LVswitch IAD Series Users Manual

www.lvswitches.inc

Catalogue

Dear Customer:

IAD series gateway is a powerful and excellent terminal product specially customized by ShangLu information technology ltd for customers,which provides you with a flexible, safe and complete enterprise network solution.It is simple to configure, easy to operate, flexible to use, safe and reliable,you can also get the technical support from Shanglu. In order to understand and use this product more effectively, we provide you with a user manual for this product. Please read it carefully.

This user manual contains:

1. Safety precautions
2. Main Product Functions
3. Panel and specification
4. First use and basic connection configuration
5. Configuration preparation
6. Quick setting
7. Network configuration
8. System Management
9. Log Management
10. Quick fault location

1.Product Introduction

1.1 Product Overview

LVswitch IAD product is a high-performance, multi-purpose voice access gateway designed by Shanglu information technology limited for small and medium-sized enterprises.The products support voice, security, VPN and other functions, to meet the needs of operators or virtual operators, enterprises through IP access to provide users with broadband, voice and fax services.The product can be used be IPPBX equipment to set up cross -regional IP voice exchange network to provide high effient voice communication.

The LVswitch IAD product includes a variety of interface types for connecting analog phones, fax machines, PCS, and broadband networks. The product adopts standard SIP protocol, conforms to TISPAN/IMS standard, is perfectly compatible with IPPBX, SIP server and operator IMS/NGN soft switch platform, and provides flexible and diverse access methods, which is suitable for large-scale deployment of operator projects and enterprise fusion communication. Shanglu information technology company has accumulated many years of practical experience and abundant technology in SIP protocol, voice processing and embedded system design, and its VOIP voice gateway has been adopted by operators and many enterprises all over the world.

1.2 Functions and features

- Connect analog telephone, fax machine and POS machine to IMS core network
- Cooperate with IMS business platform to support various telephone supplementary services;
- Support SIP protocol based on 3GPP and its call control
- Support H. 248 protocol voice
- Support FXS interface, physical interface type RJ11;
- Support static IP address configuration or dynamic IP address acquisition through DHCP and PPPoE;
- Support G. 711A, G. 711U, G. 729, G. 723.1, G. 722 speech codec;
- Support local WEB, remote OMC near end and remote maintenance management mode;
- Support ACL access control, ARP attack prevention, DDoS
- Support VPN functionsc such as IPsec,PPTP,L2TP etc.
- Support extensible wifi wireless.
- Support for extensible GPON、EPON Uplink.
- Compatible with Huawei/ZTE IMS, VOS, FreeSWITCH and Asterisk/Elastix business platforms.

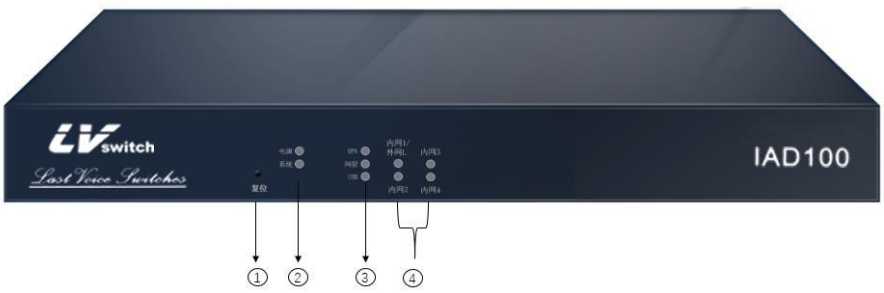
1.3 Product Seris

LVswitch IAD series product includes the following 4 kinds :

LVswitch IAD Series	Description
LVswitch-4S	4FXS Voice gateway
LVswitch-8S	8FXS Voice gateway
LVswitch-16S	16FXS Voice gateway
LVswitch-32S	32FXS Voice gateway

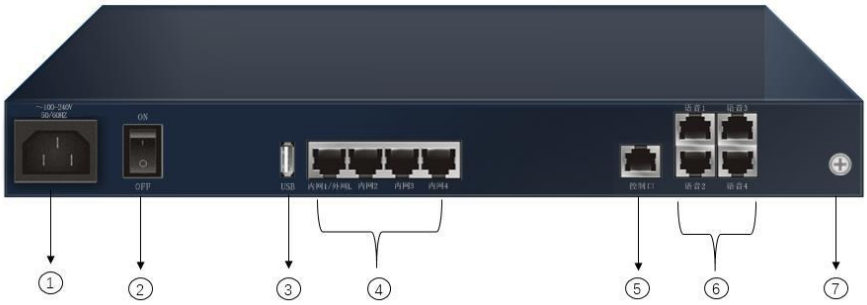
1.4 LVswitch-4S

LVswitch-4Ssupports 4 fxs interface ,the front panel is as below:



