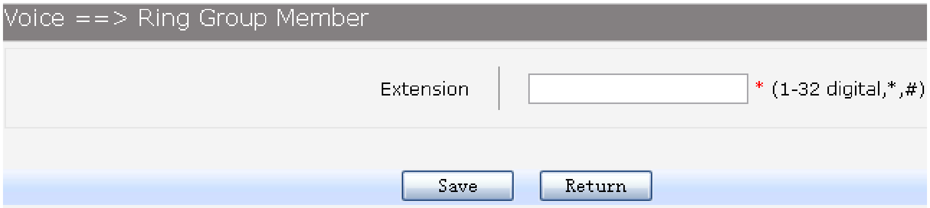


Voice ==> Ring Group Member

□	Index	Extension

Figure 3-129 Extensions List of Ring Group

On click **Add** button to load the following page.



Voice ==> Ring Group Member

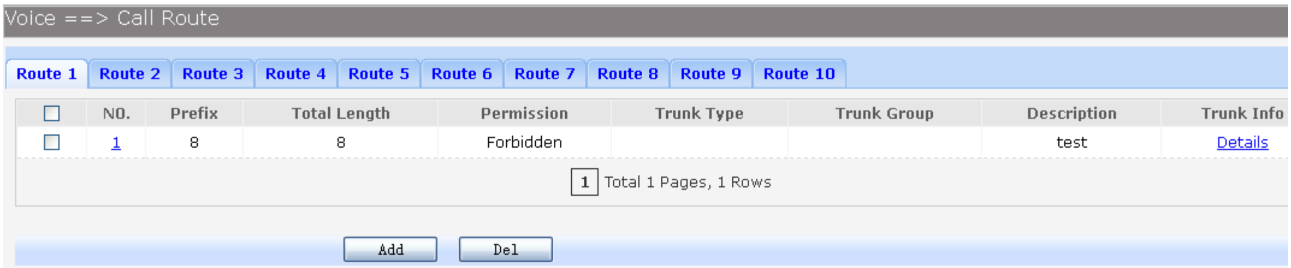
Extension	* (1-32 digital,*,#)

Figure 3-130 Extension Number

3.7.4 Call Routing

3.7.4.1 Configuration instructions

Choose the menu **Voice Service→Call Routing** to load the following page.



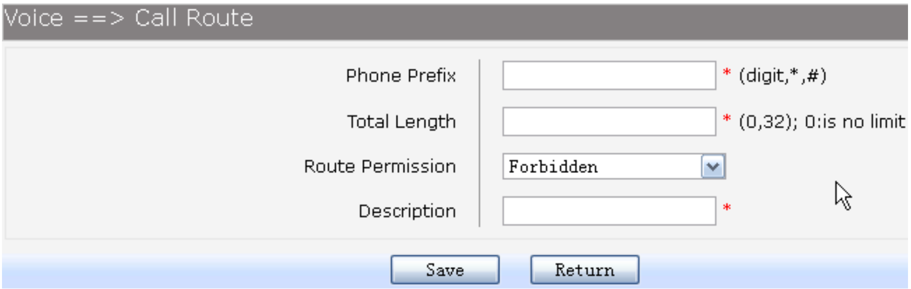
Voice ==> Call Route

□	NO.	Prefix	Total Length	Permission	Trunk Type	Trunk Group	Description	Trunk Info
□	1	8	8	Forbidden			test	Details

1 Total 1 Pages, 1 Rows

Figure 3-131 Call Routing List

On click **Add** button to load following page.



Voice ==> Call Route

Phone Prefix		* (digit,*,#)
Total Length		* (0,32); 0:is no limit
Route Permission	Forbidden	
Description		*

Figure 3-132 Parameters of Call Route

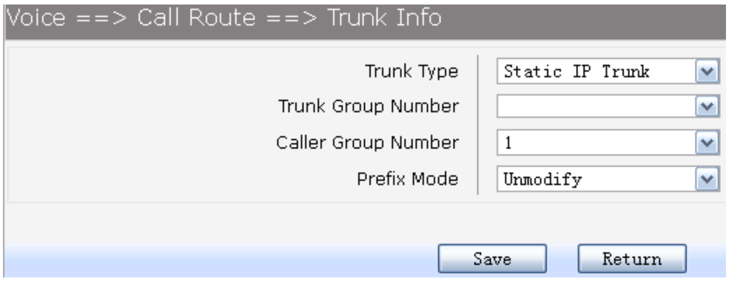
The following items are displayed on this screen:

►**Phone Prefix**: A call to the destination number which starts with this prefix will be routed with the corresponding call route table.

►**Total Length**: The length of destination number, 0 means indefinite length. A call route item is uniquely identified by the prefix and total length field. Two call route items with same prefix but different “total length” is allowable. This parameter is also used to indicate whether the number is received completely.

►**Route Permission**: The call permission of subscriber should be no less than the permission of call route item.

In order to configure trunk info, choose the menu **Voice Service→Call Routing→Details,** on click **add** button to load the following page. Each call route item supports up to 4 ways connecting to the Central Office.



Voice ==> Call Route ==> Trunk Info

Trunk Type	Static IP Trunk
Trunk Group Number	
Caller Group Number	1
Prefix Mode	Unmodify

Figure 3-133 Trunk info of Call Route

►**Trunk Type**: There are 3 trunk types supported, static IP trunk, register IP trunk and FXO (analog trunk).

►**Trunk Group Number**: The trunk resource can be grouped.

►**Caller Group Number**: **Caller Group Number** indicates which caller number to be sent when call out through the specified trunk.

►**Prefix Mode**: The parameter specifies what the transformation performed on a called number before it gets routed over a trunk. There are four transformations that can be selected: **Unmodify**, **Remove**, **Add**, **Modify**.

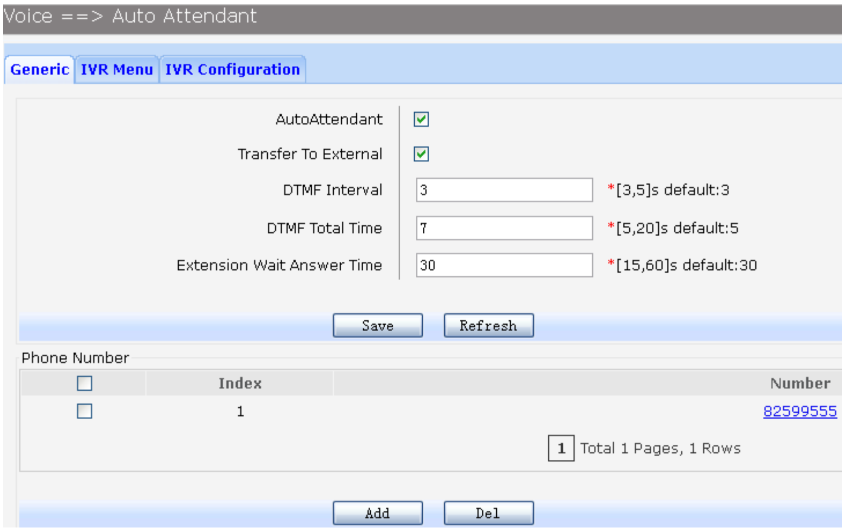
3.7.5 Auto Attendant

Auto attendant service allows callers to be automatically transferred to an extension without the intervention of an operator, and also allows a caller to reach a live operator by dialing a number, usually "0". Auto attendant will have a greeting message that is played to callers, this message can be configured. Different message to play in different time period is available. The auto attendant supports up to 20 phone numbers.

3.7.5.1 Configuration instructions

3.7.5.1.1 Generic

Choose the menu **Voice Service→Auto Attendant→Generic** to load the following page.



Voice ==> Auto Attendant

AutoAttendant	☑	
Transfer To External	☑	
DTMF Interval	3	*[3,5]s default:3
DTMF Total Time	7	*[5,20]s default:5
Extension Wait Answer Time	30	*[15,60]s default:30

Phone Number

□	Index	Number
□	1	82599555

1 Total 1 Pages, 1 Rows

Figure 3-134 Generic parameters of Auto Attendant

The following items are displayed on this screen:

►**AutoAttendant**: Enable or disable Auto attendant.

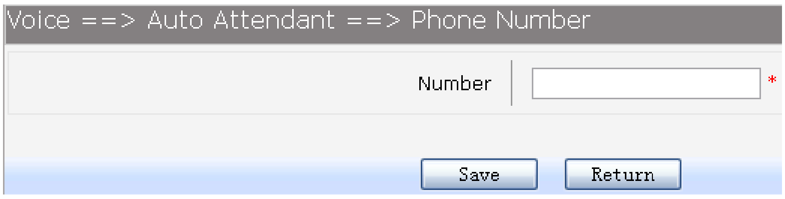
►**Transfer To External**: Control whether or not the auto attendant can dial extension number.

►**DTMF Interval**: Inter-digit timer for DTMF collecting.

►**DTMF Total Time**: The total time use for DTMF collecting.

►**Extension Wait Answer Time**: The caller will return to the main menu when the timer expired.

►**Phone Number**: All numbers are extension numbers. On click **Add** button to load following page.



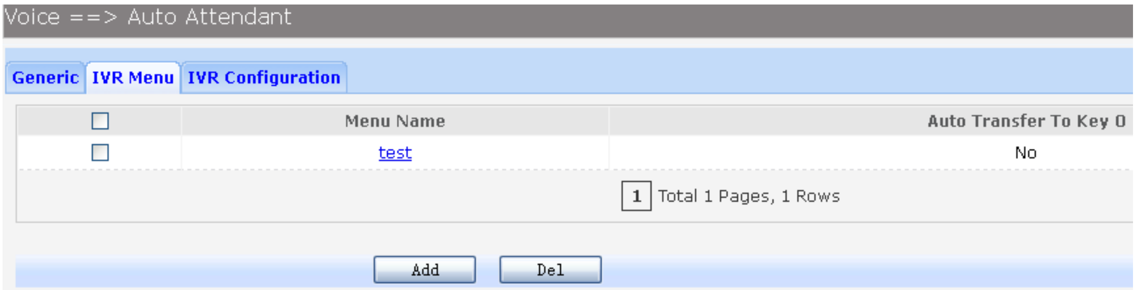
Voice ==> Auto Attendant ==> Phone Number

Number *

Figure 3-135 Attendant Number

3.7.5.1.2 IVR Menu

Choose the menu **Voice Service→Auto Attendant→IVR Menu** to load the following page.



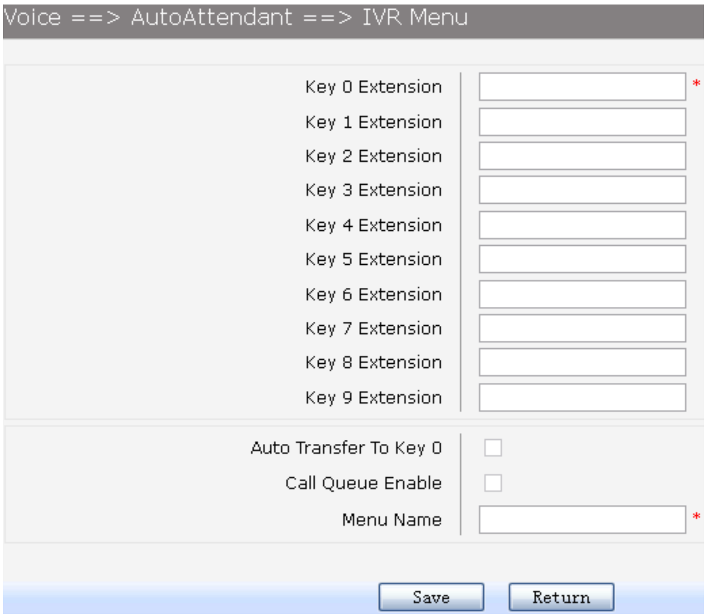
Voice ==> Auto Attendant

□	Menu Name	Auto Transfer To Key 0
□	test	No

1 Total 1 Pages, 1 Rows

Figure 3-136 IVR Menu List

On click **Add** button to load following page.



Voice ==> AutoAttendant ==> IVR Menu

Key 0 Extension *
Key 1 Extension
Key 2 Extension
Key 3 Extension
Key 4 Extension
Key 5 Extension
Key 6 Extension
Key 7 Extension
Key 8 Extension
Key 9 Extension

Auto Transfer To Key 0 □
Call Queue Enable □
Menu Name *

Save Return

Figure 3-137 Parameters of IVR Menu

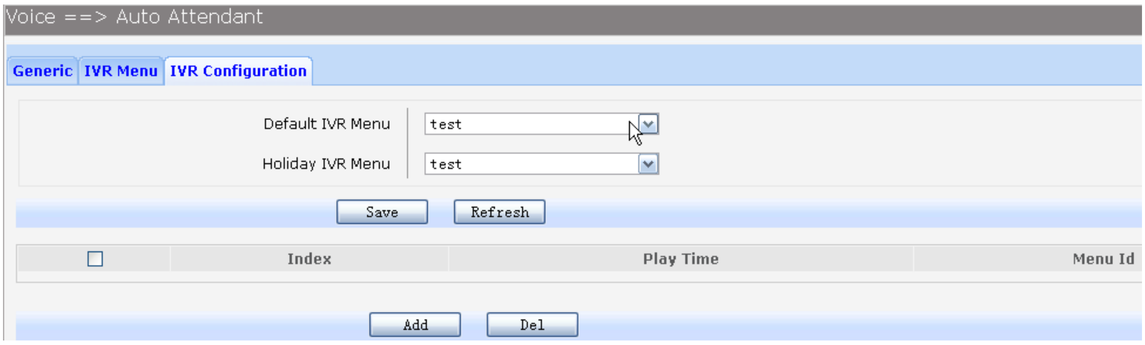
The following items are displayed on this screen:

►**Auto Transfer To Key 0**: Automatically transferred to the corresponding number of key 0 after playing greeting message.

►**Call Queue Enable:** This function is for the 0 key bindings extension. If o key binding extension is calling, third party will be queued, otherwise will hear busy tone.

3.7.5.1.3 IVR Configuration

Configure IVR menu to specify different time. Choose the menu **Voice Service→Auto Attendant→IVR Configuration** to load the following page.



Voice ==> Auto Attendant

Generic | IVR Menu | IVR Configuration

Default IVR Menu: test
Holiday IVR Menu: test

Save Refresh

□	Index	Play Time	Menu Id

Add Del

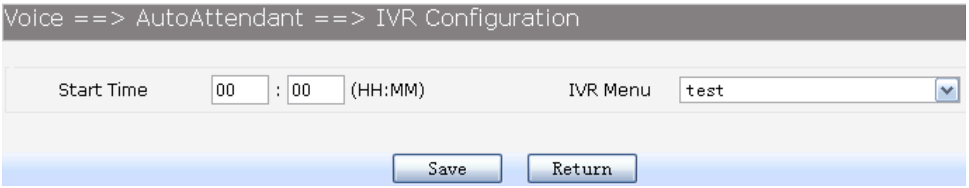
Figure 3-138 IVR Configuration

The following items are displayed on this screen:

►**Default IVR Menu**: If you don't configure IVR menu of holidays and time period, use this IVR menu.

►**Holiday Menu**: Holiday uses special IVR menu. Choose the menu **Voice Service→Advance config→Holiday** to configure.

►**IVR of time period**: On click **Add** button to load following page.



Voice ==> AutoAttendant ==> IVR Configuration

Start Time 00 : 00 (HH:MM) IVR Menu test

Save Return

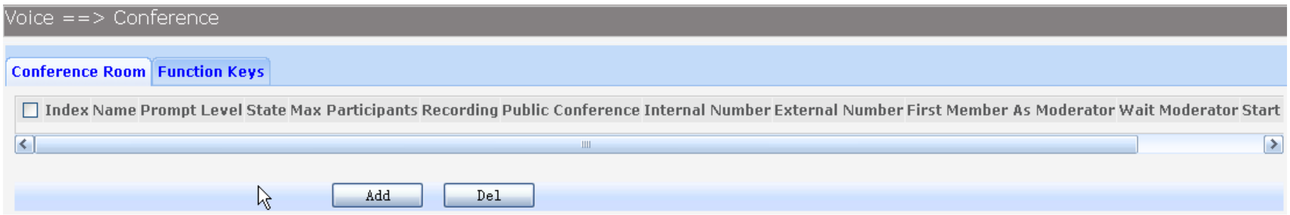
Figure 3-139 IVR of Time Period

3.7.6 Conference

Conference call allows the calling party to call the other participants and add them to the conference room. It also allows the called party to participate during the conference call.

3.7.6.1 Conference Room

Choose the menu **Voice Service→Conference→Conference Room** to load the following page.

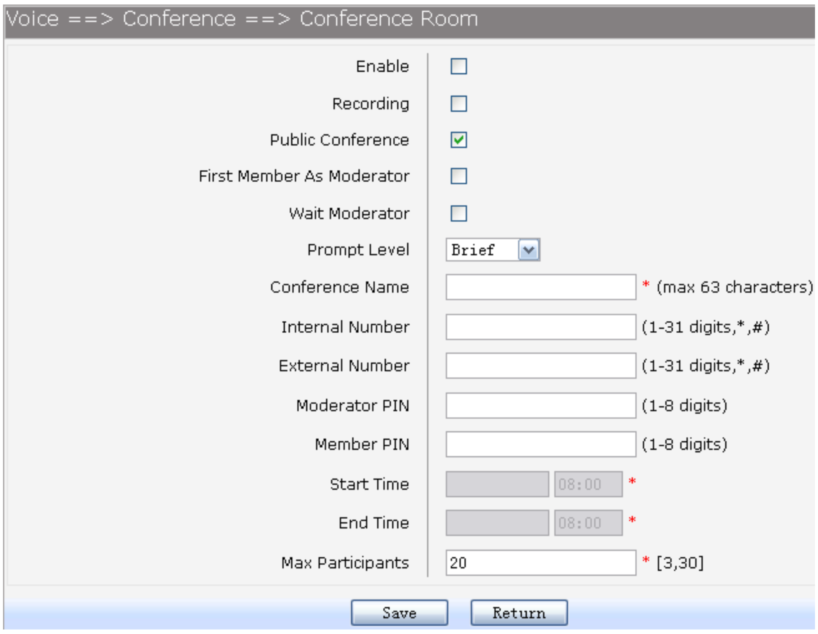


Voice ==> Conference

□	Index	Name	Prompt Level	State	Max Participants	Recording	Public Conference	Internal Number	External Number	First Member As Moderator	Wait Moderator	Start

Figure 3-140 Conference Room List

On click **Add** button to load following page.



Voice ==> Conference ==> Conference Room

Enable	□	
Recording	□	
Public Conference	☑	
First Member As Moderator	□	
Wait Moderator	□	
Prompt Level	Brief	
Conference Name		* (max 63 characters)
Internal Number		(1-31 digits,*,#)
External Number		(1-31 digits,*,#)
Moderator PIN		(1-8 digits)
Member PIN		(1-8 digits)
Start Time	08:00	*
End Time	08:00	*
Max Participants	20	* [3,30]

Figure 3-141 Parameters of Conference Room

The following items are displayed on this screen:

►**Enable**: Conference Room is valid.

►**Recording**: Check the box to enable recording for meeting.

►**Public Conference**: Indicates the conference is public or not. The public conference is always open, and the private conference is only open at specified time.

►**Fist Member As Moderator**: First telephone which enters the conference room is moderator, When the conference room is a public meeting.

►**Wait Moderator**: The participants can not speak at the beginning when the conference is configured to wait moderator, they should ask for permission of moderator to speak.

►**Internal Number**: Internal phone number to enter this conference room.

►**External Number**: DID number to enter this conference room.

►**Moderator PIN**: Used to distinguish the moderator and other participants.

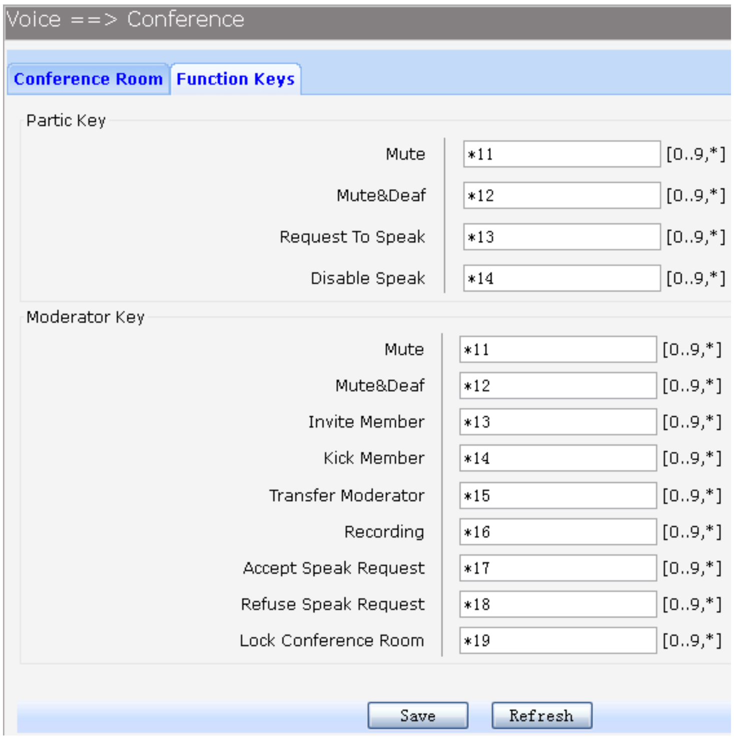
►**Member PIN**: Used for participant authentication, should be different from moderator

PIN.

- ►**Start Time**: Start time for private conference.
- ►**End Time**: End time for private conference.
- ►**Max Participants**: Max participants for this conference room.

3.7.6.2 Functions Keys

Choose the menu **Voice Service→Conference→Function Keys** to load the following page.



Voice ==> Conference

Partic Key

Mute	*11	[0..9,*]
Mute&Deaf	*12	[0..9,*]
Request To Speak	*13	[0..9,*]
Disable Speak	*14	[0..9,*]

Moderator Key

Mute	*11	[0..9,*]
Mute&Deaf	*12	[0..9,*]
Invite Member	*13	[0..9,*]
Kick Member	*14	[0..9,*]
Transfer Moderator	*15	[0..9,*]
Recording	*16	[0..9,*]
Accept Speak Request	*17	[0..9,*]
Refuse Speak Request	*18	[0..9,*]
Lock Conference Room	*19	[0..9,*]

Figure 3-142 Parameters of Function Keys

The following items are displayed on this screen:

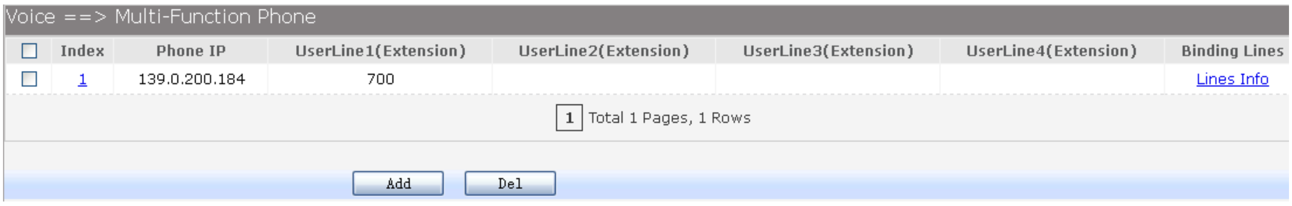
1. Participant key control.
   - ►**Mute**: Mute oneself, it's disabled in wait moderator mode. It works like toggle switch, one will be muted the first time when the keys pressed, and gets back next time.
   - ►**Mute&Deaf**: Mute and deaf oneself, it's disabled in wait moderator mode.
   - ►**Request to speak**: The participants ask for permission to speak in waiting moderator mode.
   - ►**Disable speak**: The participants mute themselves in waiting moderator mode, no need to confirm.
2. Moderator key control.
   - ►**Mute**: Mute moderator self or other participants. Instructions for participant muting, press mute keys+ participant number.
   - ►**Mute&Deaf**: Mute and deaf moderator self.
   - ►**Invite Member**: Add participant to the conference call.
   - ►**Kick Member**: Kick participant from the conference call.
   - ►**Transfer moderator**: Transfer the moderator role to another participant.
   - ►**Recording**: Start or end recording of conference call.
   - ►**Accept speak request**: Allow the participant to speak after receiving the request.
   - ►**Refuse speak request**: Refuse the participant to speak after receiving the request.

►**Lock Conference Room**: Nobody can join the conference after the conference is locked unless the moderator calls them or unlocks the conference.

3.7.7 Multi-Function Phone

3.7.7.1 Configuration instructions

Choose the menu **Voice Service→Multic-Function Phone** to load the following page.



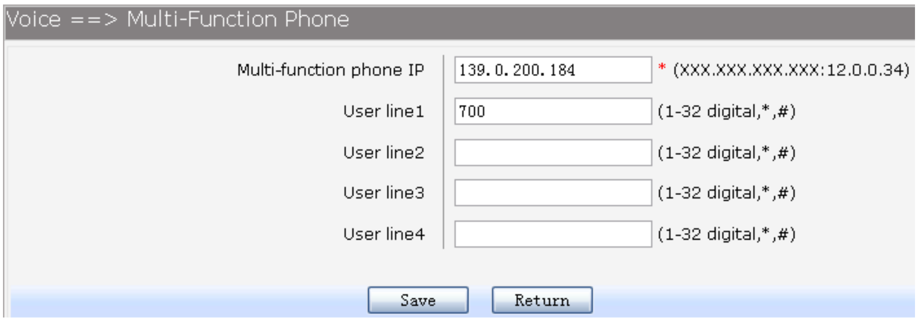
Voice ==> Multi-Function Phone

□	Index	Phone IP	UserLine1(Extension)	UserLine2(Extension)	UserLine3(Extension)	UserLine4(Extension)	Binding Lines
□	1	139.0.200.184	700				Lines Info

1 Total 1 Pages, 1 Rows

Figure 3-143 Multic-Function Phone List

On click **Add** button to load following page.



Voice ==> Multi-Function Phone

Multi-function phone IP	139. 0. 200. 184	* (XXX.XXX.XXX.XXX:12.0.0.34)
User line1	700	(1-32 digital,*,#)
User line2		(1-32 digital,*,#)
User line3		(1-32 digital,*,#)
User line4		(1-32 digital,*,#)

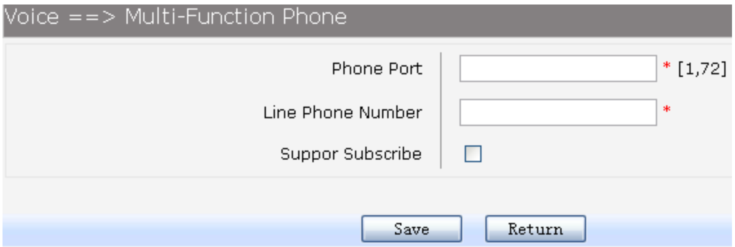
Figure 3-144 Basic Parameters of Multic-Function Phone

The following items are displayed on this screen:

►**IP**: Multi-function phone IP address to connect LAN port of device.

►**User line(N)**: Phone numbers which are monitored.

In order to bind user configuration, on click **Lines Info** to load the following page.



Voice ==> Multi-Function Phone

Phone Port		* [1,72]
Line Phone Number		*
Suppor Subscribe	□	

Figure 3-145 Binding Users Info

The following items are displayed on this screen:

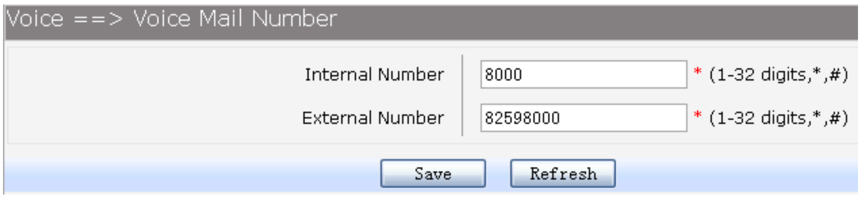
►**Phone Port**: Multifunctional phone number that is corresponding with the bound user.

►**Support Subscription**: Support sending and receiving subscription packet.

3.7.8 Voice Mail Number

Voicemail is used to convey a caller's recorded audio message when you can not answer the phone. It contains a user interface to select, play and manage messages.

Choose the menu **Voice Service→Voice Mail Number** to load the following page.

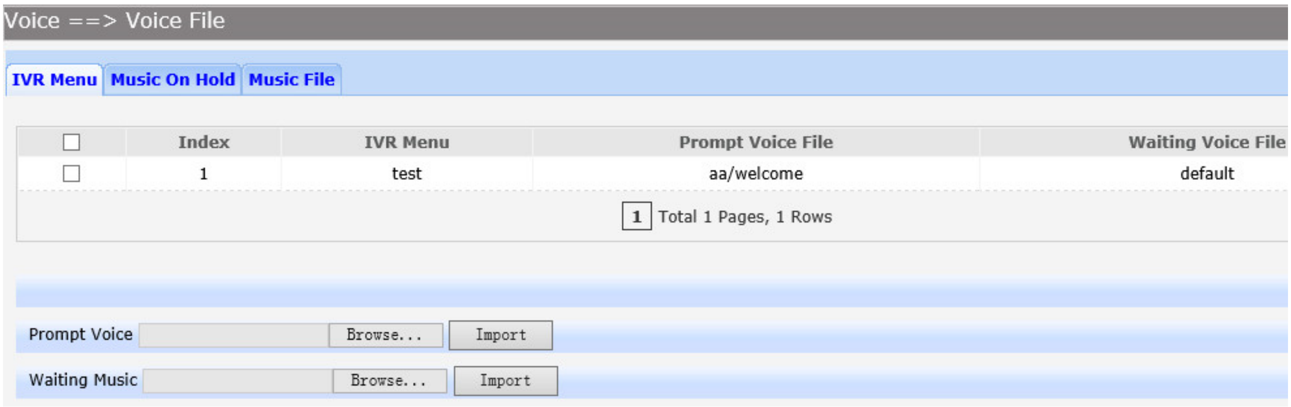


Internal Number	8000	* (1-32 digits,*,#)
External Number	82598000	* (1-32 digits,*,#)

Figure 3-146 Access Number of Voice Mail

3.7.9 Voice File

1)**IVR Menu**: Choose the menu **Voice Service→Voice File→IVR Menu** to load the following page.



□	Index	IVR Menu	Prompt Voice File	Waiting Voice File
□	1	test	aa/welcome	default

1 Total 1 Pages, 1 Rows

Figure 3-147 Voice File of IVR Menu

The following items are displayed on this screen:

►**Prompt Voice**: Set the voice file which will be played after dialing IVR access code.

►**Waiting Music**: Set the waiting music which is played before transferring to extension.

2)**Music On Hold**: Choose the menu **Voice Service→Voice File→Music On Hold** to load the following page.

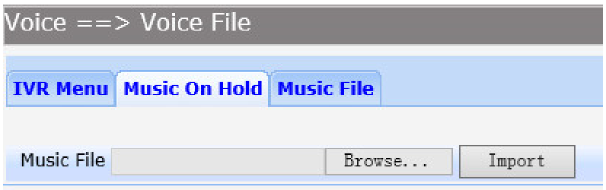


Figure 3-148 Voice File of Music on Hold

Set this music file which is used in call waiting.

3)**Music File**: Choose the menu **Voice Service→Voice File→Music File** to load the following page.

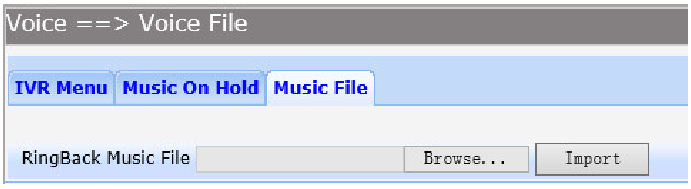
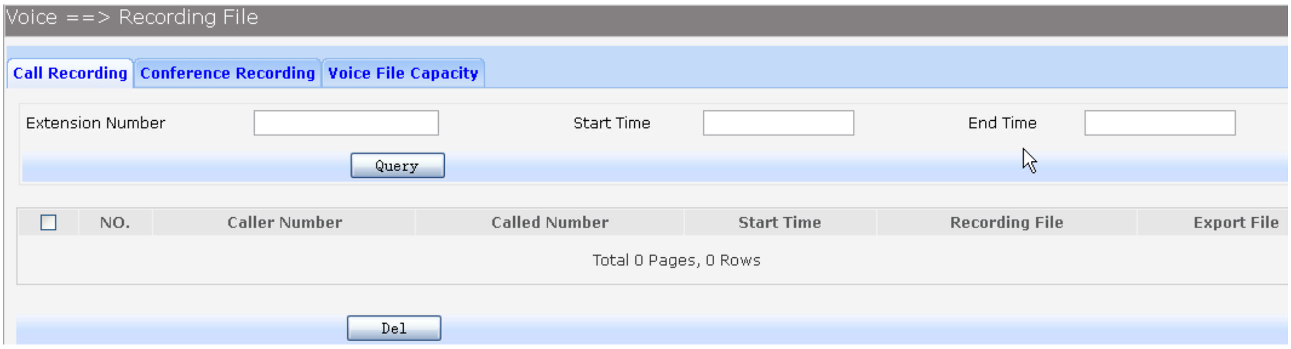


Figure 3-149 Voice File of Music

Set this music file which is used in ringback tone.

3.7.10 Record File

1)**Call Recording**: Choose the menu **Voice Service→Record File→Call Recording** to load the following page.



Extension Number
Start Time
End Time

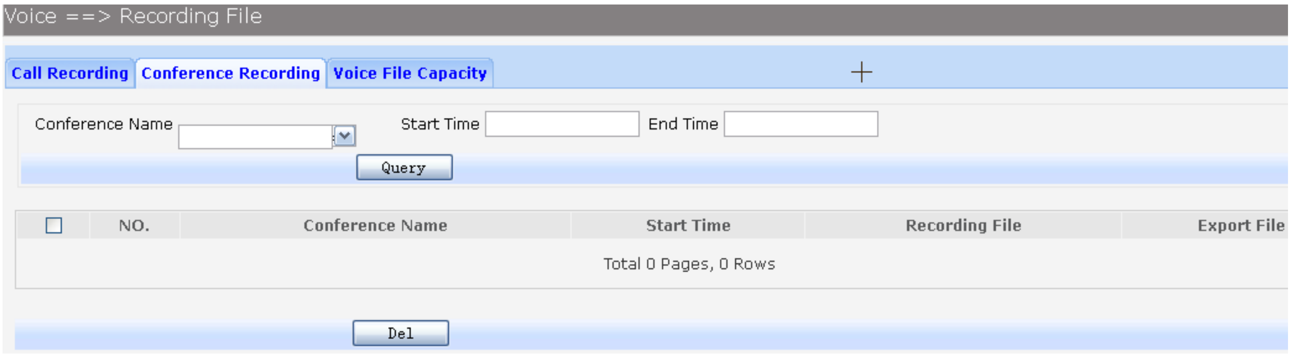
□	NO.	Caller Number	Called Number	Start Time	Recording File	Export File

Total 0 Pages, 0 Rows

Figure 3-150 Call Recording List

The call recording files can be filtered out with the extension number, start time, end time.

2)**Conference Recording**: Choose the menu **Voice Service→Record File→Conference Recording** to load the following page.



Conference Name
Start Time
End Time

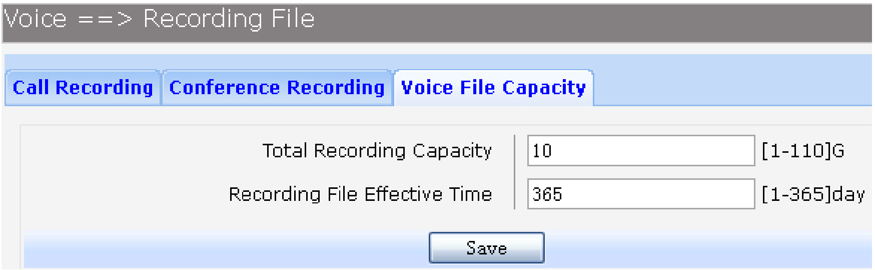
□	NO.	Conference Name	Start Time	Recording File	Export File

Total 0 Pages, 0 Rows

Figure 3-151 Conference Recording List

The conference recording files can be filtered out with the conference name, start time, end time.

3)**Voice File Capacity**: Choose the menu **Voice Service→Record File→Voice File Capacity** to load the following page.



Total Recording Capacity 10 [1-110]G

Recording File Effective Time 365 [1-365]day

Figure 3-152 Parameters of Voice File

The following items are displayed on this screen:

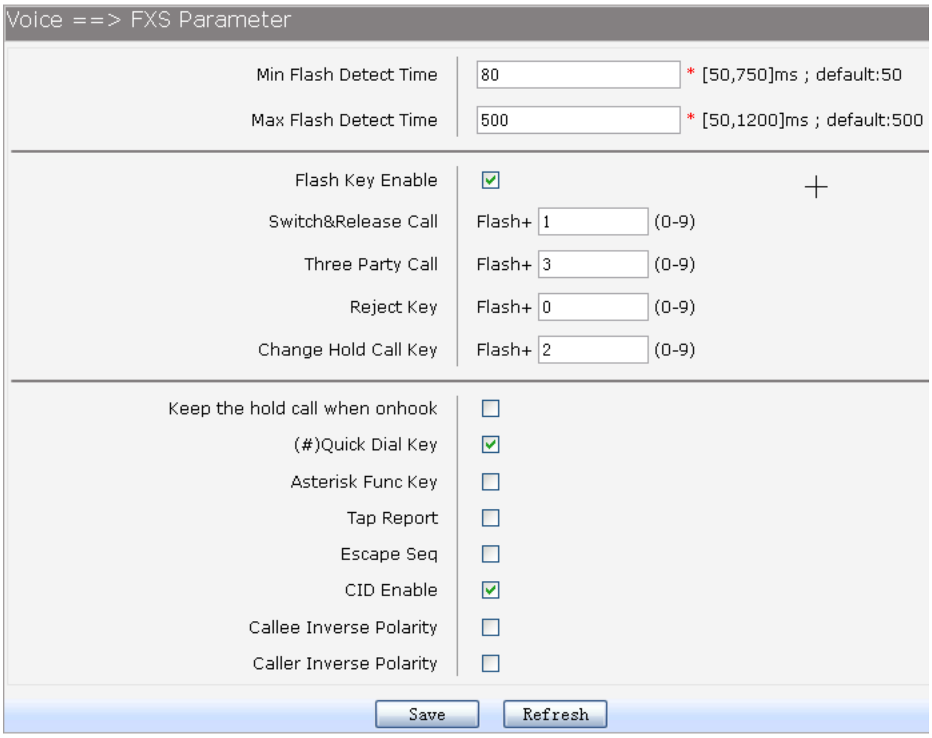
►**Total Recording Capacity**: The total size of all recording files.

►**Recording File Effective Time**: The existence time of recording file.

3.7.11 FXO/FXS Management

3.7.11.1 FXS Parameters

Choose the menu **Voice Service→FXO/FXS Management→FXS Parameters** to load the following page.



Voice ==> FXS Parameter

Min Flash Detect Time	80 * [50,750]ms ; default:50
Max Flash Detect Time	500 * [50,1200]ms ; default:500
Flash Key Enable	☑
Switch&Release Call	Flash+ 1 (0-9)
Three Party Call	Flash+ 3 (0-9)
Reject Key	Flash+ 0 (0-9)
Change Hold Call Key	Flash+ 2 (0-9)
Keep the hold call when onhook	□
(#)Quick Dial Key	☑
Asterisk Func Key	□
Tap Report	□
Escape Seq	□
CID Enable	☑
Callee Inverse Polarity	□
Caller Inverse Polarity	□

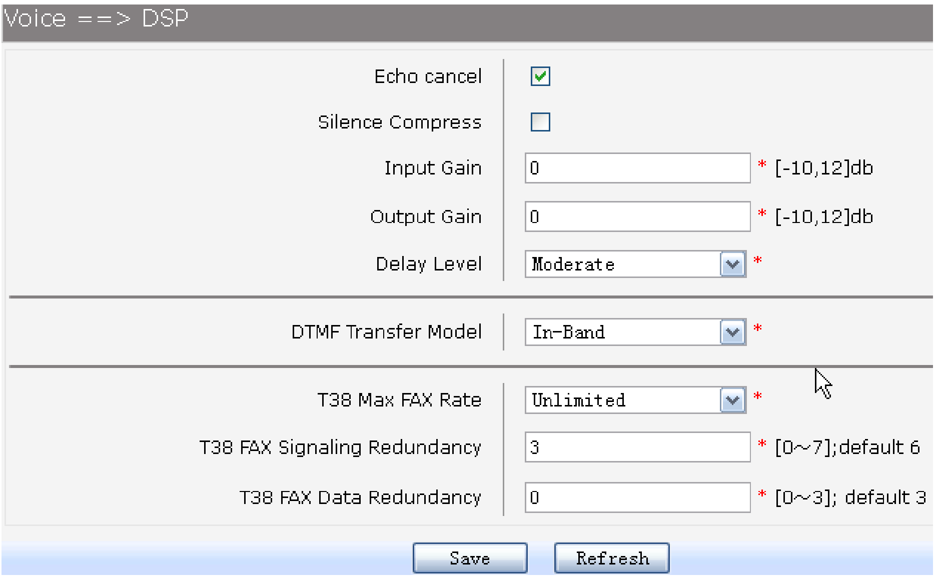
Figure 3-153FXS Parameters

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.
- ► **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 or 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.

3.7.11.2 DSP Parameters

Choose the menu **Voice Service→FXO/FXS Management→DSP Parameters** to load the following page.



Voice ==> DSP

Echo cancel ☑

Silence Compress □

Input Gain 0 * [-10,12]db

Output Gain 0 * [-10,12]db

Delay Level Moderate *

DTMF Transfer Model In-Band *

T38 Max FAX Rate Unlimited *

T38 FAX Signaling Redundancy 3 * [0~7];default 6

T38 FAX Data Redundancy 0 * [0~3]; default 3

Figure 3-154DSP 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.

3.7.11.3 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.

3.7.11.3.1 Digitmap Characters

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

3.7.11.3.2 Digitmap Example

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

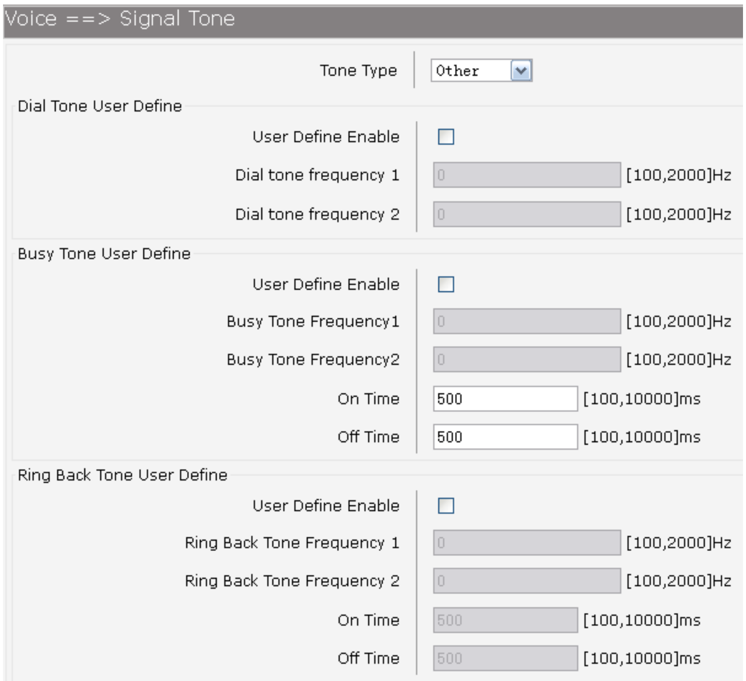
- "8XXXXXXX" denotes numbers start with 8, the length is 8.
- "1[0-24]0" denotes numbers include 100, 110, 120 and 140.
- "2[18].3" denotes numbers that start with 2 and end with 3, there can be arbitrary length of 1 or 8 after the first digit 2. 23, 213, 2183 is matched.
- "3XXSXX" denotes numbers start 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.

Note：

The digitmap is used for FXS only.

3.7.11.4 Signal Tone

Choose the menu **Voice Service→FXO/FXS Management→Signal Tone** to load the following page.



Voice ==> Signal Tone

Tone Type: Other

Dial Tone User Define

User Define Enable: □

Dial tone frequency 1: 0 [100,2000]Hz

Dial tone frequency 2: 0 [100,2000]Hz

Busy Tone User Define

User Define Enable: □

Busy Tone Frequency1: 0 [100,2000]Hz

Busy Tone Frequency2: 0 [100,2000]Hz

On Time: 500 [100,10000]ms

Off Time: 500 [100,10000]ms

Ring Back Tone User Define

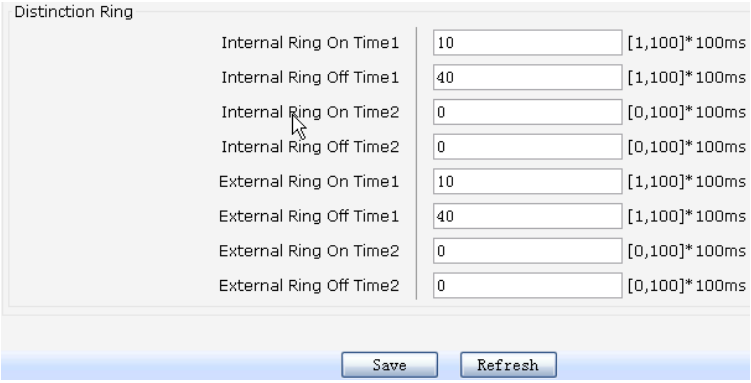
User Define Enable: □

Ring Back Tone Frequency 1: 0 [100,2000]Hz

Ring Back Tone Frequency 2: 0 [100,2000]Hz

On Time: 500 [100,10000]ms

Off Time: 500 [100,10000]ms



Distinction Ring

Internal Ring On Time1	10	[1,100]*100ms
Internal Ring Off Time1	40	[1,100]*100ms
Internal Ring On Time2	0	[0,100]*100ms
Internal Ring Off Time2	0	[0,100]*100ms
External Ring On Time1	10	[1,100]*100ms
External Ring Off Time1	40	[1,100]*100ms
External Ring On Time2	0	[0,100]*100ms
External Ring Off Time2	0	[0,100]*100ms

Figure 3-155 Signal Tone Parameters

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:**

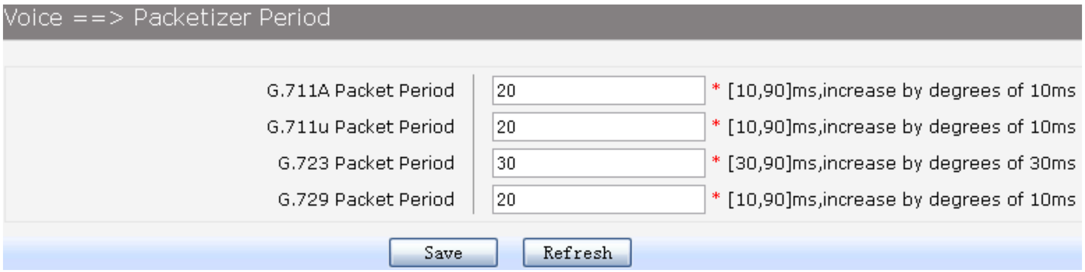
Ring Back Tone

- **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.

3.7.11.5 Packetizer Period

Packet Period defines how long the device sends a RTP packet to the other side. Choose the menu **Voice Service→FXO/FXS Management→Signal Tone** to load the following page.



Voice ==> Packetizer Period

G.711A Packet Period	20	* [10,90]ms,increase by degrees of 10ms
G.711u Packet Period	20	* [10,90]ms,increase by degrees of 10ms
G.723 Packet Period	30	* [30,90]ms,increase by degrees of 30ms
G.729 Packet Period	20	* [10,90]ms,increase by degrees of 10ms

Figure 3-156 Packetizer Period

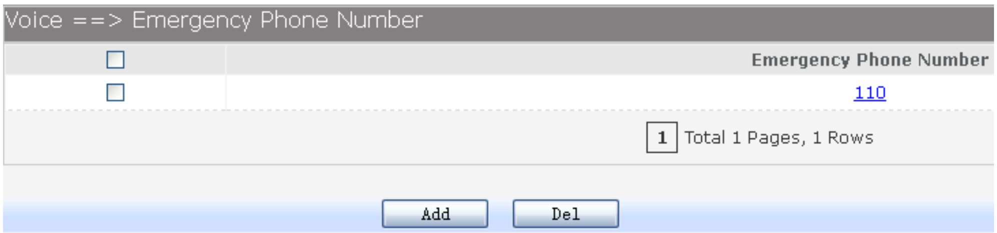
- ► **G.711A Packet Period:** RTP packetization period of G.711A codec.
- ► **G.711u Packet Period:** RTP packetization period of G.711U codec.
- ► **G.723 Packet Period:** RTP packetization period of G.723 codec.
- ► **G.729 Packet Period:** RTP packetization period of G.729 codec.