NO.	Instructions
1	Reset button
2	Power System indicator
3	VPN、NMS,USB indicator
4	4 Ethernet indicators

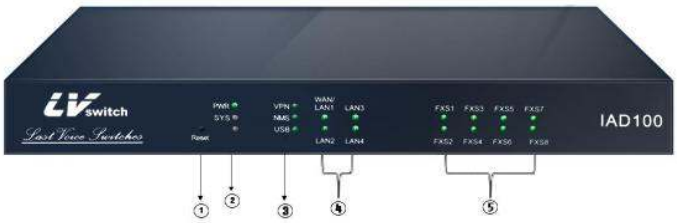
LVswitch-4SBack Panel is as following:



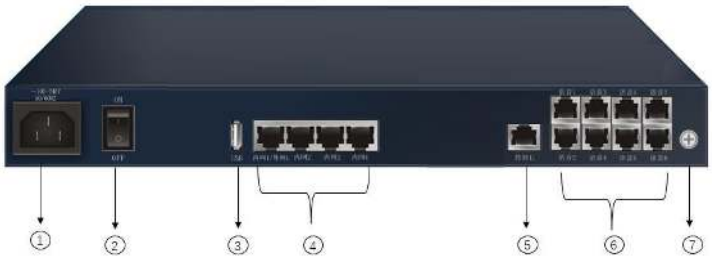
NO.	Instrutions
1	AC input
2	Power button
3	USB2.0 interface
4	10/100/1000MEthernet interface :1WAN+3LAN， RJ45
5	Console， RJ45
6	4FXS analog interface ， RJ11
7	Ground column

1.5 LVswitch-8S

LVswitch-8S support 8 fxs telephone interface,the front panel as following:



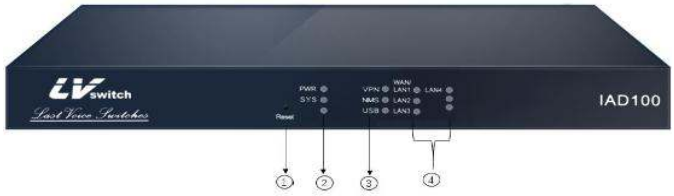
NO.	Instrutions
1	Reset indicator
2	PWR,SYS indicators
3	VPN,NMS,USB indicators
4	Ethernet indicators
5	8 FXS light indicators



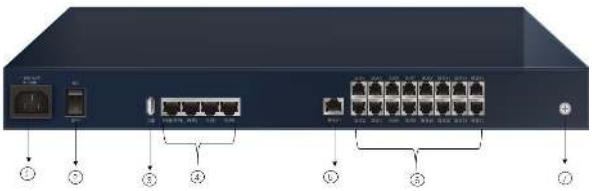
LVswitch-8S Back panel is as below ：

NO.	Instrutions
①	AC input
②	Power button
③	USB2.0 interface
4	10/100/1000MEthernet interface :1WAN+3LAN， RJ45
5	Console，RJ45
6	8 FXS analog interface ， RJ11
7	Ground column

LV switch-16S panel is as below:



NO.	Instrutions
1	RESET BUTTON
2	Power and System indicator
3	VPN、network management ,USB indicator
4	4 Ethernet indicators



NO.	Instrutions
1	AC input
2	Power button
3	USB2.0 interface
4	10/100/1000MEthernet interface :1WAN+3LAN，RJ45

5	Console，RJ45
6	16 FXS analog interface ，RJ11
7	Ground column

LVswitch-32S

LVswitch-32Ssupports 32 voice interface，The front panel as belows:

NO.	Instrutions
1	RESET BUTTON
2	Power and System indicator
3	VPN、network management ,USB indicator
4	Ethernet indicator

LVswitch-32S Back panel is as below ：

NO.	Instrutions
1	AC input
2	Power button
3	USB2.0 interface
4	10/100/1000MEthernet interface :1WAN+3LAN，RJ45
5	Console，RJ45
6	32 FXS analog interface ，RJ11
7	Ground column

1.5 Product specifications:

1.5.1 Hardware specifications:

Item	Description
Network interface	1 WAN,3LAN,RJ45 port,rate10/100/1000M
FXS interface	LVswitch-4S：4*RJ11 LVswitch-8S：8*RJ11 LVswitch-16S：16 *RJ11 LVswitch-32S：32 *RJ11
Console	1 *RJ45，115200bps
USB interface	1*USB2.0,fullspeed
Working power	100VAC～240VAC；50/60Hz
Case	1U,metal material

Power	LVswitch-4S ≤20W LVswitch-8S： ≤25W LVswitch-16S： ≤35W LVswitch-32S： ≤45W
Weight	LVswitch-4S： ≤1.6KG LVswitch-8S： ≤1.8KG LVswitch-16S： ≤2.0KG LVswitch-32S： ≤2.2KG
Working environment requirements	Operating environment temperature -5℃～55℃ Ambient relative humidity 95% (non-condensation) No performance degradation within 3000m above sea level Atmospheric pressure 86KPa~106KPa The concentration of particles in the air≤180mg/m3