3.7.12 Advanced Config

3.7.12.1 Emergency Phone Number

User dials the number without calling privileges restricted.

Choose the menu **Voice Service→Advance Config→Emergency Phone Number** to load the following page.



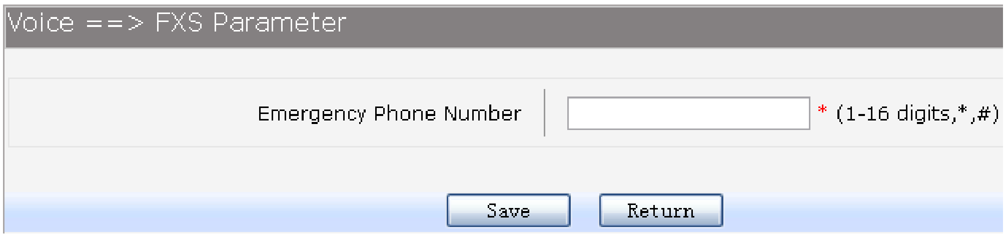
Voice ==> Emergency Phone Number

□	Emergency Phone Number
□	110

1 Total 1 Pages, 1 Rows

Figure 3-157 Emergency Phone Number List

On click **Add** button to load following page.



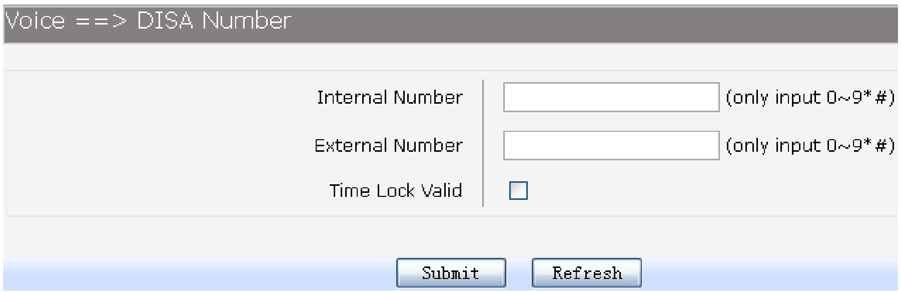
Voice ==> FXS Parameter

Emergency Phone Number		* (1-16 digits,*,#)

Figure 3-158 Emergency Number

3.7.12.2 DISA Number

DISA Number is access code to enter the DISA system. Choose the menu **Voice Service→Advance Config→DISA Number** to load the following page.



Voice ==> DISA Number

Internal Number		(only input 0~9*#)
External Number		(only input 0~9*#)
Time Lock Valid	□	

Figure 3-159 Access Number of DISA

The following items are displayed on this screen:

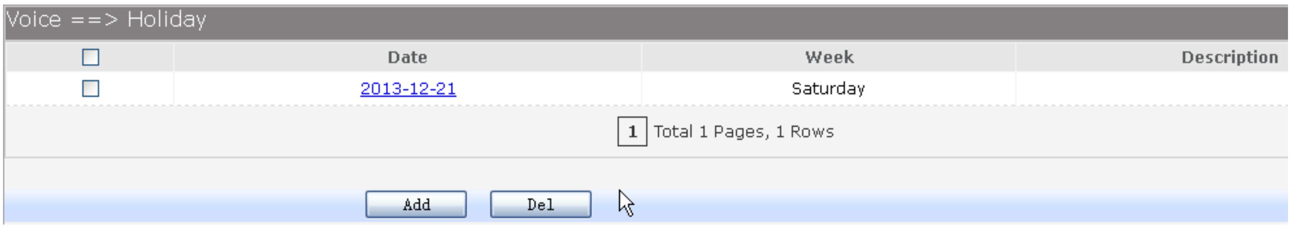
►**Internal number**: Phone number to access the DISA IVR system.

►**Extenal number**: DID number for external users to access the DISA IVR system.

►**Time Lock Valid**: Call permission is affected by Time Lock or not when authenticated by DISA.

3.7.12.3 Holiday

Choose the menu **Voice Service→Advance Config→Holiday** to load the following page.



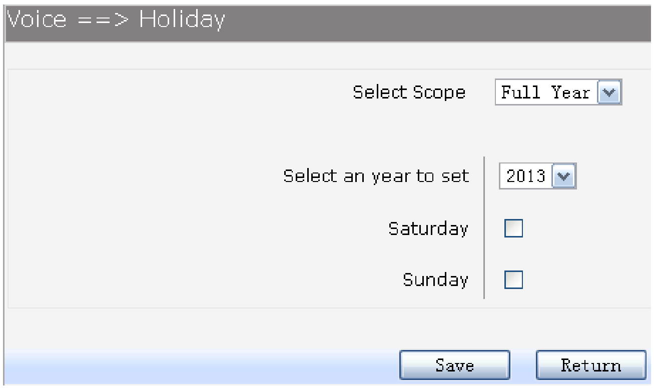
Voice ==> Holiday

□	Date	Week	Description
□	2013-12-21	Saturday	

1 Total 1 Pages, 1 Rows

Figure 3-160 Holiday List

On click **Add** button to load following page.



Voice ==> Holiday

Select Scope: Full Year

Select an year to set: 2013

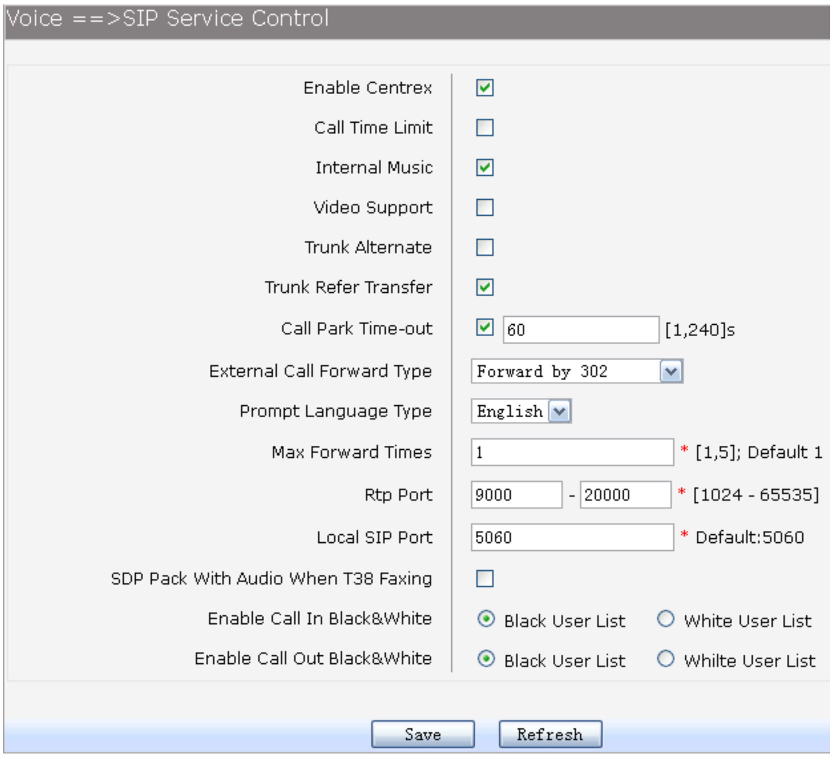
Saturday □

Sunday □

Figure 3-161 Holiday Parameter

3.7.12.4 SIP Service Control

Choose the menu **Voice Service→Advance Config→SIP Service Control** to load the following page.



Voice ==>SIP Service Control

Enable Centrex	☑
Call Time Limit	□
Internal Music	☑
Video Support	□
Trunk Alternate	□
Trunk Refer Transfer	☑
Call Park Time-out	☑ 60 [1,240]s
External Call Forward Type	Forward by 302
Prompt Language Type	English
Max Forward Times	1 * [1,5]; Default 1
Rtp Port	9000 - 20000 * [1024 - 65535]
Local SIP Port	5060 * Default:5060
SDP Pack With Audio When T38 Faxing	□
Enable Call In Black&White	● Black User List ○ White User List
Enable Call Out Black&White	● Black User List ○ Whilte User List

Figure 3-162SIP Service Control Parameters

The following items are displayed on this screen:

►**Centrex**: Whether or not to enable centrex function globally.

►**Call Time Limit**: Set the call time to prevent long talk.

►**Internal Music**: Hear music when extensions call each other.

►**Video Support**: Enable or disable the support of video call.

►**Trunk Alternate**: If the calls of one register IP trunk has reached the maximum, then poll next register IP trunk.

►**Trunk Refer Transfer**: Transfer a call by sending refer or reinvite request.

►**External Call Forward Type**: Reply 302 or send reinvite request.

►**Prompt Language Type**: The language of prompt tone is Chinese or other.

►**Max Forward Times**: A call can be transferred maximum time in the device.

►**Rtp Port**: RTP port range.

►**Local SIP Port**: SIP signaling port number.

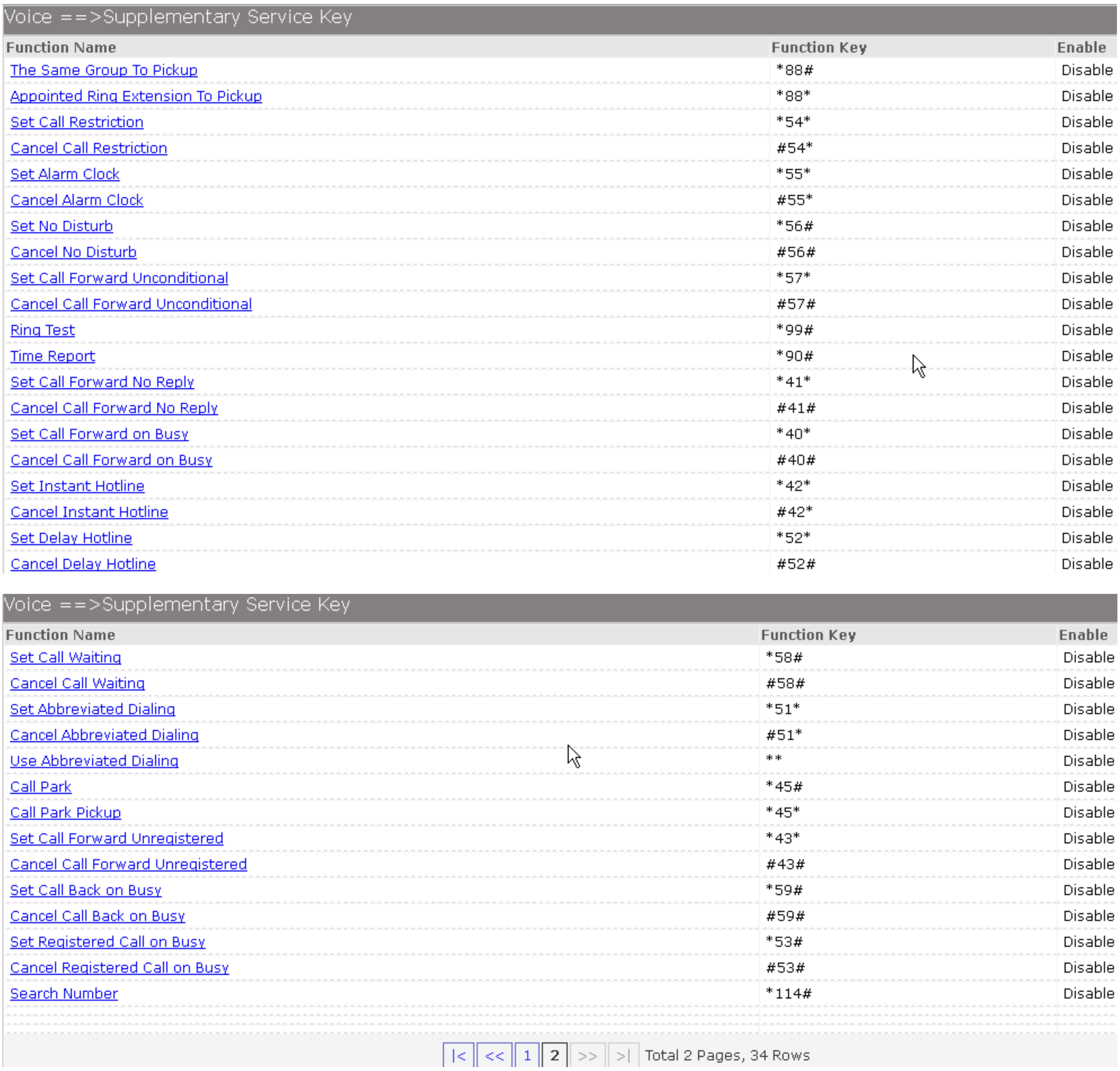
►**SDP Pack With Audio When T38 Faxing**: T38 fax packets with audio information.

►**Enable Call In Black&White**: Enable or disable incoming blacklist or whitelist.

►**Enable Call Out Black&White**: Enable or disable outgoing blacklist or whitelist.

3.7.12.5 Supplementary Service Key

Choose the menu **Voice Service→Advance Config→Supplementary Key** to load the following page.



Voice ==>Supplementary Service Key

Function Name	Function Key	Enable
The Same Group To Pickup	*88#	Disable
Appointed Ring Extension To Pickup	*88*	Disable
Set Call Restriction	*54*	Disable
Cancel Call Restriction	#54*	Disable
Set Alarm Clock	*55*	Disable
Cancel Alarm Clock	#55*	Disable
Set No Disturb	*56#	Disable
Cancel No Disturb	#56#	Disable
Set Call Forward Unconditional	*57*	Disable
Cancel Call Forward Unconditional	#57#	Disable
Ring Test	*99#	Disable
Time Report	*90#	Disable
Set Call Forward No Reply	*41*	Disable
Cancel Call Forward No Reply	#41#	Disable
Set Call Forward on Busy	*40*	Disable
Cancel Call Forward on Busy	#40#	Disable
Set Instant Hotline	*42*	Disable
Cancel Instant Hotline	#42*	Disable
Set Delay Hotline	*52*	Disable
Cancel Delay Hotline	#52#	Disable

Voice ==>Supplementary Service Key

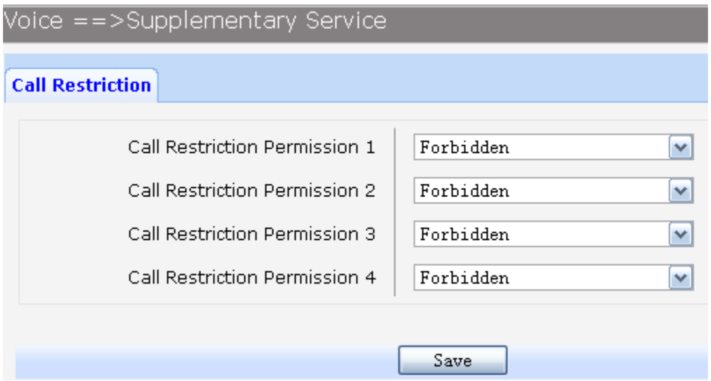
Function Name	Function Key	Enable
Set Call Waiting	*58#	Disable
Cancel Call Waiting	#58#	Disable
Set Abbreviated Dialing	*51*	Disable
Cancel Abbreviated Dialing	#51*	Disable
Use Abbreviated Dialing	**	Disable
Call Park	*45#	Disable
Call Park Pickup	*45*	Disable
Set Call Forward Unregistered	*43*	Disable
Cancel Call Forward Unregistered	#43#	Disable
Set Call Back on Busy	*59#	Disable
Cancel Call Back on Busy	#59#	Disable
Set Registered Call on Busy	*53#	Disable
Cancel Registered Call on Busy	#53#	Disable
Search Number	*114#	Disable

Figure 3-163 Supplementary Service Key List

The items can only be modified, and can't be added, deleted.

3.7.12.6 Supplementary Service

Choose the menu **Voice Service→Advance Config→Supplementary** to load the following page.



Voice ==>Supplementary Service

Call Restriction Permission 1	Forbidden
Call Restriction Permission 2	Forbidden
Call Restriction Permission 3	Forbidden
Call Restriction Permission 4	Forbidden

Figure 3-164 Call Restriction Parameters

Four time-lock corresponding permissions, one must be chosen when user enables password lock.

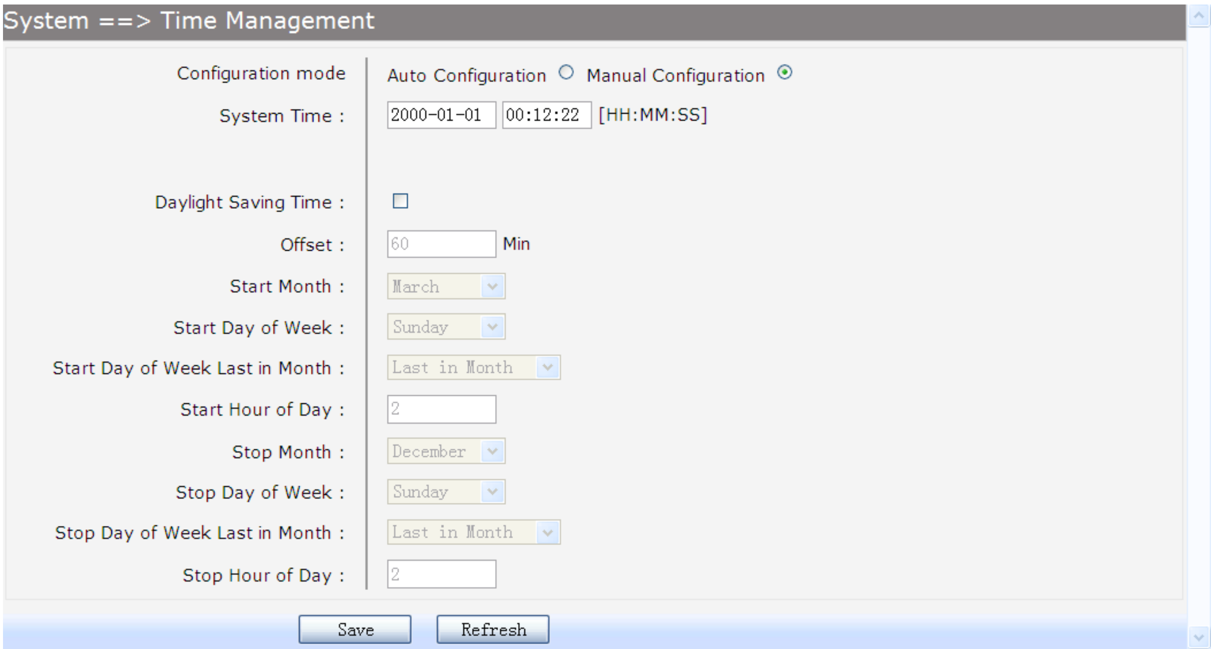
3.8 System

3.8.1 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 ○ Manual Configuration ●

System Time : 2000-01-01 00:12:22 [HH:MM:SS]

Daylight Saving Time : □

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

Figure 3-165 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.

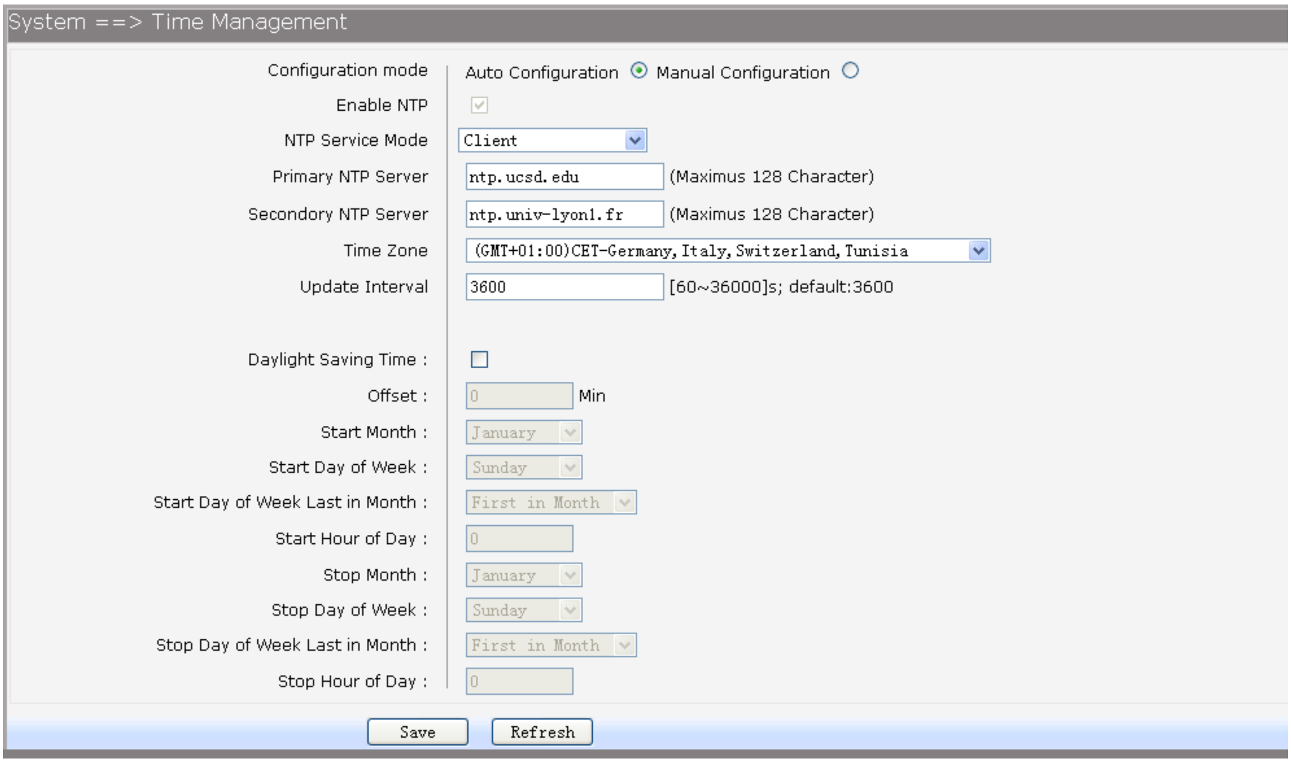
► **End Day of Week:** Specify the end weekday of DST, range from Sunday to Saturday.

► **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 ● Manual Configuration ○

Enable NTP: ☑

NTP Service Mode: Client

Primary NTP Server: ntp.ucsd.edu (Maximus 128 Character)

Secondory NTP Server: ntp.univ-lyon1.fr (Maximus 128 Character)

Time Zone: (GMT+01:00)CET-Germany,Italy,Switzerland,Tunisia

Update Interval: 3600 [60~36000]s; default:3600

Daylight Saving Time : □

Offset : 0 Min

Start Month : January

Start Day of Week : Sunday

Start Day of Week Last in Month : First in Month

Start Hour of Day : 0

Stop Month : January

Stop Day of Week : Sunday

Stop Day of Week Last in Month : First in Month

Stop Hour of Day : 0

Figure 3-166 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.

3.8.2 Upgrade

3.8.2.1 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.

3.8.2.2 Configuration

3.8.2.2.1 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.

3.8.2.2.2 Export Configuration

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

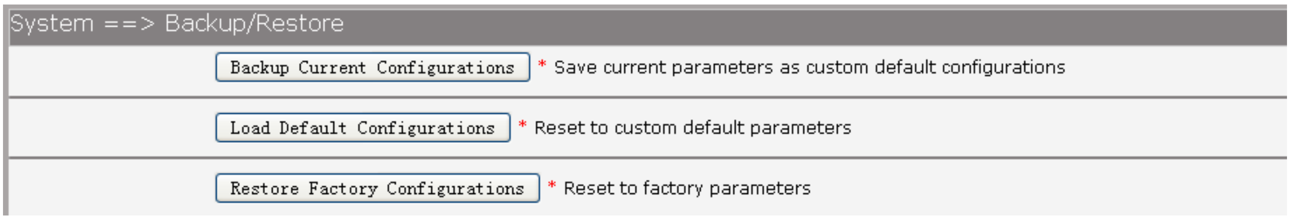
Web interface configuration index: **System**→**Upgrade**→(**Configuration)**.

3.8.3 Reboot System

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

3.8.4 Backup/Restore

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



System ==> Backup/Restore

Backup Current Configurations * Save current parameters as custom default configurations

Load Default Configurations * Reset to custom default parameters

Restore Factory Configurations * Reset to factory parameters

Figure 3-167 Backup/Restore Configurations

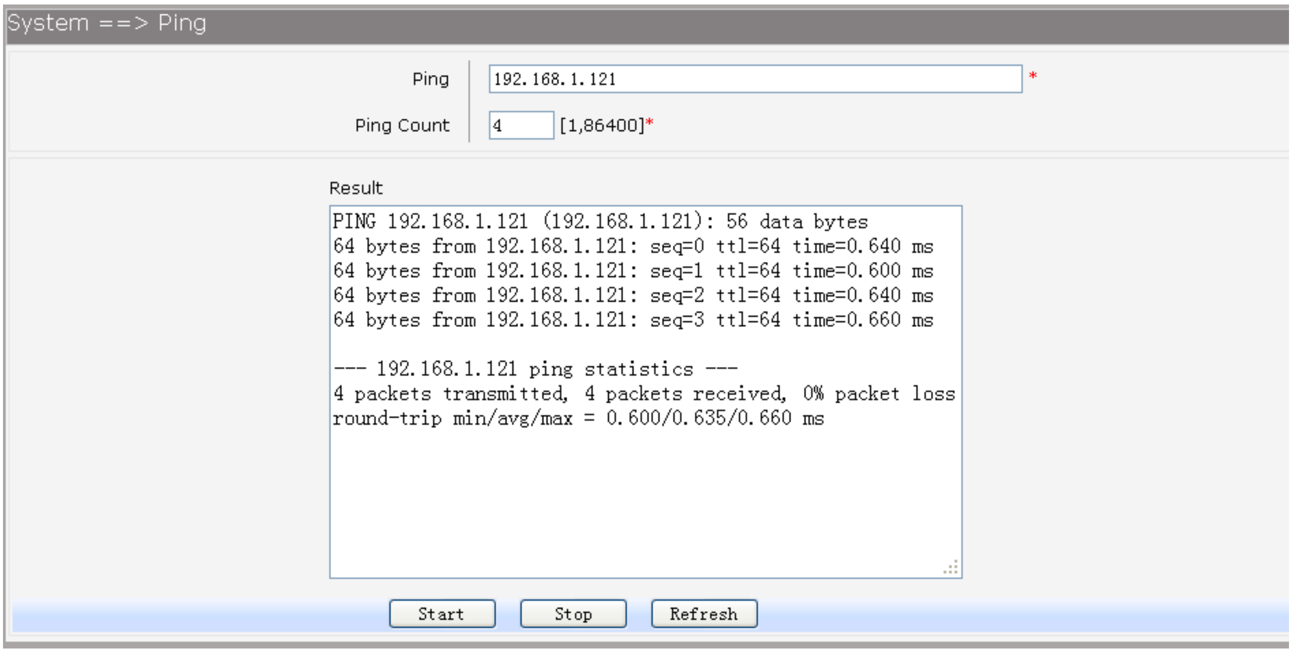
The following items are displayed on this screen:

- **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.

3.8.5 Diagnostic

3.8.5.1 Ping

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



System ==> Ping

Ping: 192.168.1.121 *

Ping Count: 4 [1,86400]*

Result

```
PING 192.168.1.121 (192.168.1.121): 56 data bytes
64 bytes from 192.168.1.121: seq=0 ttl=64 time=0.640 ms
64 bytes from 192.168.1.121: seq=1 ttl=64 time=0.600 ms
64 bytes from 192.168.1.121: seq=2 ttl=64 time=0.640 ms
64 bytes from 192.168.1.121: seq=3 ttl=64 time=0.660 ms

--- 192.168.1.121 ping statistics ---
4 packets transmitted, 4 packets received, 0% packet loss
round-trip min/avg/max = 0.600/0.635/0.660 ms
```

Figure 3-168 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.

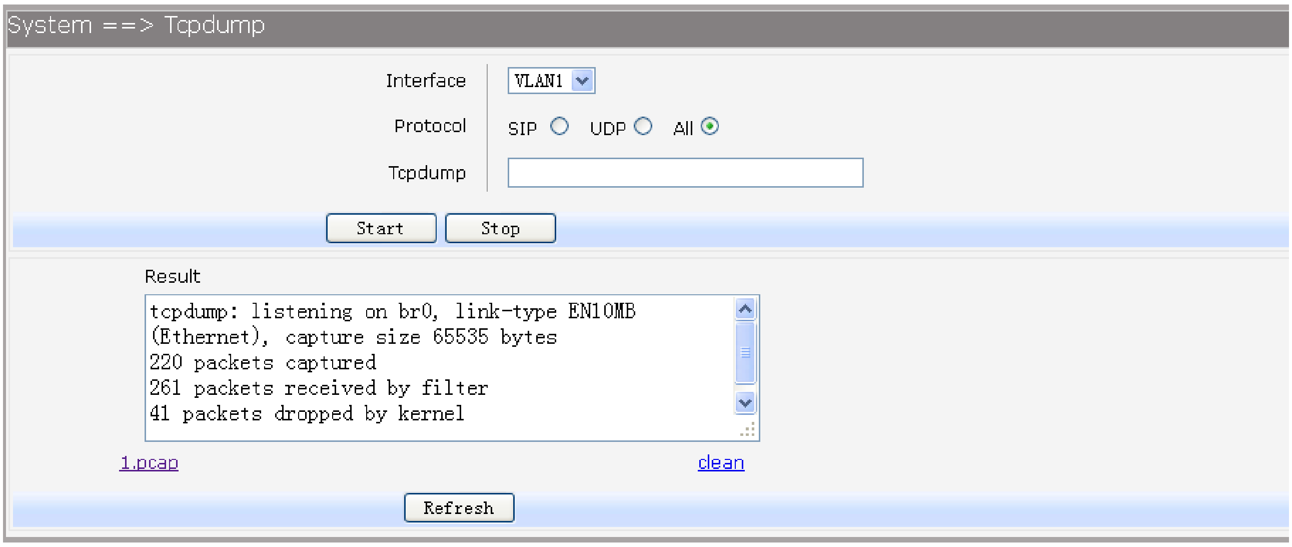
Click **Stop** button to stop sending the Echo Request messages.

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

3.8.5.2 Tcpdump

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

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



System ==> Tcpdump

Interface: VLAN1

Protocol: SIP ○ UDP ○ All ●

Tcpdump:

Result

```
tcpdump: listening on br0, link-type EN10MB
(Ethernet), capture size 65535 bytes
220 packets captured
261 packets received by filter
41 packets dropped by kernel
```

Figure 3-169 Tcpdump Diagnostic

The following items are displayed on this screen:

► **Interface:** By selecting the interface, only packets through this interface will be captured.

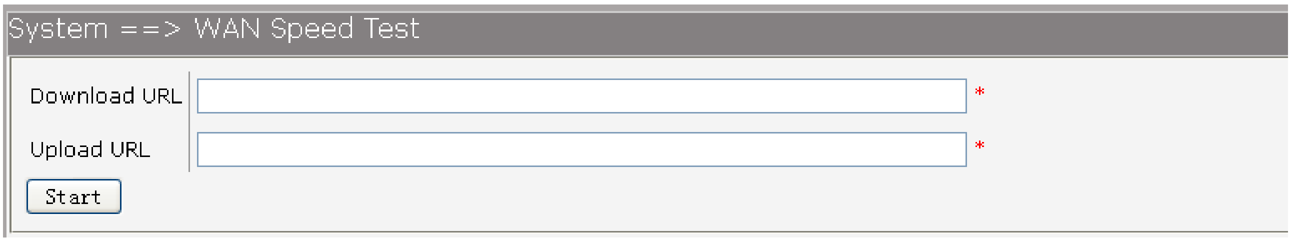
- ► **Protocol:** By selecting the protocol, only packets of this protocol will be captured.
- ► **Tcpdump:** Enter some options of tcpdump(e.g. -n -s0 -c 100**)**
- ► **Result:** This page displays the result of capture packets.

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.

3.8.5.3 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.



System ==> WAN Speed Test

Download URL: *
Upload URL: *

Figure 3-170 WAN Speed Test

The following items are displayed on this screen:

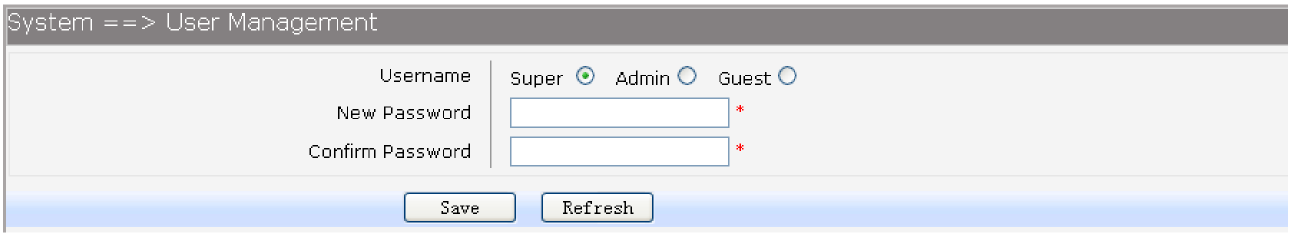
- ► **Download URL:** Enter the URL to test the download speed of WAN. For example http://speedtest1.szunicom.com/speedtest/random1000x1000.jpg
- ► **Upload URL:** Enter the URL to test the upload speed of WAN. For example http://speedtest1.szunicom.com/speedtest/random2000x2000.jpg

Click the **Start** button to starting test.

3.8.6 User Management

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

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



System ==> User Management

Username: Super ● Admin ○ Guest ○
New Password: *
Confirm Password: *

Figure 3-171 User Management

The following items are displayed on this screen:

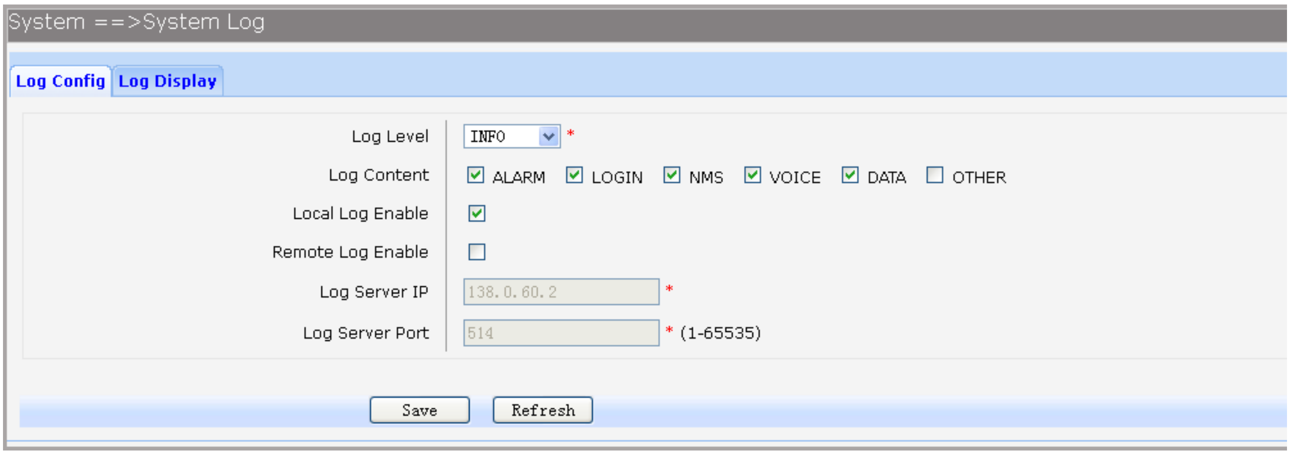
- ► **Username:** You can select the user with different permissions. However, you can not select the user whose permission is higher than your permission.
- ► **New Password:** Enter the new password for specified user, not more than 32 characters, and the space is not supported.
- ► **Confirm Password:**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

3.8.7 System Log

3.8.7.1 Log Config

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



Log Level: INFO *

Log Content: ☑ ALARM ☑ LOGIN ☑ NMS ☑ VOICE ☑ DATA □ OTHER

Local Log Enable: ☑

Remote Log Enable: □

Log Server IP: 138.0.60.2 *

Log Server Port: 514 * (1-65535)

Figure 3-172 Configure System Log

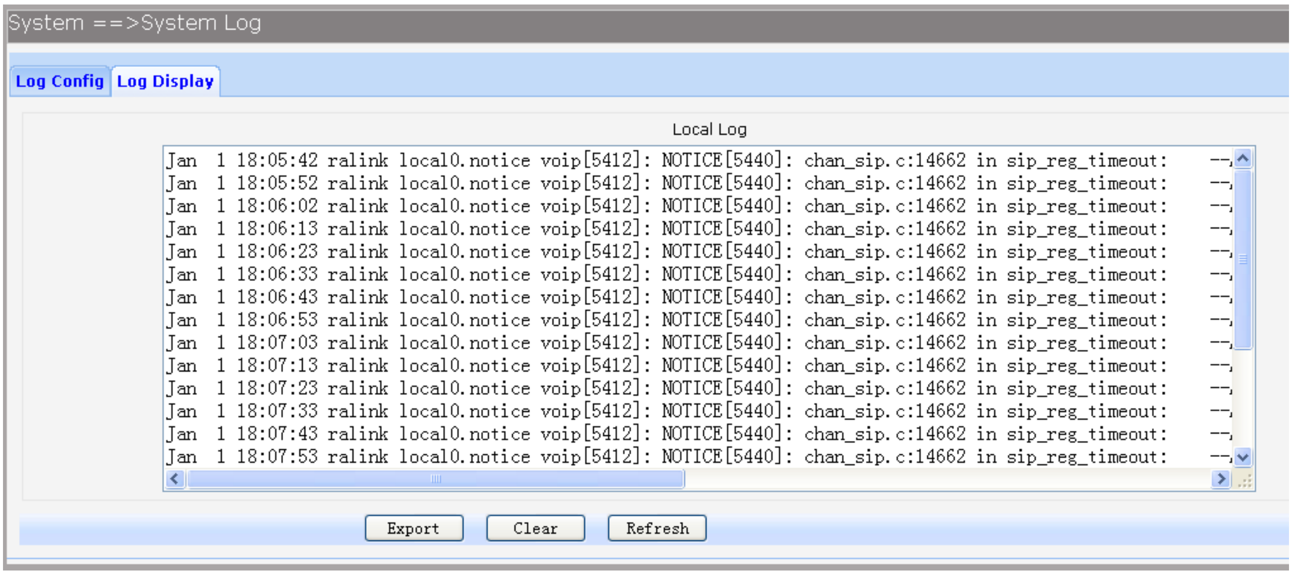
The following items are displayed on this screen:

- ► **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.

3.8.7.2 Log Display

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



Local Log

```
Jan  1 18:05:42 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:05:52 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:06:02 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:06:13 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:06:23 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:06:33 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:06:43 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:06:53 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:07:03 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:07:13 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:07:23 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:07:33 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:07:43 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
Jan  1 18:07:53 ralink local0.notice voip[5412]: NOTICE[5440]: chan_sip.c:14662 in sip_reg_timeout:    --
```

Figure 3-173 Display System Log

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

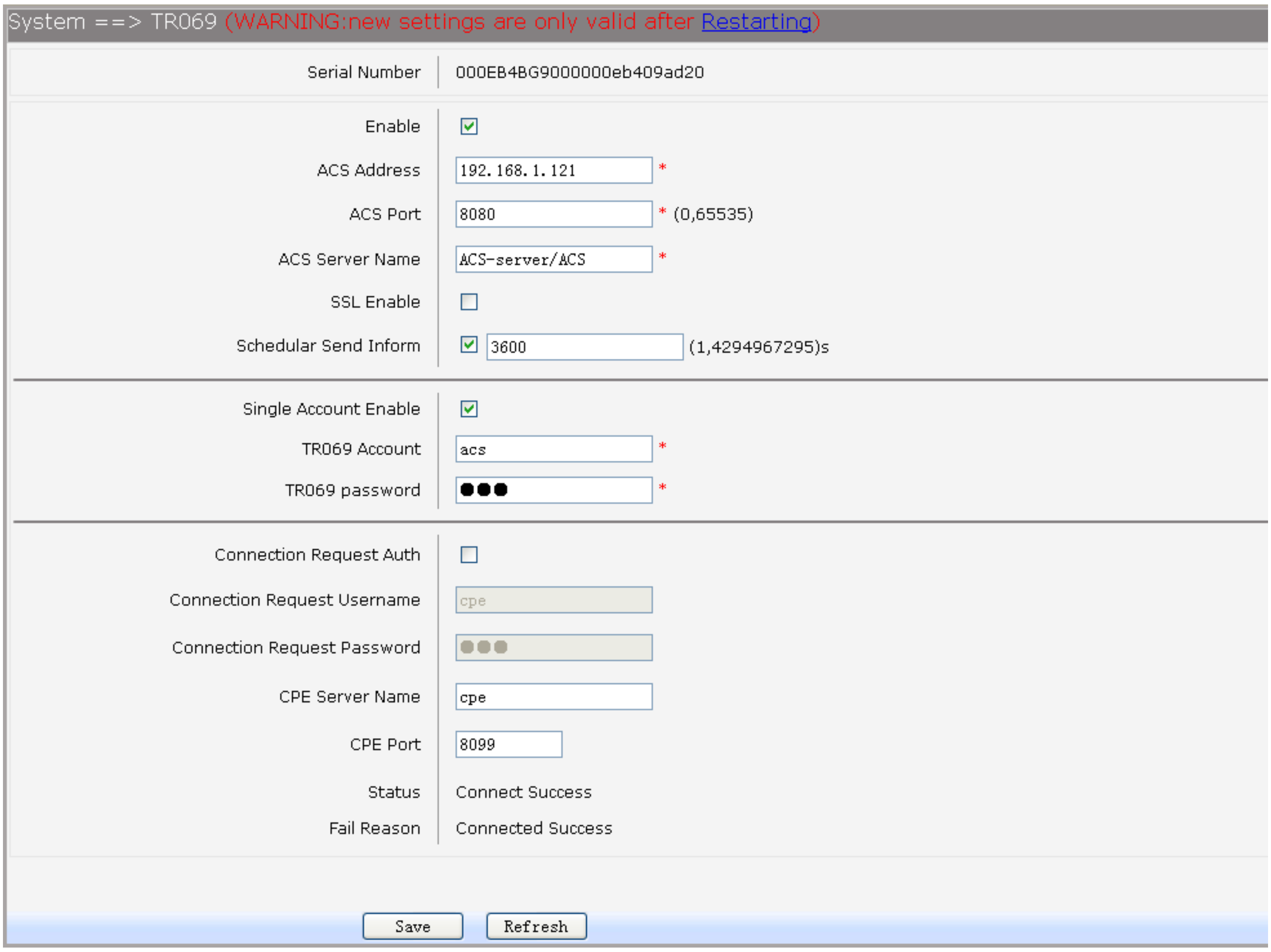
Click the **Clear** button to clear all the local logs from the device permanently, not just from the page.

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

3.8.8 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	000EB4BG9000000eb409ad20
Enable	☑
ACS Address	192.168.1.121 *
ACS Port	8080 * (0,65535)
ACS Server Name	ACS-server/ACS *
SSL Enable	□
Schedular Send Inform	☑ 3600 (1,4294967295)s
Single Account Enable	☑
TR069 Account	acs *
TR069 password	●●● *
Connection Request Auth	□
Connection Request Username	cpe
Connection Request Password	●●●
CPE Server Name	cpe
CPE Port	8099
Status	Connect Success
Fail Reason	Connected Success

Figure 3-174 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.
- **Schedular 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.

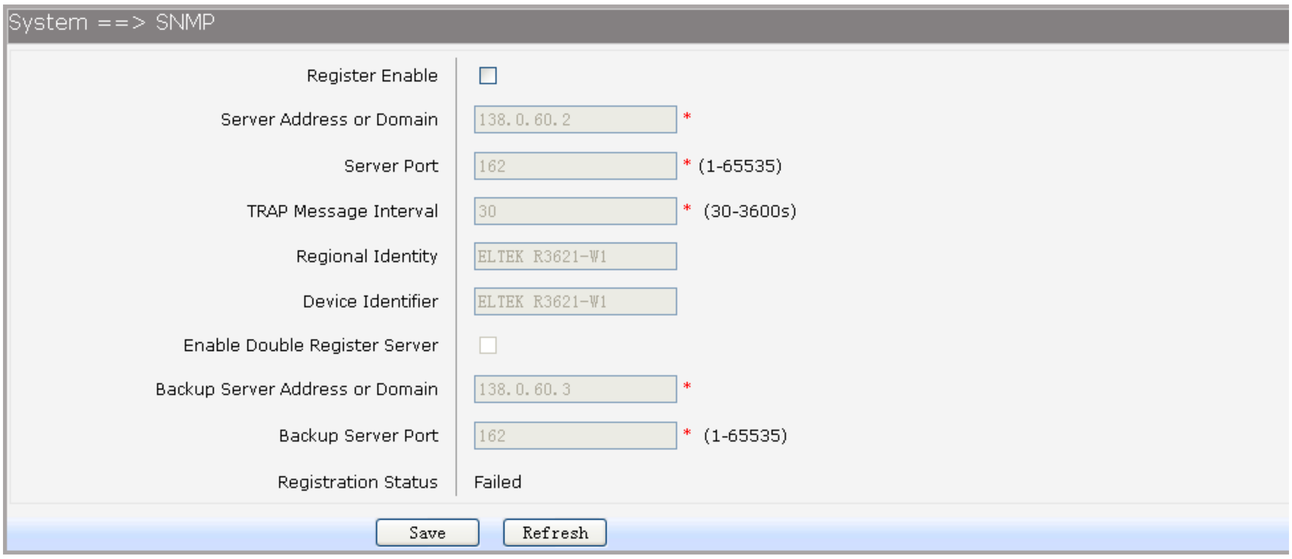
- ► **Single Account Enable:** Whether or not the TR069 Account is enabled.
- ► **TR069 Account:** Username used to authenticate the CPE when making a connection to the ACS.
- ► **TR069 password:** Password used to authenticate the CPE when making a connection to the ACS.
- ► **Connection Request Auth:** 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.

3.8.9 SNMP

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



System ==> SNMP

Register Enable	□
Server Address or Domain	138.0.60.2 *
Server Port	162 * (1-65535)
TRAP Message Interval	30 * (30-3600s)
Regional Identity	ELTEK R3621-W1
Device Identifier	ELTEK R3621-W1
Enable Double Register Server	□
Backup Server Address or Domain	138.0.60.3 *
Backup Server Port	162 * (1-65535)
Registration Status	Failed

Figure 3-175 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.

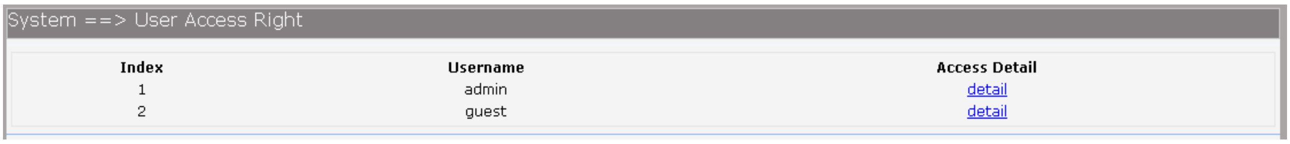
Click the **Save** button when finished.

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

3.8.10 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.