1.5.2 Software specifications

Item	Sub-item	Description
Voice Function	Voice Protocol	IMS/NGN SIP、H.248
		SIP v2.0、RFC3261、SDP、RTP(RFC2833) 、RFC3262、3263、 3264、3265、3515、2976、3311、RTP/RTCP、RFC2198、 1889、RFC4028 Session Timer、RFC3266 IPv6 in SDP、 RFC2806 TEL URI、RFC3581、NAT、Rport
		Master/standby SIP server External proxy server
	Voice Processing	Speech codec：G.711A、G.711U、G.729、G.723.1、G.722
		Echo cancellation：G.168，tail length is 64

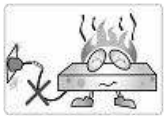
		milliseconds long
		Comfortable background sound, silent compression (VAD)
		Supports signaling and media DSCP/TOS tagging
		Digitmap
	DTMF	RFC2833、SIP INFO、INband
	FXS call	RJ11 interface，Support sending reverse polarity，DTMF dialing，FSK caller ID
	SIP users	SUPPORT up to 32 SIP extensions
	SIP server	none
	Fax	T.30 pass through、T.38
	Voice bussiness	Basic calling, caller ID,Call waiting,call on hold,call transfer,3-way calling With implementation withIPPBX/IMS：Caller id display limit，Forward unconditonal，Forward on busy，Forward on answer，Find malicious calls，Call barring，DND，Abbreviated dialing，hotline service，Alarm ，Call back on busy，Conference call
Data function	Uplink IP access	Support static IP, DHCP Client, PPPoE, WAN subinterfaces
	Uplink interface mode	Support routing mode,bridge mode
	IP service	DDNS、Static route、NAT、Port mapping、uPnP、Virtual domain name、ALG、 DNS、NTP、DHCP service
	Traffic management	QoS strategy、Broadband strategy
Safety Management	WAN port access control	WEB access、Ban Ping、SSH protocol、SIP protocol
	IP address black and white list	IP address black and white list
	ARP attack prevention	IP/MAC binding、ARP attack prevention
	DDoS protection	Ping of Death、Tear drop、TCP Flood、UDP Flood、Traceroute、IP Spoofing、Port Scan、WINNUKE Attack
	VPN	IPsec、L2TP、PPTP
System Management and Maintenance	Local management	Web mode、SSH2
	Remote management	SNMP、TR069
	System debugging	Ping、Traceroute、Ifconfig、Route、HttpGet、DNS Query
	Log management	Log query、log settings

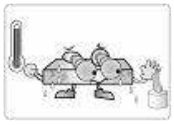
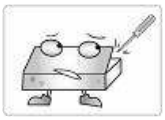
	System maintenance	SUpport configuration backup&recover、Support software upgrade、Support factory default reset、Time setting

2.Preparation before installation

2.1 Safety precautions

During the installation and use of the equipment, please pay attention to the following safety precautions.

	In case of thunderstorm,please stop using the equipment, disconnect the power supply and unplug the power cord and telephone line to avoid the equipment being damaged by lightning.		Please place the equipment on a stable working table and place it in a ventilated environment without direct sunlight.
	The equipment must be kept strictly dry during storage, transportation and use. In case of accidental liquid flow into the case, please immediately disconnect the power supply and contact the designated service point.		Please use the power source adaptor and other accessories with the equipment. Please keep the plug clean and dry to avoid electric shock or other hazards. Do not use damaged or aged power cords.
	Do not allow children to use the equipment without supervision; Do not allow children to play with equipment and swallowing.		If there are abnormal phenomena, such as smoke, abnormal sound, peculiar smell, etc., please immediately stop using and disconnect

			the power
	When installing the equipment, please leave a heat dissipation space above 10cm around and on the top, and keep away from heat sources or exposed fire sources, such as electric heaters and candles.		Do not place any object on the device or on the power cord or plug. Please do not cover the vents of the cabinet with objects
	Before cleaning, please stop using the equipment and cut off the power supply. To clean, use a soft, dry cloth to wipe down the equipment enclosure.		Do not disassemble the equipment by yourself. In case of equipment failure, please contact the designated maintenance point.
If the equipment is used for a long time, the shell will have a certain degree of heat. Please do not worry, this is a normal phenomenon, the equipment can still work normally.			

2.2 Basic connection configuration

2.2.1 System application environment

This product is a set of routers, switches, IAD voice access gateway altogether functional equipment, to provide enterprises with integrated office access.

The system application environment is shown in figure 2-1.

Figure 2.1 Application environment

2.2.2 First