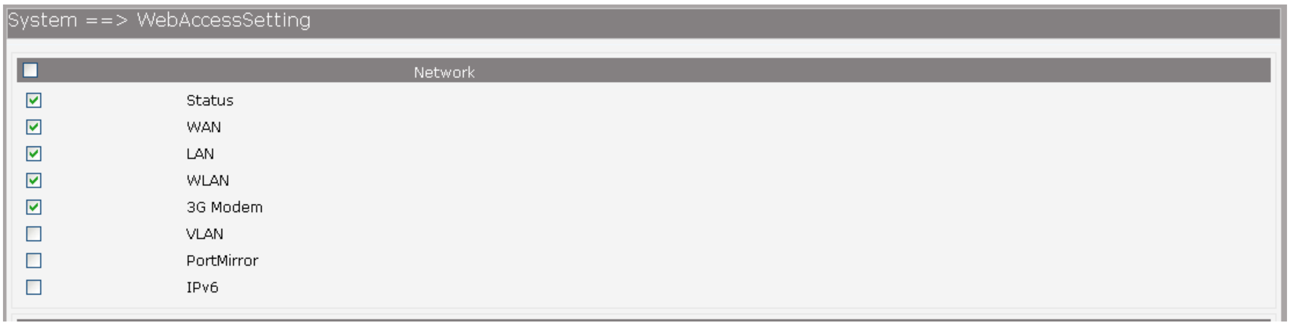


System ==> User Access Right

Index	Username	Access Detail
1	admin	detail
2	guest	detail

Figure 3-176 View users

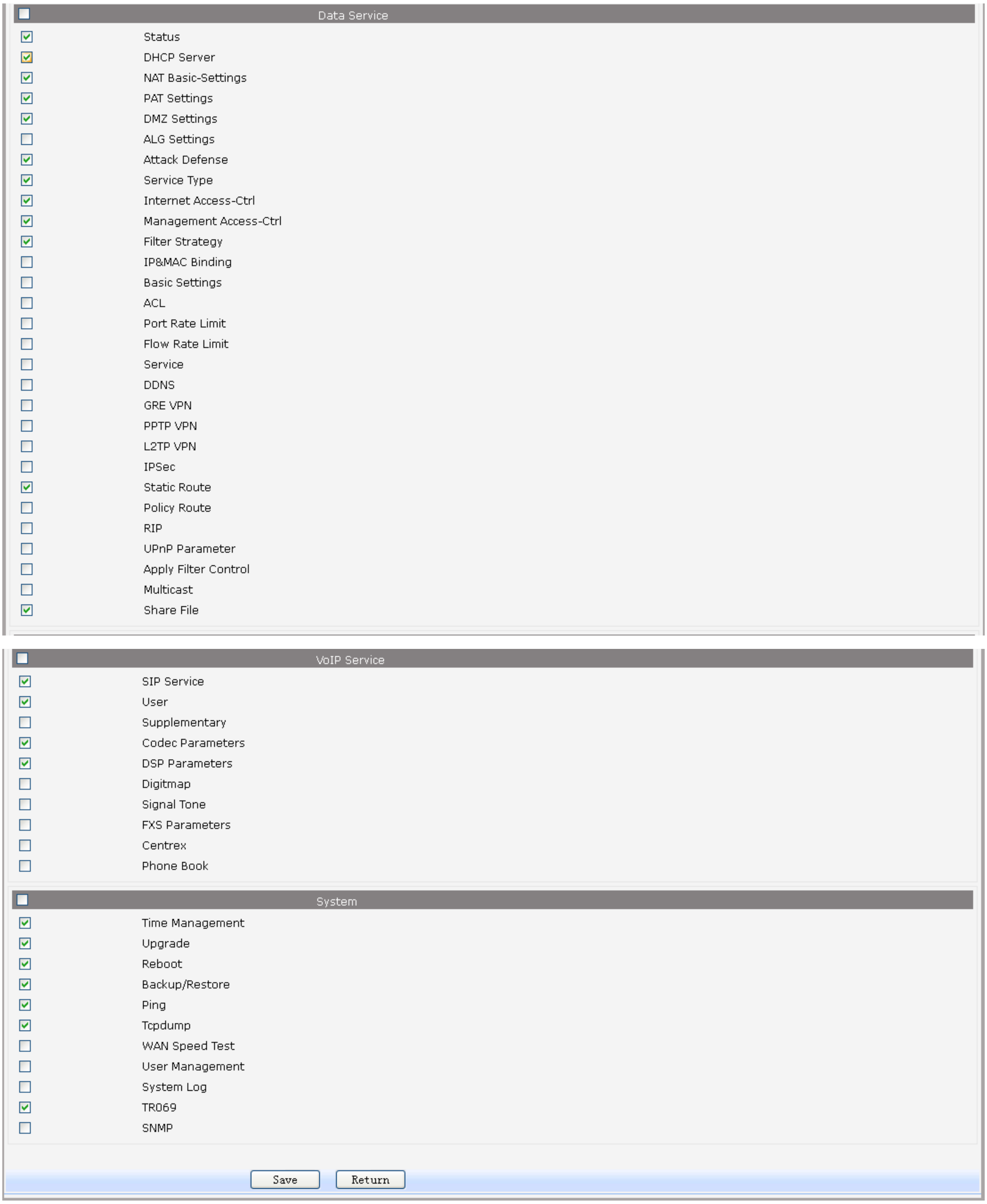
If you want to change the user access right, click **detail** in the entry to load the following page.



System ==> WebAccessSetting

□ Network

- ☑ Status
- ☑ WAN
- ☑ LAN
- ☑ WLAN
- ☑ 3G Modem
- □ VLAN
- □ PortMirror
- □ IPv6



☐ Data Service

☑ Status
☑ DHCP Server
☑ NAT Basic-Settings
☑ PAT Settings
☑ DMZ Settings
☐ ALG Settings
☑ Attack Defense
☑ Service Type
☑ Internet Access-Ctrl
☑ Management Access-Ctrl
☑ Filter Strategy
☐ IP&MAC Binding
☐ Basic Settings
☐ ACL
☐ Port Rate Limit
☐ Flow Rate Limit
☐ Service
☐ DDNS
☐ GRE VPN
☐ PPTP VPN
☐ L2TP VPN
☐ IPSec
☑ Static Route
☐ Policy Route
☐ RIP
☐ UPnP Parameter
☐ Apply Filter Control
☐ Multicast
☑ Share File

☐ VoIP Service

☑ SIP Service
☑ User
☐ Supplementary
☑ Codec Parameters
☑ DSP Parameters
☐ Digitmap
☐ Signal Tone
☐ FXS Parameters
☐ Centrex
☐ Phone Book

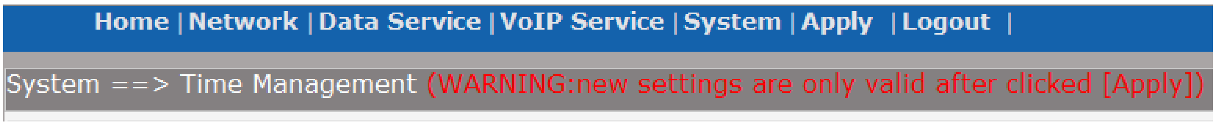
☐ System

☑ Time Management
☑ Upgrade
☑ Reboot
☑ Backup/Restore
☑ Ping
☑ Tcpdump
☐ WAN Speed Test
☐ User Management
☐ System Log
☑ TR069
☐ SNMP

Figure 3-177 Modify User Access Right

3.9 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])

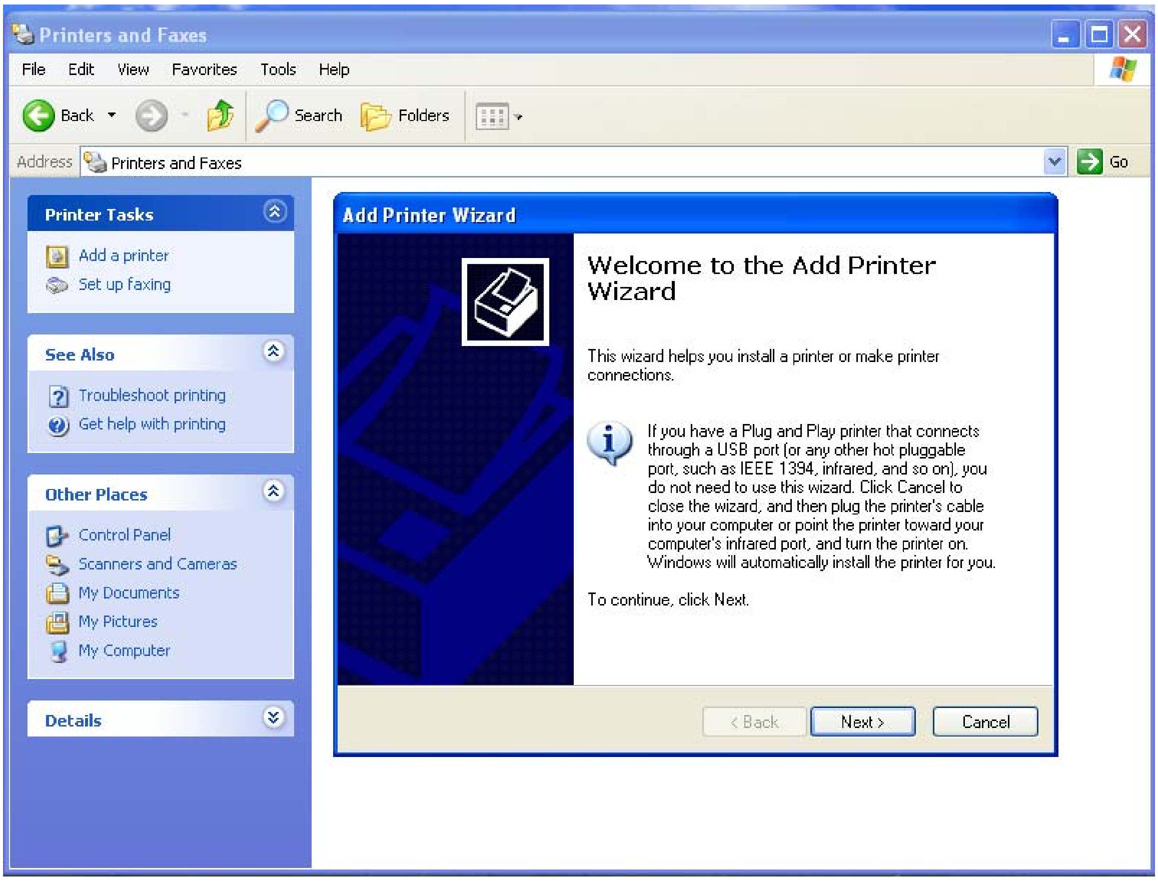
Figure 3-178 Apply

3.10 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



Welcome to the Add Printer Wizard

This wizard helps you install a printer or make printer connections.

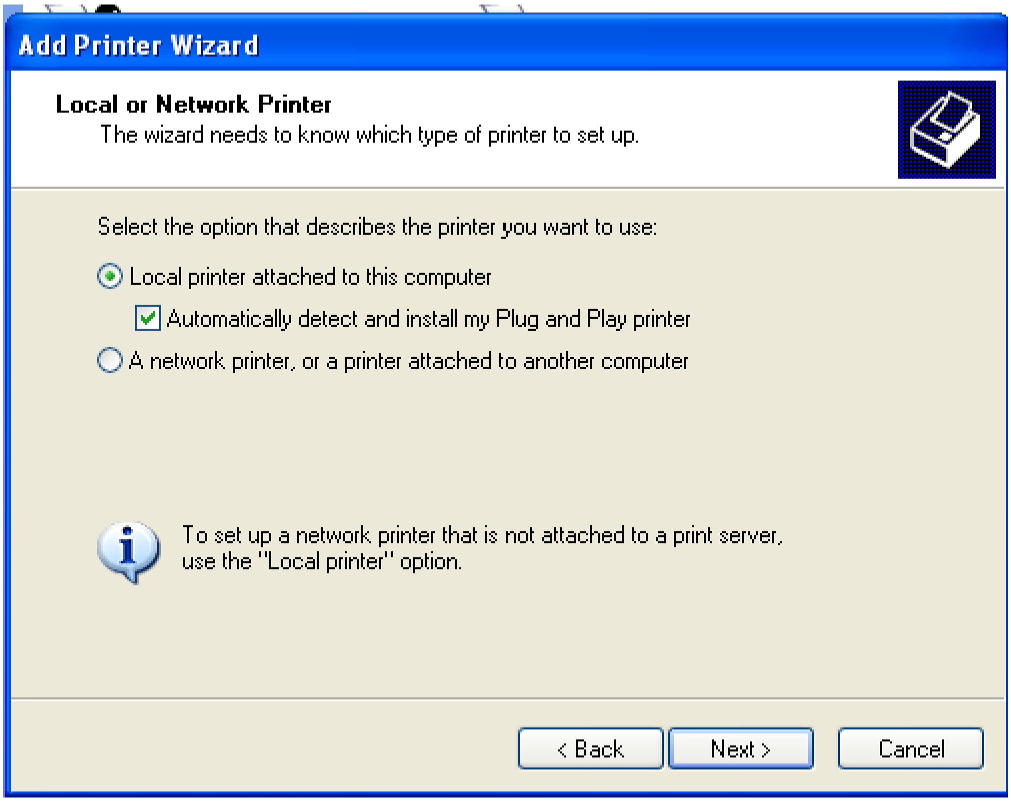
If you have a Plug and Play printer that connects through a USB port (or any other hot pluggable port, such as IEEE 1394, infrared, and so on), you do not need to use this wizard. Click Cancel to close the wizard, and then plug the printer's cable into your computer or point the printer toward your computer's infrared port, and turn the printer on. Windows will automatically install the printer for you.

To continue, click Next.

Figure 3-179 Add Printer

2. Connecting local printer

Select "Local printer attached to this computer."



Add Printer Wizard

Local or Network Printer

The wizard needs to know which type of printer to set up.

Select the option that describes the printer you want to use:

● Local printer attached to this computer

☑ Automatically detect and install my Plug and Play printer

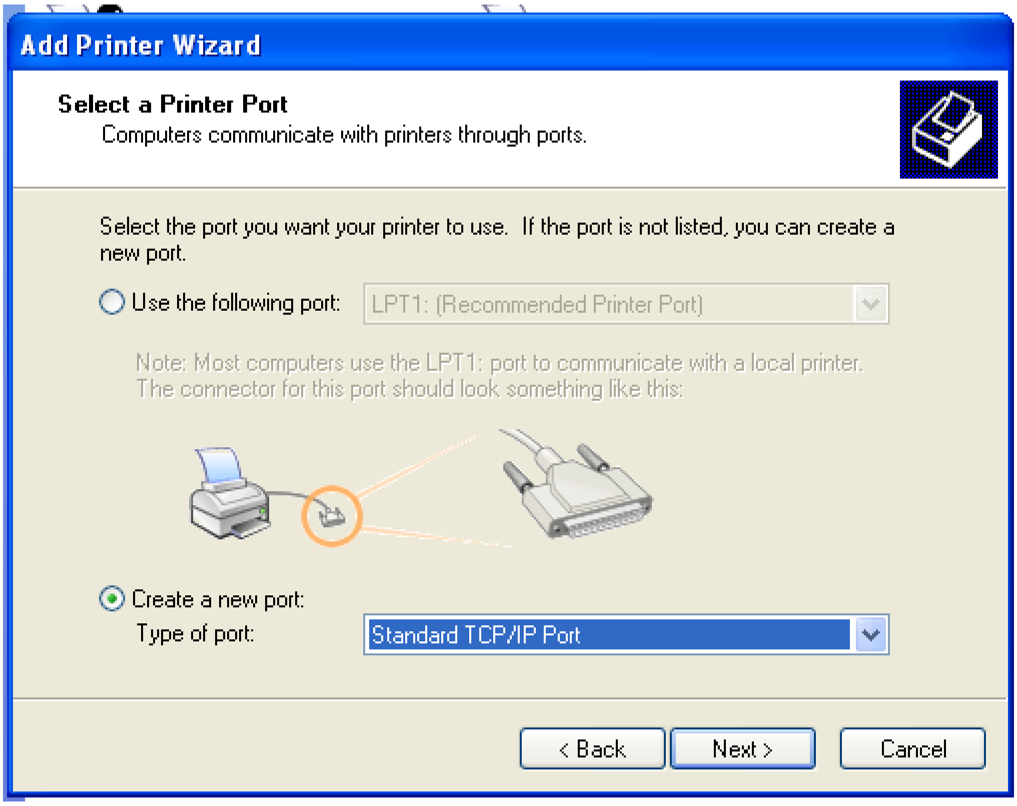
○ A network printer, or a printer attached to another computer

To set up a network printer that is not attached to a print server, use the "Local printer" option.

Figure 3-180 Connecting local printer

3. Create a new port

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



Add Printer Wizard

Select a Printer Port

Computers communicate with printers through ports.

Select the port you want your printer to use. If the port is not listed, you can create a new port.

○ Use the following port: LPT1: (Recommended Printer Port)

Note: Most computers use the LPT1: port to communicate with a local printer. The connector for this port should look something like this:

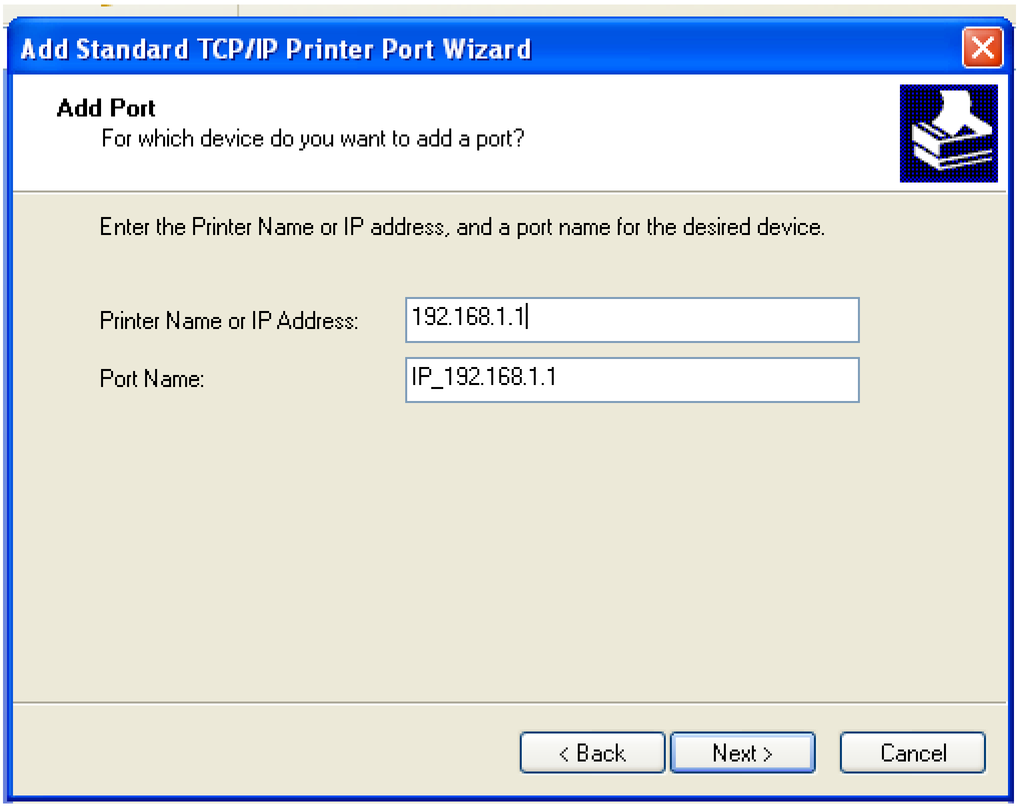
● Create a new port:

Type of port: Standard TCP/IP Port

Figure 3-181 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.

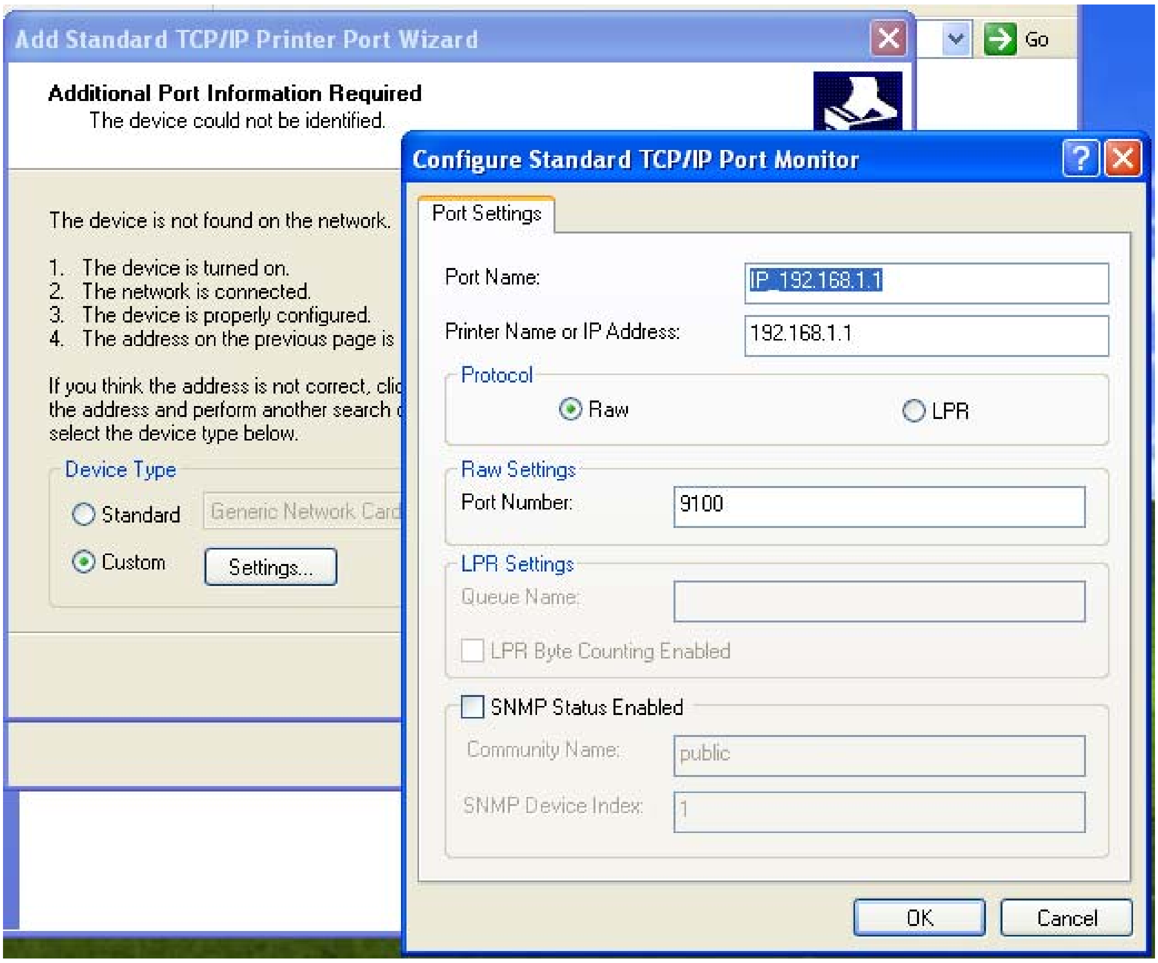
Printer Name or IP Address: 192.168.1.1

Port Name: IP_192.168.1.1

Figure 3-182 Add IP LAN devices

5. Configure printer port

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



Add Standard TCP/IP Printer Port Wizard

Additional Port Information Required

The device could not be identified.

The device is not found on the network.

1. The device is turned on.
2. The network is connected.
3. The device is properly configured.
4. The address on the previous page is

If you think the address is not correct, clic the address and perform another search c select the device type below.

Device Type

○ Standard Generic Network Card

● Custom Settings...

Configure Standard TCP/IP Port Monitor

Port Settings

Port Name: IP_192.168.1.1

Printer Name or IP Address: 192.168.1.1

Protocol

● Raw ○ LPR

Raw Settings

Port Number: 9100

LPR Settings

Queue Name:

□ LPR Byte Counting Enabled

□ SNMP Status Enabled

Community Name: public

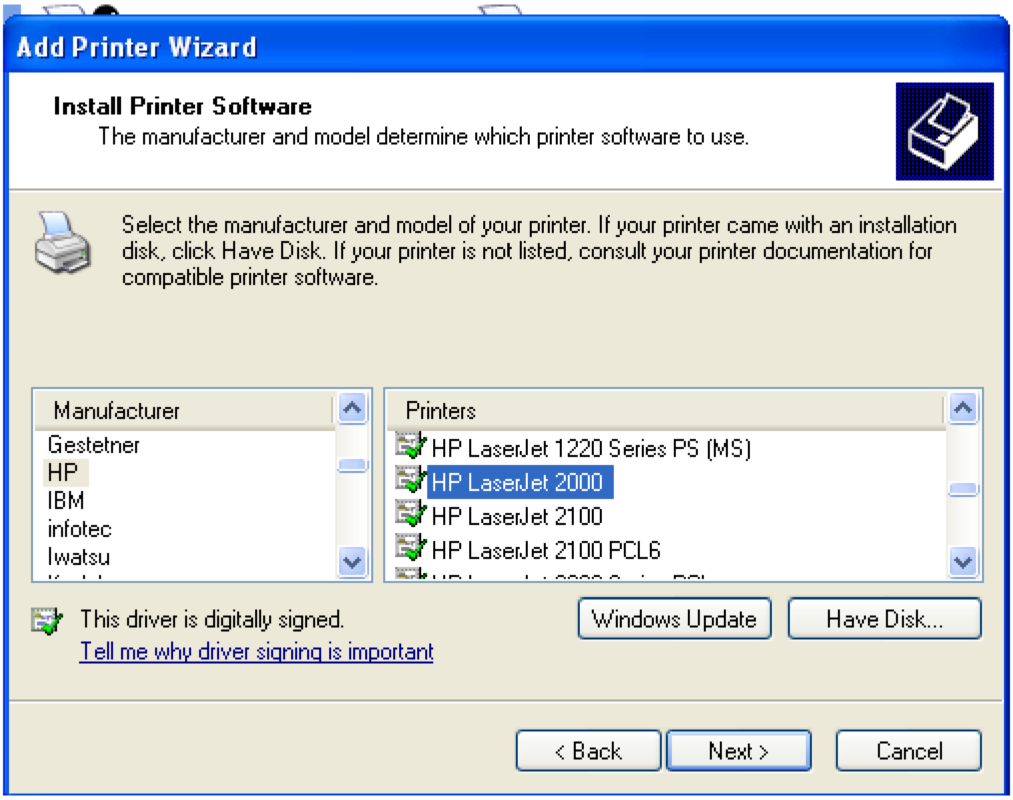
SNMP Device Index: 1

Figure 3-183 Configuer 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.



Install Printer Software

The manufacturer and model determine which printer software to use.

Select the manufacturer and model of your printer. If your printer came with an installation disk, click Have Disk. If your printer is not listed, consult your printer documentation for compatible printer software.

Manufacturer
Gestetner
HP
IBM
infotec
Iwatsu

Printers
HP LaserJet 1220 Series PS (MS)
HP LaserJet 2000
HP LaserJet 2100
HP LaserJet 2100 PCL6

This driver is digitally signed.

Tell me why driver signing is important

Figure 3-184 Add Printer Driver

4 Voice Functions Introduction

4.1 Check Phone Number

4.1.1 Introduction

You can dial a specified number to check your own extension number. The number to be reported is the first group of caller number.

4.1.2 Configuration

The default number for checking is 114. WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**, and click Search number.

4.1.3 Operation Guide

Pick up the phone, listen for the dial tone, and then press 114. A prerecorded voice will let you know the extension number of the phone.

4.2 Time Lock

4.2.1 Introduction

Time Lock is just time-based call restriction. Call permission can be changed automatically for different time period. For example, the extension has permission for local call at working time, and has permission only for internal call at off-duty time. The device supports up to 100 time lock items. Each time lock has 6 time periods setting and a holiday setting. Holidays can be configured to any day you need.

4.2.2 Configuration

1. Enable time lock
   WEB configuration: Choose the menu: **Voice Service→Time Lock→Enable Time Lock**.
2. Add time lock item
   WEB configuration: Choose the menu: **Voice Service→Time Lock→Add**.
3. Select time lock index of subscriber
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.

4.2.3 Operation Guide

Time lock 0 is configured to 8:00 local call, 12:00 internal call, 14:00 local call, 17:30 internal call, and holiday internal call. Time lock 1 is configured to 8:00 long distance call, 12:00 local call, 14:00 long distance call, 17:30 local call, and holiday internal call. Extension A selects time lock 0, extension B selects time lock 1.

1) 8:30, extension B can dial long distance call, extension A can not dial long distance call.
2) 12:30, extension A can only dial internal call, extension B can dial local call and internal call.
3) 15:00, extension B can dial long distance call, extension A can not dial long distance call.
4) 18:00, extension A can only dial internal call, extension B can dial local call and internal call.

4.3 Call Transfer

4.3.1 Introduction

Call transfer enables a user to relocate an existing call to another phone by using the transfer button and dialing the required number. You can tap (quickly press and release) switch-hook if there is no transfer button on the phone.

4.3.2 Configuration

It's no need to configure for call transfer service.

4.3.3 Operation Guide

Extension A is in conversation with user B, A can be the calling party or the called party.

1) A press transfer button, listen for dial tone, and then enter phone number;
2) B will be put on hold, hear MOH(music on hold);
3) A can hang up the phone at any time to finish call transfer.
   - ✧ A hang up after hearing the echo ring, C answer, B and C in conversation.
   - ✧ C answer, A and C in conversation, A hang up, B and C in conversation.

4.4 Call Holding

4.4.1 Introduction

Call holding service allows the user to put an ongoing call on hold, while at the same time making or receiving a second call on the same phone. The held call can be retrieved, and the two calls can be alternate. Call holding can also be used in conjunction with call waiting to allow two calls to be handled at once, so ensuring that important incoming calls are not missed.

4.4.2 Configuration

1) It's no need to configure for call holding service.

2) Flash Key Disable

Choose the menu: **Voice Service→FXO/FXS Management→FXS Parameters** to disable Flash Key.

4.4.3 Operation Guide

Extension A is in conversation with user B, A can be the calling party or the called party.

1) A press transfer button, listen for dial tone;
2) B will be put on hold, hear MOH(music on hold);

3) There are 3 situations next:
   - ✧ A press transfer button again, A and B in conversation;
   - ✧ A call user C, press transfer button before C answer, A and B in conversation;
   - ✧ A call user C, C answer, A and C in conversation;
4) There are 3 situations after C answer:
   - ✧ C hang up, A hear busy tone, A press transfer button, A and B in conversation;
   - ✧ A press transfer button and then press button 2, C will be held, A and B in conversation;
   - ✧ A press transfer button and then press button 1, C will be disconnected, A and B in conversation.

4.5 Call Pickup

4.5.1 Introduction

Call pickup allows one to answer someone's telephone call. This service is accessed by pressing a special sequence of buttons on the telephone.

In places where call pickup is used, the extensions may be divided into groups. Under such an arrangement, using call pickup will only pick up a call in the same group.

Call pickup can be directed. Directed call pickup is used for picking up a call that is ringing at a specific extension number; this feature is accessed through a different sequence of buttons.

4.5.2 Configuration

1. Enable group call pickup and directed call pickup.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Put related extensions to the same group, the device supports up to 100 pickup groups.
   WEB configuration: Choose the menu: **SIP Account→SIP Account Assiged**.

4.5.3 Operation Guide

Extension A and B are in the same pickup group, extension A and C are in different pickup group.

1) User D call extension A , A start ring;
2) B off-hook, press *88#;
3) A stop ring, B and D in conversation;
4) User D call extension C, C start ring;
5) B off-hook, press *88*TN#, TN is the extension number of C;
6) C stop ring, B and D in conversation.

4.6 Call Forwarding Unconditional

4.6.1 Introduction

Call Forwarding Unconditional (CFU) allows an incoming call to be redirected to another phone number in any condition.

4.6.2 Configuration

1. Enable “Set Call Forward Unconditional” and “Cancel Call Forward Unconditional”.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Set CFU number.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
   Keypad service system: ***57*TN#**, TN is the phone number to be redirected to.
3. Cancel CFU.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
   Keypad service system: **#57#**.

4.6.3 Operation Guide

1) Extension A off-hook, press “*57*8001#”, 8001 is the phone number of C, voice prompts “operation is successful” will be heard;
2) User B call A, C start ring;
3) C answer, B and C in conversation.

4.7 Call Forwarding on Busy

4.7.1 Introduction

Call Forwarding on Busy (CFB) allows an incoming call to be redirected to another phone number when the user is busy.

4.7.2 Configuration

1. Enable “Set Call Forward on Busy” and “Cancel Call Forward on Busy”.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Set CFB number.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
   Keypad service system: ***40*TN#**, TN is the phone number to be redirected to.
3. Cancel CFB.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
   Keypad service system: **#40#**.

4.7.3 Operation Guide

1) Extension A off-hook, press “*40*8001#”, 8001 is the phone number of C, voice prompts “operation is successful” will be heard;
2) A keep off-hook;
3) User B call A, C start ring;
4) C answer, B and C in conversation.

4.8 Call Forwarding No Reply

4.8.1 Introduction

Call Forwarding No Reply (CFNR) allows an incoming call to be redirected to another phone number when the user is no reply within a specified period of time.

4.8.2 Configuration

1. Enable “Set Call Forward No Reply” and “Cancel Call Forward No Reply”.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Set CFNR number.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
   Keypad service system: ***41*TN#**, TN is the phone number to be redirected to.
3. Cancel CFNR.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
   Keypad service system: **#41#.**
4. Set CFNR wait time.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.

4.8.3 Operation Guide

1) Extension A off-hook, press “*41*8001#”,8001 is the phone number of C, voice prompts “operation is successful” will be heard;
2) User B call A, A start ring;
3) Wait 30 seconds, C start ring;
4) C answer, B and C in conversation.

4.9 Call Forwarding Unregistered

4.9.1 Introduction

Call Forwarding Unregistered (CFUR) allows an incoming call to be redirected to another phone number when the user is unregistered. This feature is only for SIP user.

4.9.2 Configuration

1. Enable “Set Call Forward Unregistered” and “Cancel Call Forward Unregistered”.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Set CFUR number.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
   Keypad service system: ***43*TN#**, TN is the phone number to be redirected to.
3. Cancel CFUR.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.

Keypad service system: **#43#**.

4.9.3 Operation Guide

1) SIP user A off-hook, press “*43*8001#”, 8001 is the phone number of C, voice prompts “operation is successful” will be heard;
2) A unregister from the device;
3) User B call A, C start ring;
4) C answer, B and C in conversation.

4.10 Hunt Group

4.10.1 Introduction

A hunt group is a collection of extensions that ring in a particular order when the hunt group number is dialed. Hunt group usually have a phone number associated with them, which is 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.

4.10.2 Configuration

1. Add a hunt group.
   WEB configuration: Choose the menu: **Voice Service→Ring Group→Add.**
2. Add related extensions into the group. The first extension added has the highest priority.
   WEB configuration: Choose the menu: **Voice Service→Ring Group→Extension Number**.

4.10.3 Operation Guide

a) Hunt Group 8000, internal type, parallel ring sequence, members include extension A, extension B and extension C.
   1) Extension D dial 8000, A, B and C ring at the same time;
   2) B answer, B and D in conversation.
b) Hunt Group 8001, internal type, ordinal ring sequence, ring time 15 seconds, members include extension A, extension B and extension C, the extension configured order is ABC.
   1) Extension D dial 8001, A start ring;
   2) A don’t answer, B start ring after 15 seconds;
   3) B don’t answer, B start ring after more 15 seconds;
   4) C answer, D and C in conversation;
   5) D hang up and dial 8001 again, A start ring.
c) Hunt Group 87654321, external type, alternate ring sequence, ring time 15 seconds, members include extension A, extension B and extension C, the extension configured order is ABC.
   1) User D dial 87654321, A start ring;
   2) A don’t answer, B start ring after 15 seconds;
   3) B don’t answer, B start ring after more 15 seconds;

4) C answer, D and C in conversation;
5) D hang up and dial 87654321 again, B start ring.

4.11 Auto Attendant

4.11.1 Introduction

Auto attendant service allows callers to be automatically transferred to an extension without the intervention of an operator, and also allows a caller to reach a live operator by dialing a number, usually "0". Auto attendant will have a greeting message that is played to callers, this message can be configured. Different message to play in different time period is available. Each user group has an auto attendant, supports up to 40 phone numbers.

4.11.2 Configuration

1. Parameters.
   - **DTMF interval**: inter-digit timer for DTMF collecting.
   - **DTMF total time**: total time use for DTMF collecting.
   - **Extension wait answer time**: the caller will return to the main menu when the timer expired.
   - **Auto attendant number**: the phone number to access the auto attendant system.
   - **IVR menu**: a set of parameters for time-based application.
   - **Auto transfer**: auto transfer to the operator after playing greeting message.
   - **Key define**: define the key to reach the operator or a certain department.
2. Enable auto attendant.
   WEB configuration: Choose the menu: **Voice Service→Auto Attendant→Generic.**
3. Add auto attendant number.
   WEB configuration: Choose the menu: **Voice Service→Auto Attendant→Generic**.
4. Add IVR menu.
   WEB configuration: Choose the menu: **Voice Service→Auto Attendant→IVR Menu**.
5. Specify IVR menu for different time period.
   WEB configuration: Choose the menu: **Voice Service→Auto Attendant→IVR Configuration**.
6. Change greeting prompts.
   WEB configuration: Choose the menu: **Voice Service→Voice File→IVR Menu**.
7. Disable auto transfer to an extension.
   WEB configuration: Choose the menu: **Voice Service→Auto Attendant→Generic**.

4.11.3 Operation Guide

An auto attendant with number 87654321, IVR menu 1 uses greeting prompts for business hours, key 0 is correspond to hunt group 8888 which includes extension A and extension B, IVR menu 2 uses greeting prompts for non-business hours, key 0 is correspond to extension C, start time 1 8:00 with IVR menu 1, start time 1 17:300 with IVR menu 2.

1) User D dial 87654321 at 9:00, greeting prompts for business hours will be heard, dial 0, A start ring;
2) A answer, A and D in conversation;

3) User E dial 87654321 next, dial 0, B start ring;
4) B answer, B and E in conversation;
5) B transfer the call to extension C, C answer, B and C in conversation;
6) D hang up, E hang up;
7) D dial 87654321 at 18:00, greeting prompts for non-business hours will be heard, dial 0, C start ring;
8) C answer, D and C in conversation.

4.12 DISA

4.12.1 Introduction

DISA (Direct Inward System Access) allows external callers to place a call to outside after pass authorization, as if they were placing a call from the internal extension. It is very helpful for cost saving. DISA also can be used for internal callers, provides password authentications and elevates call permission when the extension wants to make an external call.

DISA authentication information includes account and password, the password can be omitted. The system uses the extension number as the DISA account, so that the account can be regarded as an extension easily. For adding a DISA account, simply add a SIP account, and then configure the extension number. The length of DISA account should be specified for fast dialing, while the length of password can be arbitrary in stated range.

Once the caller accesses into the DISA system, the system will prompt the caller to input DISA information for authorization. Flexible input method is available at this time. The caller can input the account, password and destination number together, or input the account and password first, the input the destination number follow the prompts. The internal caller can access the DISA feature by using DISA direct dialing key, without Interactive Voice Response (IVR) support.

4.12.2 Configuration

1. Parameters.
   - **Internal number**: phone number to access the DISA IVR system.
   - **External number**: DID number for external users to access the DISA IVR system.
   - **Time Lock Effective**: call permission is affected by Time Lock or not when get through DISA authentication.
   - **DISA enable**: DISA feature is enabled for this extension.
   - **DISA password**: password for authentication.
   - **DISA bind caller number**: the caller from this number does not need to input authentication codes.
   - **DISA restrictive caller**: only caller from these numbers is permitted for this account, authentication is requisite all the same.
2. Configure DISA access number.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→DISA Number**.
3. Add DISA account.
   Add SIP account first, and then configure the extension number of the corresponding SIP account.
4. Configure DISA password.

WEB configuration: Choose the menu: **SIP Account→Advance Config**.

5. Modify DISA direct dialing key.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→DISA Number**.

4.12.3 Operation Guide

DISA access number is 333, account length is 4. Extension number of user A is 8001, DISA password is 1234, call permission is Long Distance, and current call permission is degraded to Internal by Call Restriction feature. DISA account of user B is 7001, which is bound with an unregistered SIP account, DISA password is 5678, and call permission is Local.

1) User B make a local call to 87654321 directly on extension A, failure prompts will be heard;
2) B dial 333,input 7001*5678, then input 81234567 follow the voice prompts, the call can be connected;
3) A make a local call to 87654321 directly on extension A, failure prompts will be heard;
4) A dial 333, input 8001*1234, then input 81234567 follow the voice prompts,a call to 87654321 will be placed.

4.13 Conference Call

4.13.1 Introduction

Conference call allows the calling party to call the other participants and add them to the conference. It also allows the called party to participate during the call.

4.13.2 Configuration

3. Parameters.
   - **Public conference**: Indicates the conference is public or not. The public conference is always open, and the private conference is only open at specified time.
   - **Wait moderator**: the participants can not speak at the beginning when the conference is configured to wait moderator, they should ask for permission of moderator to speak.
   - **Internal conference number**: internal phone number to enter this conference room.
   - **External conference number**: DID number to enter this conference room.
   - **Moderator PIN**: used to distinguish the moderator and other participants.
   - **Member PIN**: used for participant authentication, should be different from moderator authenticate code.
   - **Start time**: start time for private conference.
   - **End time**: end time for private conference.
   - **Max participants**: max participants for this conference room.
4. Participant key control.
   - **Mute**: mute oneself on one’s own. It’s disabled in wait moderator mode. It works like toggle switch, one will be muted the first time the keys pressed, and gets back next time.
   - **Mute&Deaf**: mute and deaf oneself on one’s own, it’s disable in wait moderator mode.
   - **Request to speak**: participants ask for permission to speak in wait moderator mode.
   - **Disable speak**: participants mute themselves in wait moderator mode, no need to confirm.
5. Moderator key control.

- **Mute**: mute moderator self or other participants. Instructions for participant mute, mute keys+ participant number.
- **Mute&Deaf**: mute and deaf moderator self.
- **Invite Member**: add participant to the conference call.
- **Kick Member**: Kick participant to the conference call.
- **Transfer moderator**: transfer the moderator role to another participant.
- **Recording**: start or end recording of conference call
- **Accept speak request**: allow the participant to speak after received the request.
- **Refuse speak request**: disallow the participant to speak after received the request.
- **Conference lock**: nobody can join the conference after the conference is locked unless the moderator call them or unlock the conference.

6. Add conference room.
   WEB configuration: Choose the menu: **Voice Service→Conference**.

4.13.3 Operation Guide

A conference room is configured as public conference, with internal phone number 5555, the moderator authentication code is 1234.

1) Extension A dial 5555, a greeting message will be heard, then dial 1234, A will become the moderator of conference;
2) A dial *13+TN+# to add B to the conference call, TN is the phone number of B;
3) B answer, A and B can talk to each other;
4) Extension C dial 5555 to join the conference;
5) User D call the Auto Attendant, then dial 5555 to join the conference;
6) A, B, C, D are all in conference call.

4.14Voicemail

4.14.1 Introduction

Voice mail is used to convey a caller's recorded audio message when you can not answer the phone. It contains a user interface to select, play and manage messages. If one’s voice mail is enabled, the call will be transferred to the voice mail system when the phone is busy or ring time out. Special dial tone will be played in order to inform the FXS user of a waiting message.

4.14.2 Configuration

1. Parameters.
   - **Voice mail number**: the phone number to access the voice mail system.
   - **Total message time**: total time for message depositing.
   - **Password**: password used for message retrieving.
   - **Overflow action**: describes the action to be taken when the messages are full.
   - **Voice file**: Specify a greeting prompts which will be played to the caller.
2. Set voice mail number.
   WEB configuration: Choose the menu: **Voice Service→Voice Mail Number**.
3. Enable voice mail.

WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.

4.14.3 Operation Guide

Voice mail number is 7777, Extension A enable voice mail.

1) A off-hook, keep busy;
2) B make a call to A, the call will be transferred to the voice mail;
3) B hear greeting prompts, and leave a message after the beep;
4) B hang up, A hang up;
5) A off-hook, special dial tone will be heard;
6) A dial 7777, retrieve the message follow the voice prompts.

4.15 Call Waiting

4.15.1 Introduction

Call Waiting lets you to take a second call without disconnecting the first. When you're on the phone, a Call Waiting tone (two fast beeps for FXS user) alerts you when you have another incoming call. You can simply put the first caller on hold and answer the second call. If you're on an important call and do not wish to answer the incoming call, you can simply continue talking.

4.15.2 Configuration

1. Enable "Set Call Waiting" and "Cancel Call Waiting".
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Enable call waiting.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary.**
   Keypad service system: ***58#**.
3. Cancel call waiting.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**
   Keypad service system: **#58#**.

4.15.3 Operation Guide

1) Extension A dial *58#, voice prompts "operation is successful" will be heard;
2) A make a call to B, B answer;
3) C make a call to A, A hear two fast beeps;
4) A press transfer button, then press 2, B will be holded, A and C in conversation;
5) A press transfer button, then press 1, C will be disconnected, A and B in conversation.

4.16 Three Party Calling

4.16.1 Introduction

Three Party Calling allows you to add a third party to your conversation. You can create a three party call base on Call Holding or Call Waiting.

4.16.2 Configuration

1. Enable "Set Call Waiting" and "Cancel Call Waiting"
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Enable call waiting.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary.** And choose the menu: **Voice Service→FXO/FXS Management→FXS Parameter** to configure Flash Key Enable.
   Keypad service system: ***58#**.
3. Change Three Party Calling key settings.
   WEB configuration: Choose the menu: **Voice Service→FXO/FXS Management→FXS Parameter**.

4.16.3 Operation Guide

1) Extension A place a call to B, B answer, A and B in conversation;
2) A press transfer button, put B on hold;
3) A listen for dial tone, place a second call to C;
4) C answer, A and C in conversation;
5) A press transfer button, then press 3, A, B and C are in three party call;
6) C hang up, A and B keep talking as a ordinary call;
7) C place a call to A, A hear call waiting tone;
8) A press transfer button, then press 2, A and C in conversation;
9) A press transfer button, then press 3, A, B and C are in three party call;

4.17 Call Restriction

4.17.1 Introduction

Call Restriction enables you to restrict or bar certain or all types of calls from your phone, i.e. long distance calls, international calls.

4.17.2 Configuration

1. Enable "Set Call Restriction" and "Cancel Call Restriction".
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Set Call Restriction permission classification, to associate K value with call permission, K value range [1-4].
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary.**
3. Set Call Restriction PIN code.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary.**
4. Enable Call Restriction.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.

Keypad service system: ***54*KSSSS#**, K stands for call permission, SSSS is the PIN code.

5. Cancel Call Restriction
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
   Keypad service system: **#54*SSSS#**, SSSS is the PIN code.

4.17.3 Operation Guide

Call Restriction permission classification: 1 – Forbidden, 2 – Internal, 3 – Local, 4 – Long Distance. Extension A with call permission Long Distance, call restriction PIN is 1234.

1) A off-hook, dial ***54*21234#**, lock call permission to Internal, voice prompts “operation is successful” will be heard;
2) A place a long distance call, failure prompts will be heard;
3) A dial **#54*2234#**, switch off Call Restriction;
4) A place a long distance call, the call can be connected.

4.18 Color Ring

4.18.1 Introduction

Color Ring, also called Color Ring Back Tone (CRBT), allows you to replace traditional ring back tone with euphonic song when someone places a call to you.

4.18.2 Configuration

1. Enable Color Ring.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
2. Import music file for Color Ring, personalized Color Ring is not supported currently.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.

4.18.3 Operation Guide

1) Extension A enable Color Ring;
2) B make a call to A, A start Ring, B hear the specified color ring.

4.19 Blacklist & Whitelist

4.19.1 Introduction

Blacklist & Whitelist is an application which detects incoming calls and rejects unwanted callers who are blacklisted or allow only whitelist numbers to come through. It also can be used for outgoing calls that you can not make a call to the number in the blacklist or only whitelist numbers is permitted.

4.19.2 Configuration

1. Enable Call In Black&White.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→SIP Service**

Control.

2. Enable Call Out Black&White.

   WEB configuration: Choose the menu: **Voice Service→Advance Config→SIP Service Control**.

3. Add incoming blacklist.

   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Incoming Black&White List**.

4. Add outgoing blacklist.

   WEB configuration: Choose the menu: **SIP Account→Account Parameter→OutGoing Black&White List**.

4.19.3 Operation Guide

Extension number of A is 6001, extension number of B is 7001, and extension number of C is 8001. Extension A with outgoing blacklist 7001 and incoming whitelist 8001, extension B with outgoing whitelist 6 and incoming blacklist 8.

1) A dial 7001, failure prompts will be heard;
2) A dial 8001, C start ring;
3) B dial 6001, failure prompts will be heard;
4) C dial 6001, A start ring;
5) B dial 6001, failure prompts will be heard;
6) B dial 8001, C start ring;
7) A dial 7001, failure prompts will be heard;
8) C dial 7001, B start ring;

4.20 Emergency Phone Number

4.20.1 Introduction

Users dial the number without calling privileges restricted.

4.20.2 Configuration

1)Configure user power

WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary.**

2)Add emergency phone number

WEB configuration: Choose the menu: **Voice Service→Advance Config→Emergency Phone Number.**

3)Add Call route

WEB configuration: Choose the menu: **Voice Service→Call Route**

4.20.3 Operation Guide

1) The call out permission of extension A is Internal.
2) 110 is emergency phone number.
3) Add call route, prefix is 1, total length is 0.
4) A dial 18902301718, failure prompts will be heard.

5) A dial 110, successful.

4.21 Call Time Limit

4.21.1 Introduction

Call Time Limit lets the call disconnect automatically when the call duration reached the specified time.

4.21.2 Configuration

1. Parameters.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**
   - **Internal Call Limit**: time limit for internal call, a setting of 0 disables the time limit.
   - **IP Trunk Call Limit**: time limit for outgoing calls via SIP trunk.
2. Set the interval for disconnecting the call.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→SIP Service Control**.

4.21.3 Operation Guide

Extension A configured internal call limit time to 1 minute.

1) A place a call to extension B, B answer;
2) Wait 1 minute, the call will be disconnected.

4.22 Alarm Clock

4.22.1 Introduction

Alarm Clock lets the phone ring at a specified time for alerting.

4.22.2 Configuration

1. Enable “Set Alarm Clock” and “Cancel Alarm Clock”.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Set alarm clock.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
   Keypad service system: ***55*HHMM#,** HH denotes hour, MM denotes minute.
3. Cancel alarm clock.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
   Keypad service system: **#55*HHMM#**.

4.22.3 Operation Guide

1) Extension A dial *55*1200#, set alarm clock to 12:00 noon.
2) Wait alarm clock time out, A start ring, A off-hook, alerting prompts will be heard.

4.23 Do Not Disturb

4.23.1 Introduction

Do Not Disturb (DND) allows you to totally block incoming calls at any time. When activated, your phone no longer rings when callers attempt to reach you. Callers are presented with a message that you are busy.

4.23.2 Configuration

1. Enable “Set Do Not Disturb” and “Cancel Do Not Disturb”.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Enable DND.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
   Keypad service system: ***56#.**
3. Cancel DND.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary**.
   Keypad service system: **#56#**.

4.23.3 Operation Guide

1) Extension A dial *56#, voice prompts “operation is successful” will be heard;
2) B make a call to A, failure prompts will be heard;
3) A dial #56#, cancel Do Not Disturb;
4) B make a call to A again, A start ring;

4.24 Delay Hotline

4.24.1 Introduction

Stored hotline number will be sent if no key was pressed in 5 seconds after off-hook.

4.24.2 Configuration

1. Enable “Set Delay Hotline” and “Cancel Delay Hotline”.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Set delay hotline.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary,** Delay Time Long must Greater than 0.
   Keypad service system: ***52*TN#**, TN is the hotline number.
3. Cancel delay hotline.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary,** empty hotline number.
   Keypad service system: **#52#**.

4.24.3 Operation Guide

1) Extension A dial *52*8001#, 8001 is phone number of user B;
2) A off-hook, special dial tone will be heard, B start ring after 5 seconds;
3) B answer, A and B in conversation;
4) A on-hook, end conversation;
5) A off-hook, dial #52#, deactivate delay hotline, then on-hook;
6) A off-hook, hear normal dial tone, and hear busy tone after 10 seconds;

4.25 Instant Hotline

4.25.1 Introduction

Stored hotline number will be sent immediately when you pick up the phone.

4.25.2 Configuration

1. Enable “Set Instant Hotline” and “Cancel Instant Hotline”.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Set instant hotline.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary,** Delay Time Long must equal to 0.
   Keypad service system: ***42*TN#**, TN is the hotline number.
3. Cancel instant hotline.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary,** empty hotline number.
   Keypad service system: **#42*EN#**, instant hotline can be deactivated at other extension, and EN is the extension number which needs to deactivate instant hotline.

4.25.3 Operation Guide

Extension number of A is 8000, extension number of B is 8001.

1) Extension A dial *42*8001#, then on-hook;
2) A off-hook, B start ring immediately;
3) B answer, A and B in conversation;
4) A on-hook, end conversation;
5) B off-hook, dial #42*8000#, deactivate instant hotline of extension A;
6) A off-hook, dial tone will be heard;

4.26 Call Park

4.26.1 Introduction

Call Park allows an extension to put a call on hold at one telephone and retrieve the call from any other extension by pressing a special sequence of buttons.

4.26.2 Configuration

1. Enable “Call Park” and “Call Park Pickup”.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**.
2. Set call park timeout ring back.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→SIP Service Control,** Call Park Time-out.

4.26.3 Operation Guide

Extension number of A is 8001.

1) A and B in conversation;
2) A press transfer button, dial *45#, A will be heard park number XXXX;
3) Extension C off-hook, dial #45*XXXX#, C in conversation with B.

4.27 Recording

4.27.1 Introduction

User conversation is being recorded, Recording files are automatically stored on the device, A call corresponds to a file.

4.27.2 Configuration

1)Set Record file
WEB configuration: Choose the menu: **Voice Service→Record File→Voice File Capacity**.

2)Extension enable record
WEB configuration: Choose the menu: **SIP Account→Account Parameter→Advance Config**

4.27.3 Operation Guide

Enable record of Extension A.

1)A dial B, B ring.
2)B off-hook, A talking B.
3)A on-hook, end conversation.
4)Choose the menu: **Voice Service→Record File→Call Recording,** you will find record file**.**

4.28 Call Back On Busy

4.28.1 Introduction

When you dial busy number, you can register callback service on the busy number. The other phone is idle, the caller will automatically ring, after caller off hook, the busy call will ring.

4.28.2 Configuration

1.Enable “Set Call Back on Busy” and “Cancel Call Back on Busy”.

WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key**

2.Extension enable Call Back On Busy

WEB configuration: Choose the menu: **SIP Account→Account Parameter→Supplementary,** Call Back On Busy.

3.Set Call Back on Busy

Keypad service system: ***59#.**

4.Cancel Call Back on Busy

Keypad service system: **#59#.**

4.28.3 Operation Guide

Enable Call Back on Busy of Extension A, Extension B number is 8001.

1)B off-hook, busying.

2)A dial 80001.then input 1 follow the voice prompts.

3)A on-hook, B on-hook.

4)A ring, A off-hook.

5)B ring, B off-hook, A talking B.

4.29 Centrex

4.29.1 Introduction

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

4.29.2 Configuration

1. Enable Centrex.

WEB configuration: Choose the menu: **Voice Service→Advance Config→SIP Service Control.**

2. Cancel Centrex

WEB configuration: Choose the menu: **Voice Service→Advance Config→SIP Service Control.**

4.29.3 Operation Guide

1)A, B are two extensions equipment;

2)Centrex open;

3)A make a call to B, or B make a call to A, don't call out by SIP Server, talk normal;

4)Centrex close;

5)A make a call to B, or B make a call to A, don't call out by SIP Server, call failed;

4.30 Abbreviated Dialing

4.30.1 Introduction

Abbreviated Dialing allows you to store selected phone numbers for quick and easy dialing. Each telephone number can be dialed by using a two-digit code with a simple prefix. Stored numbers may be up to 32 digits in length.

4.30.2 Configuration

1. Enable “Set Abbreviated Dialing”, “Cancel Abbreviated Dialing” and “Use Abbreviated Dialing”.
   WEB configuration: Choose the menu: **Voice Service→Advance Config→Supplementary Key.**
2. Add an abbreviated dialing entry.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Abbreviated Dialing,**on click Add.
   Keypad service system: ***51*SS*TN#,** SS is the two-digit short code, TN is the phone number.
3. Delete an abbreviated dialing entry.
   WEB configuration: Choose the menu: **SIP Account→Account Parameter→Abbreviated Dialing,**on click Del.
   Keypad service system: **#51*SS#.**

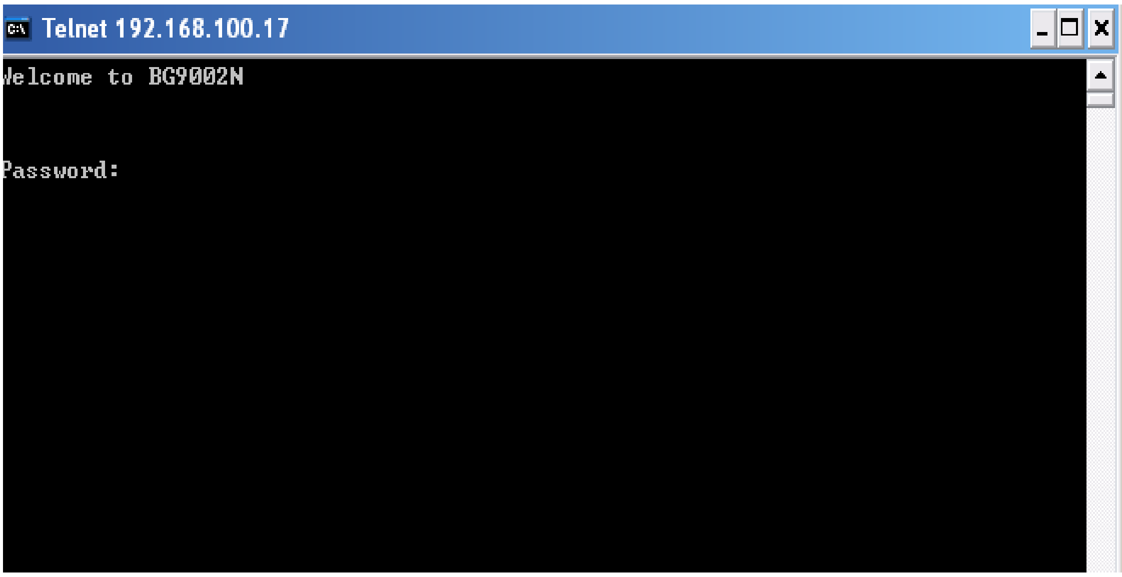
4.30.3 Operation Guide

1) Extension A off-hook, listen for dial tone;
2) A dial *51*11*12345678#, set 11 short for 12345678;
3) A hear voice prompts “operation is successful”, then hang up;
4) A off-hook, dial **11, a call to 12345678 will be placed.

5 CLI Introduction

5.1 Login

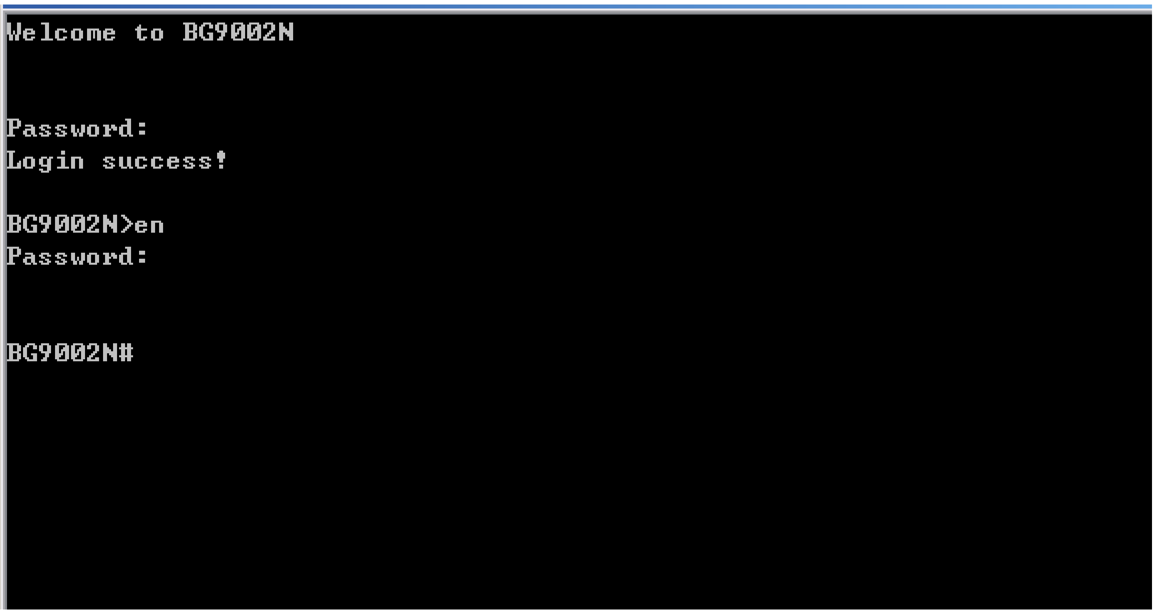
The CLI interface is ready for accessing about one minute after the device powers on. The default LAN IP address is 192.168.100.1, you can access the CLI interface via either WAN port or LAN port. Enter telnet with IP address and then press ENTER, you can get access to the Login interface. Such as IP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



```
Welcome to BG9002N


Password:
```

Figure 5-1 Telnet Login

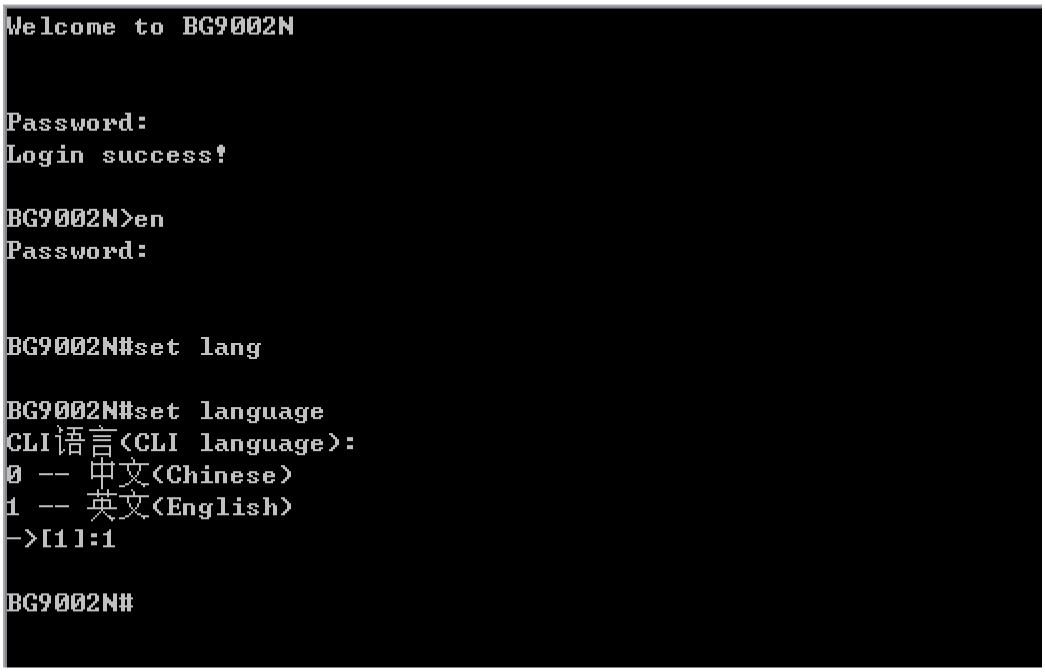
And input the “password” and “en” and the privileged password, you will enter the CLI command interface:



```
Welcome to BG9002N


Password:
Login success!

BG9002N>en
Password:


BG9002N#
```

Figure 5-2 Telnet Command Interface

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



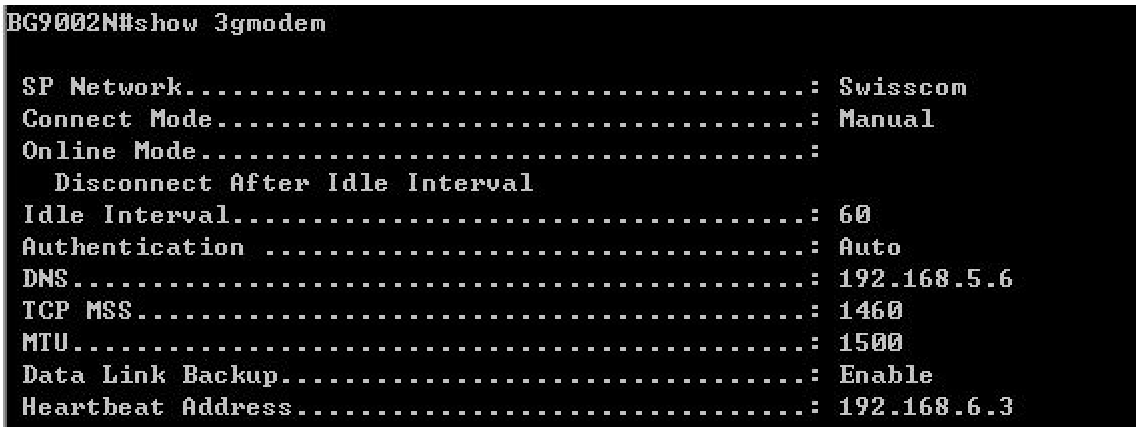
```
Welcome to BG9002N


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 5-3 Set CLI Language

5.2 Network

5.2.1 3G Modem

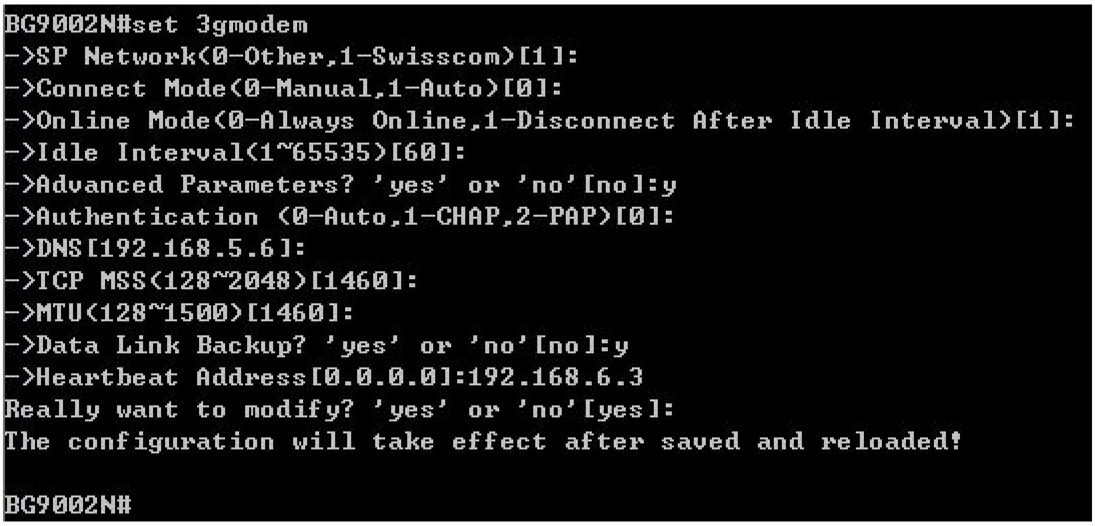
The command “show 3gmodem” show the 3G modem information as below:



```
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 5-4 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 5-5 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.

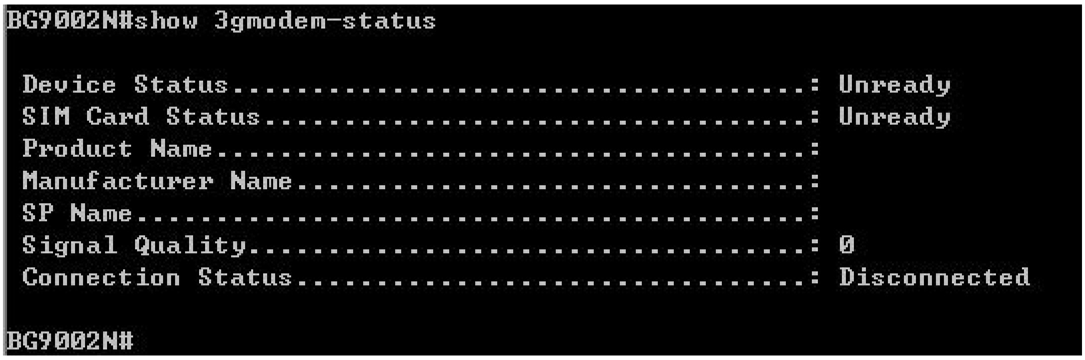
► **TCP MSS:** Configure TCP maximum segment, we recommend using the default value.

► **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 5-6 Show 3G Modem Status

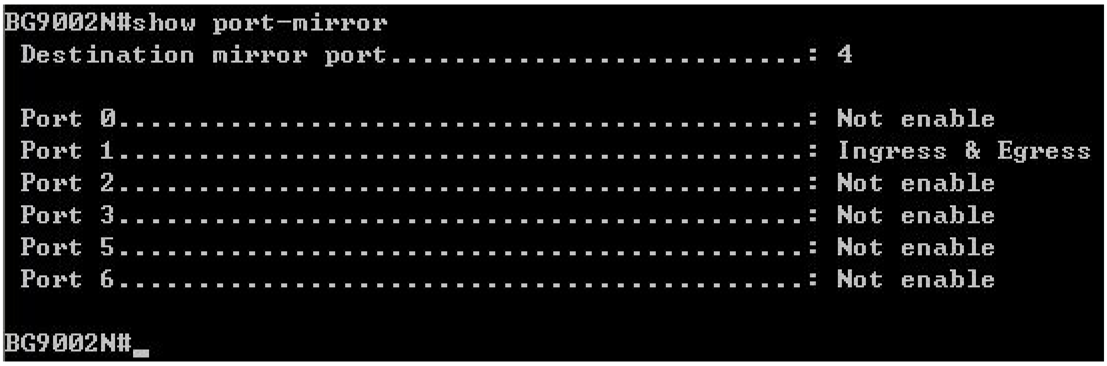
The following items are displayed on this screen:

- ▶ **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.

5.2.2 Port Management

5.2.2.1 Port Mirror

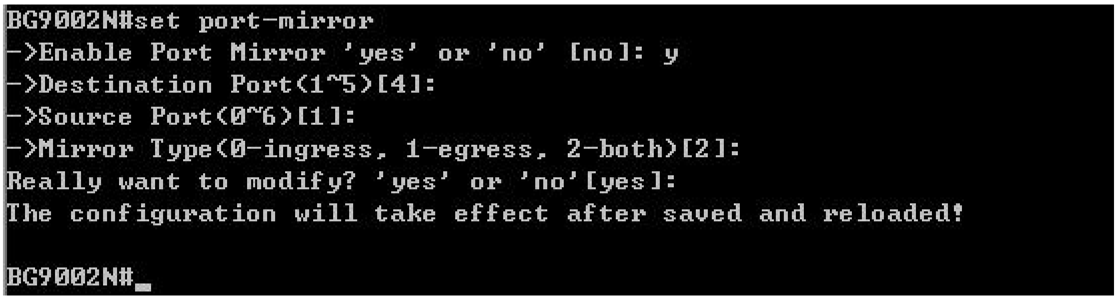
The command “show port-mirror” show the port mirror information as below:



```
BG9002N#show port-mirror
 Destination mirror port...........................: 4

 Port 0...........................................: Not enable
 Port 1...........................................: Ingress & Egress
 Port 2...........................................: Not enable
 Port 3...........................................: Not enable
 Port 5...........................................: Not enable
 Port 6...........................................: Not enable

BG9002N#_
```

Figure 5-7 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' [no]: y
->Destination Port(1~5)[4]:
->Source Port(0~6)[1]:
->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#_
```

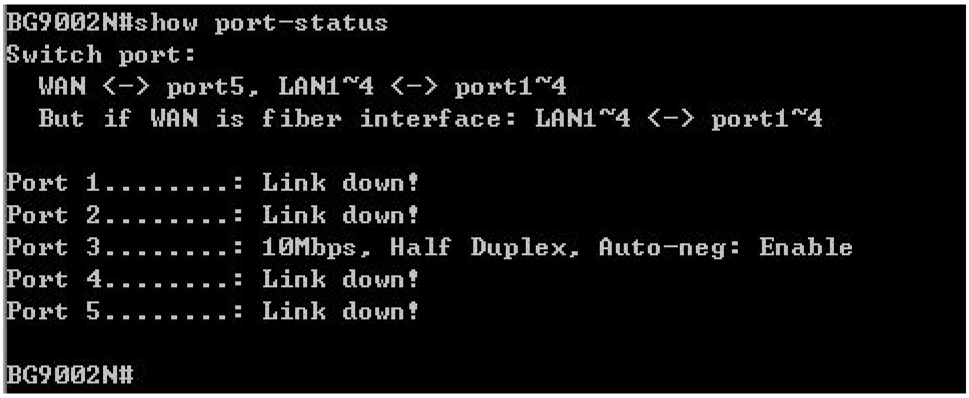
Figure 5-8 Configure Port Mirror Parameters

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**.

5.2.2.2 Media Type

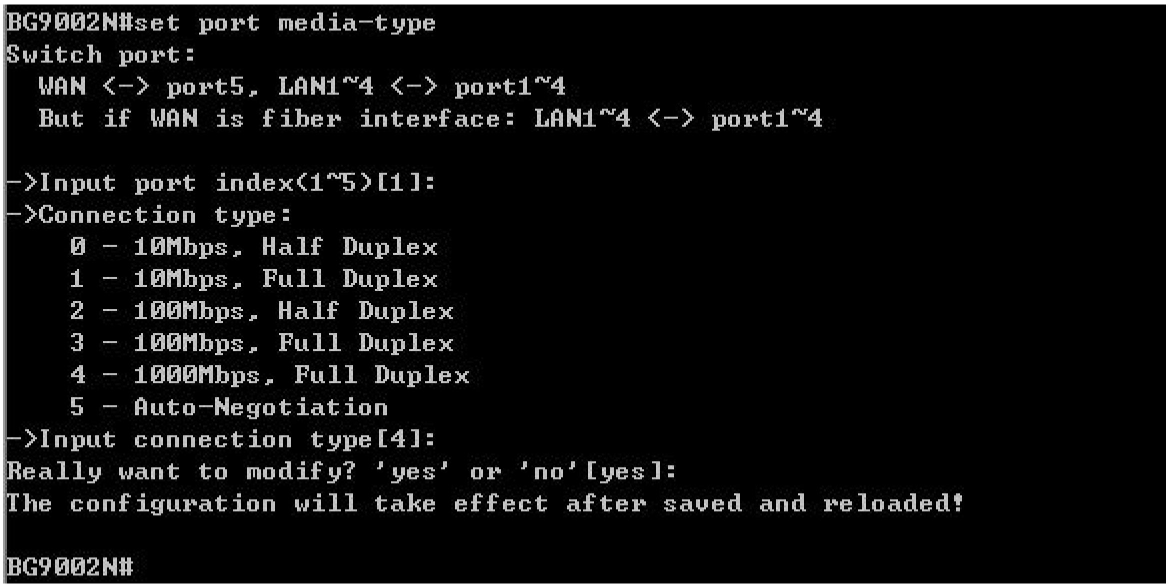
The command “show port-status” show the port status information as below:



```
BG9002N#show port-status
Switch port:
  WAN <-> port5, LAN1~4 <-> port1~4
  But if WAN is fiber interface: LAN1~4 <-> port1~4

Port 1........: Link down!
Port 2........: Link down!
Port 3........: 10Mbps, Half Duplex, Auto-neg: Enable
Port 4........: Link down!
Port 5........: Link down!

BG9002N#
```

Figure 5-9 Show Port Status Information

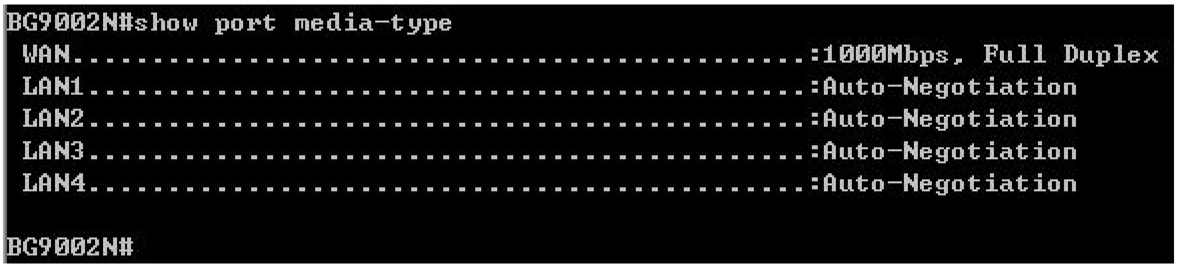
The command “show port media-type” show the port media type information as below:



```
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 5-10 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 5-11 Configure Port Media Type Parameters

The following items are displayed on this screen:

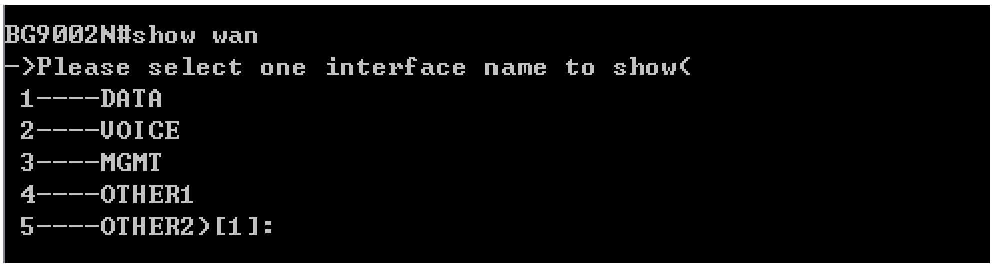
► **Media Type:** provides the following six modes to all physical ports: 10M Half Duplex, 10M Full Duplex, 100M Half Duplex, 100M Full Duplex, 1000M Full Duplex, Auto-Negotiation.

► **Current Status:** Current link status of all physical ports. Read only.

5.2.3 Wan Parameter

5.2.3.1 Show Wan Parameter

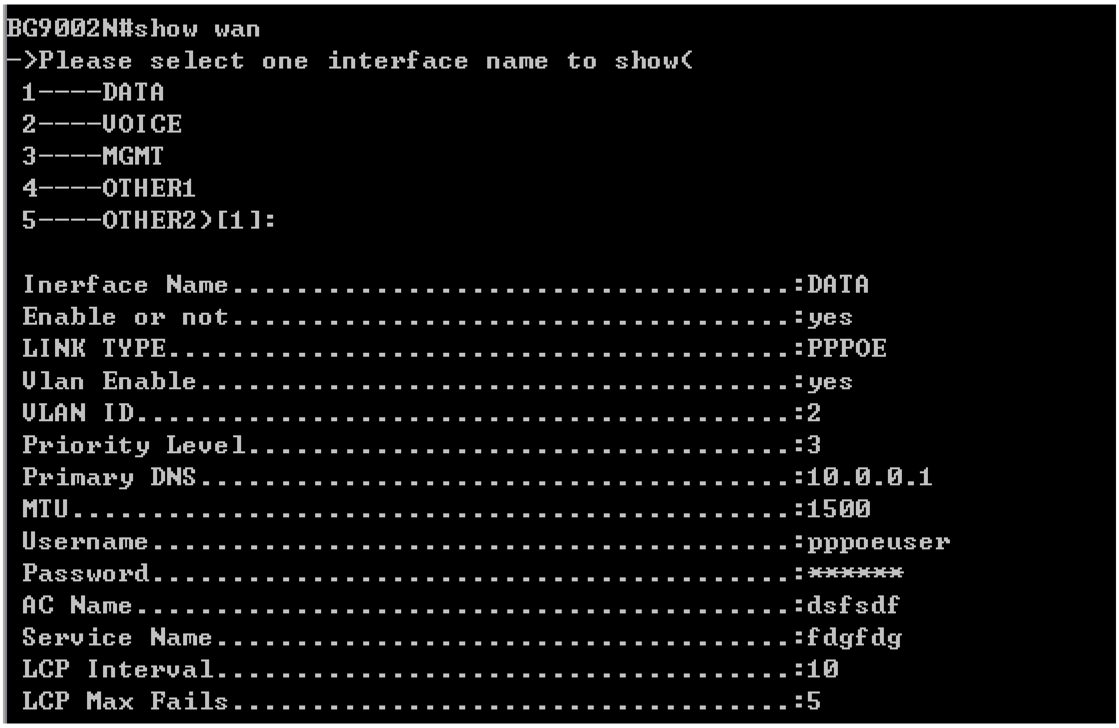
The commad “show wan” show the WAN interface configuration as below:



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

Figure 5-12 Show Wan Parameter

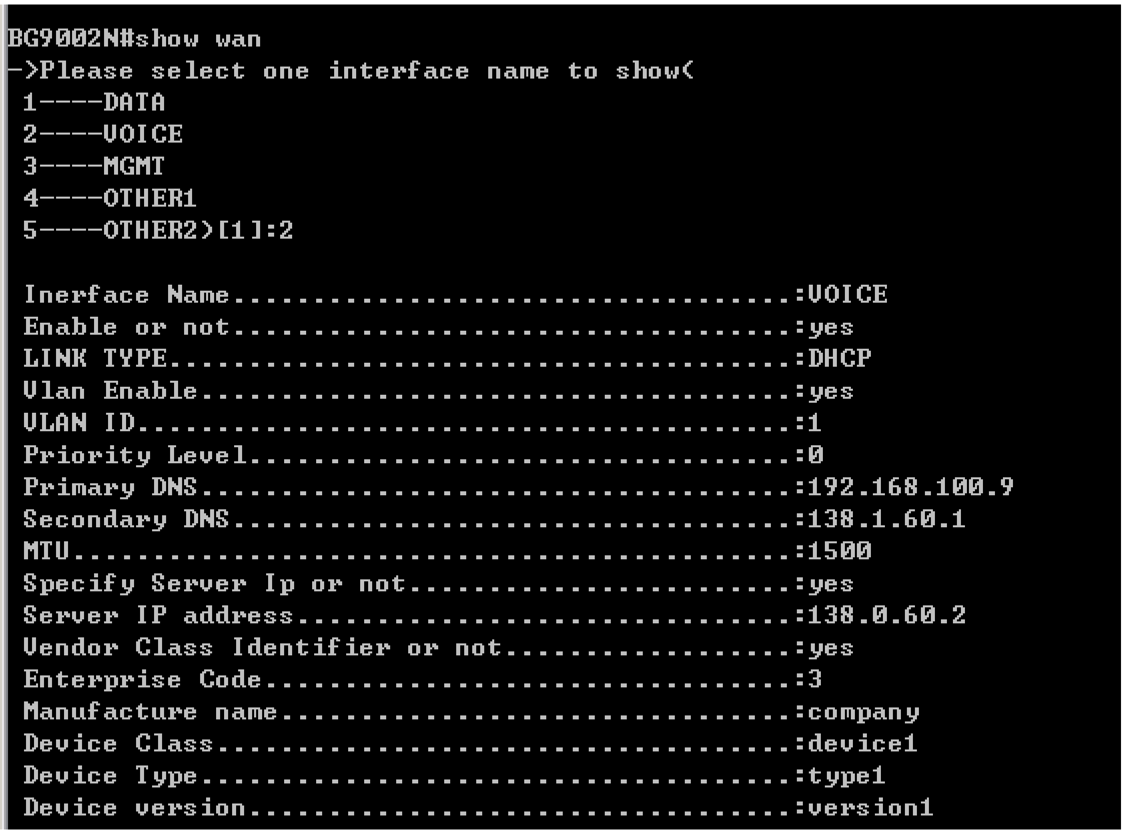
The wan interfaces include DATA、VOICE、MGMT、OTHER1 and OTHER2.
Input “1” to show DATA parameter as below:



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

 Inerface 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 5-13 Show DATA Interface Parameter

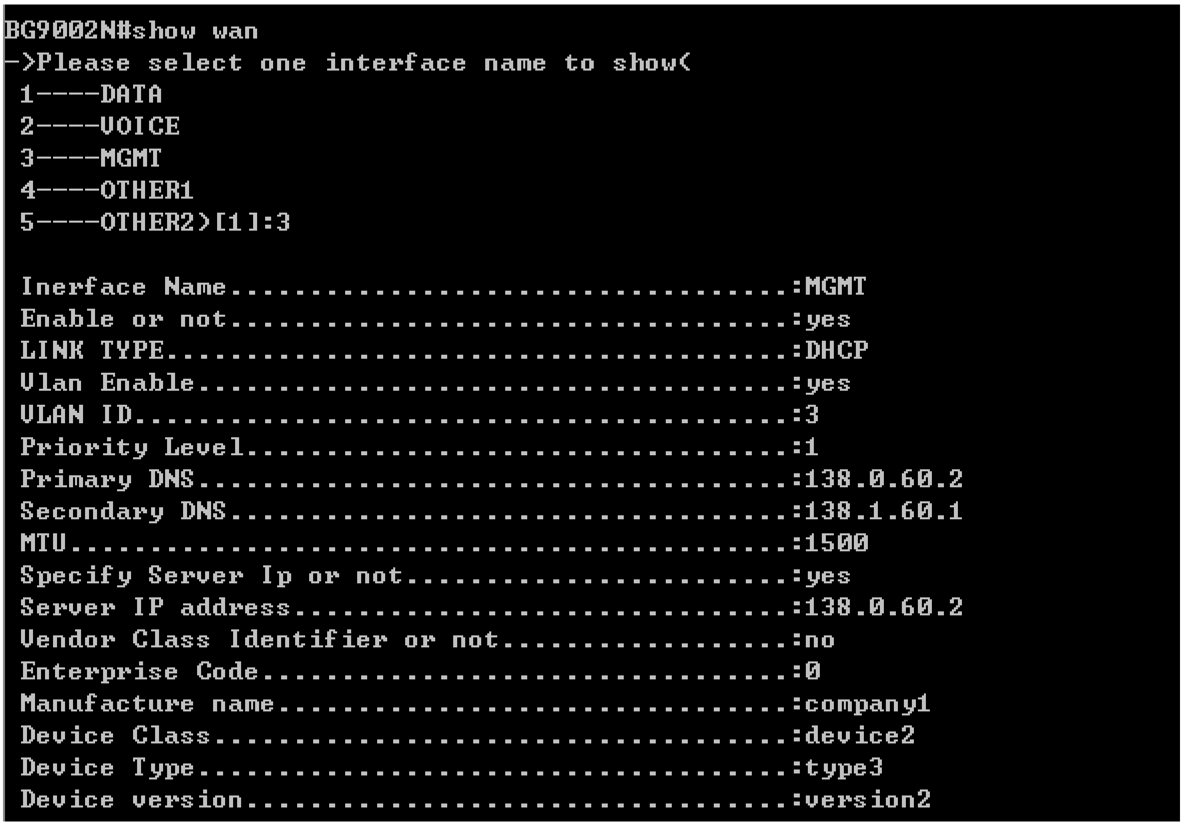
Input “2” to show VOICE parameter as below:



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

 Inerface Name...................................:VOICE
 Enable or not...................................:yes
 LINK TYPE.......................................:DHCP
 Vlan 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 5-14 Show VOICE Interface Parameter

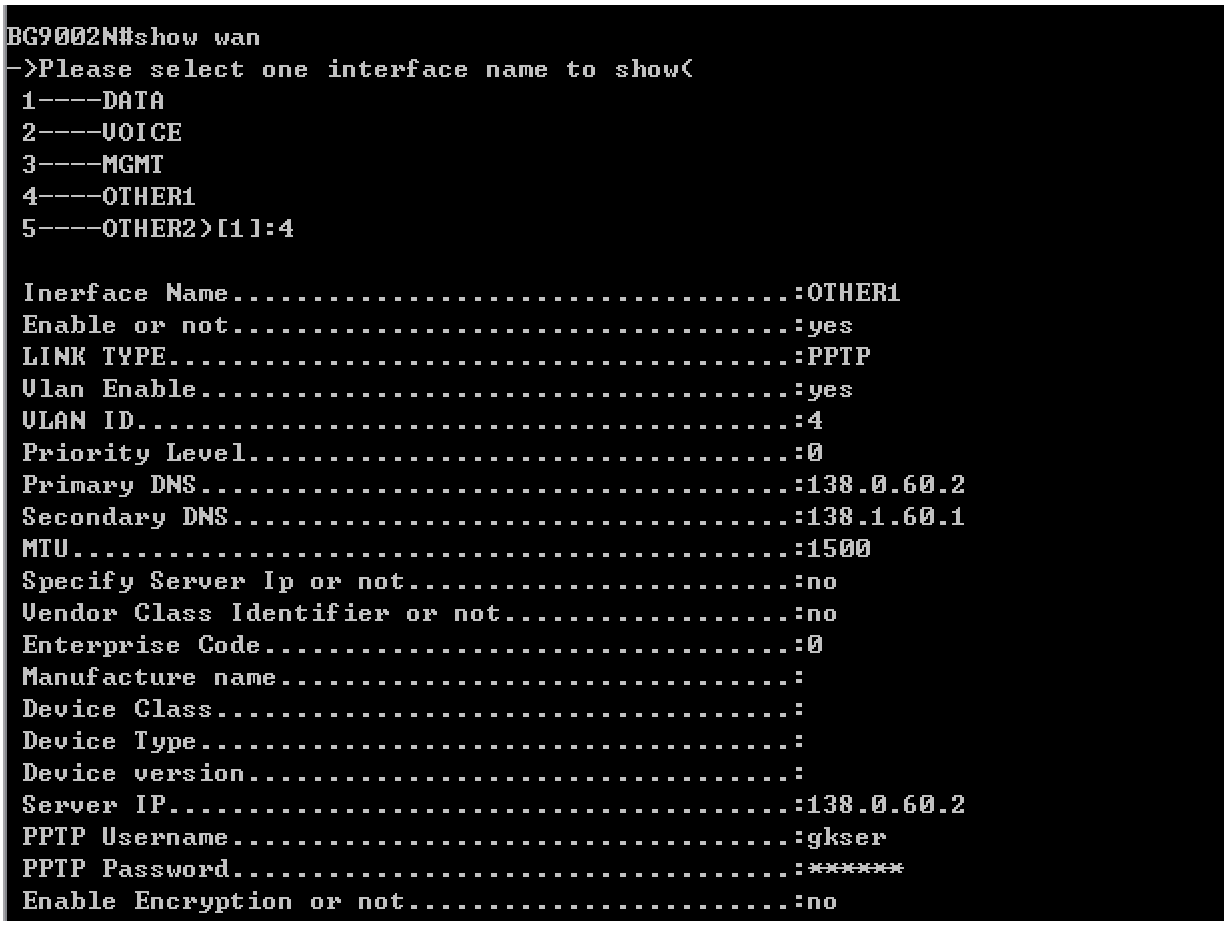
Input “3” to show MGMT parameter as below:



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

 Inerface Name...................................:MGMT
 Enable or not...................................:yes
 LINK TYPE.......................................:DHCP
 Vlan 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 5-15 Show MGMT Interface Parameter

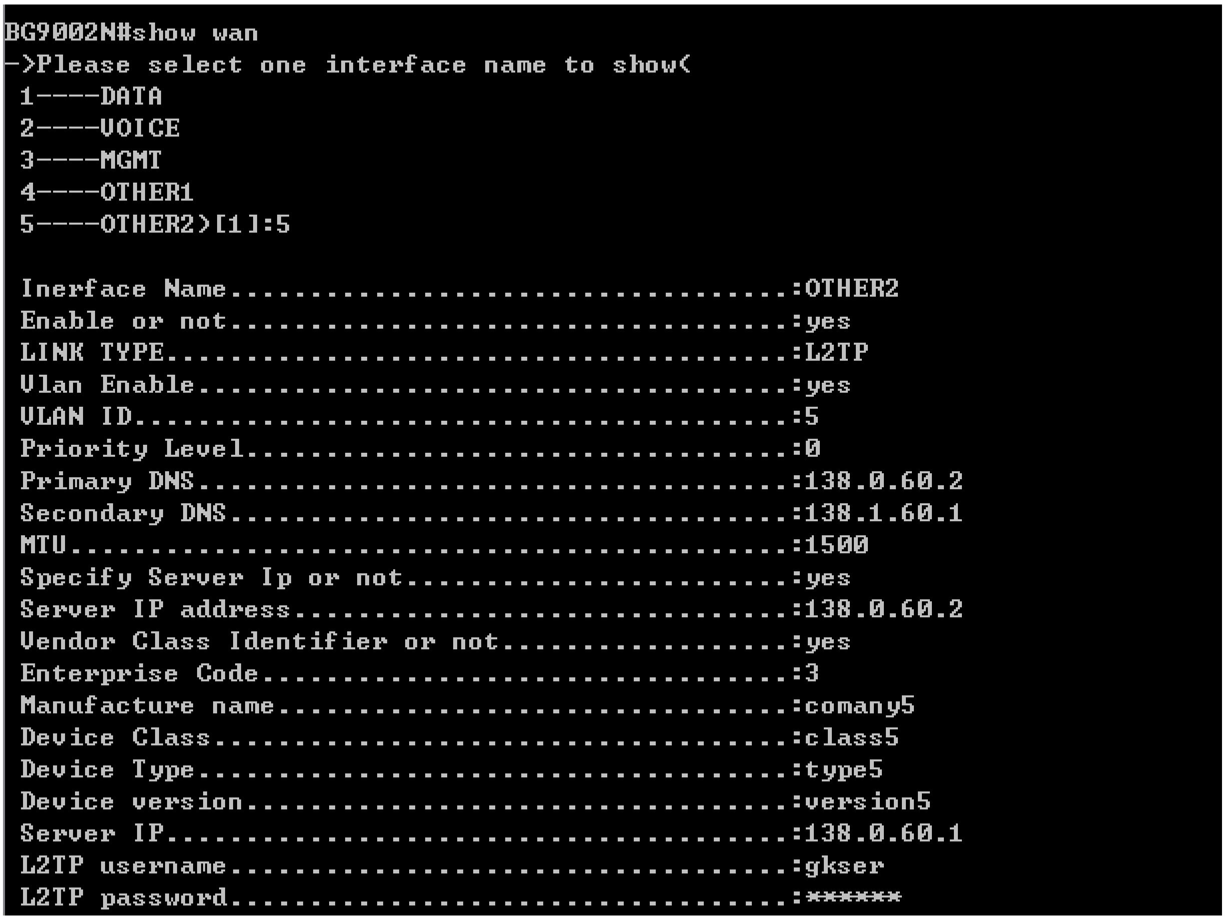
Input “4” to show OTHER1 parameter as below:



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

 Inerface 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 5-16 Show OTHER1 Interface Parameter

Input “5” to show OTHER2 parameter as below:

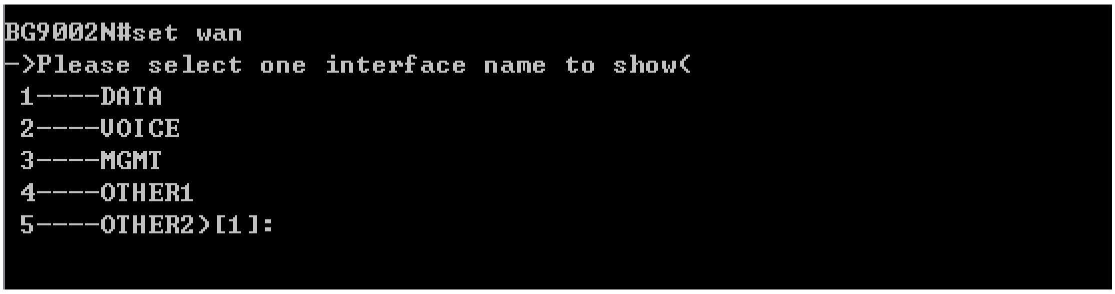


```
BG9002N#show wan
->Please select one interface name to show(
 1----DATA
 2----VOICE
 3----MGMT
 4----OTHER1
 5----OTHER2)[1]:5

 Inerface 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 5-17 Show OTHER2 Interface Parameter

5.2.3.2 Configure Wan Parameter

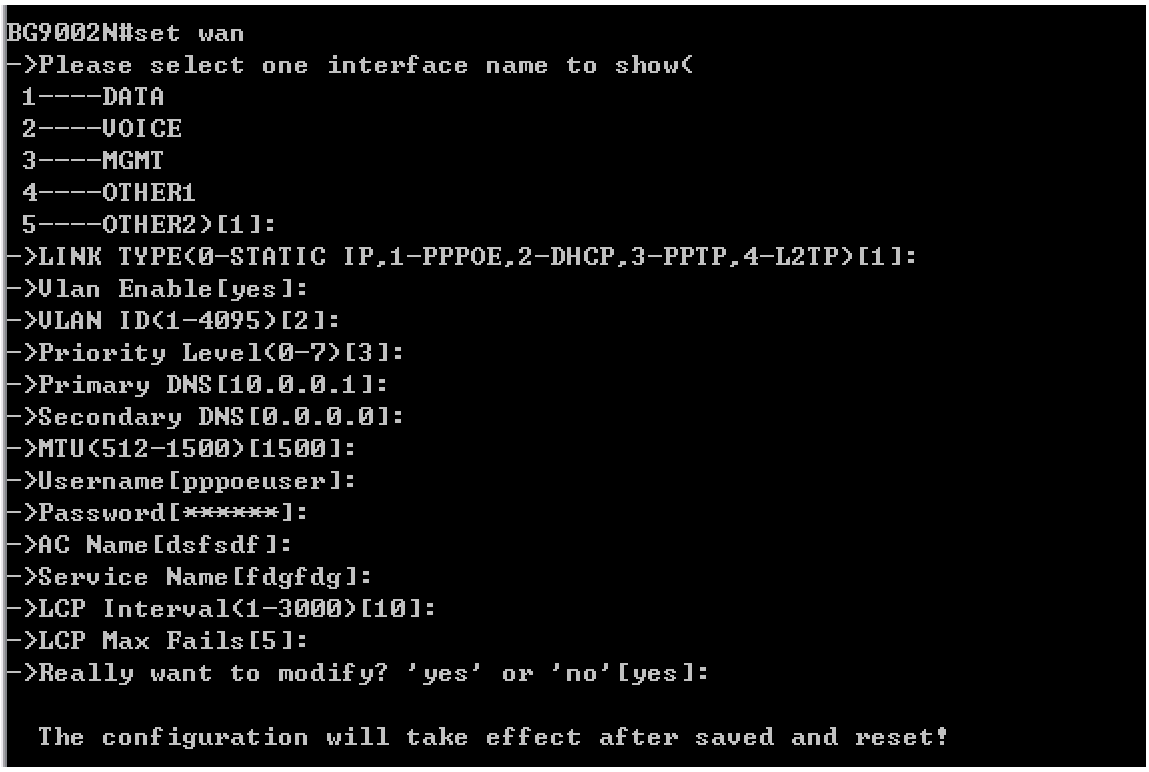
The commad “set wan” configure the wan interface parameter as below:



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

Figure 5-18 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 5-19 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: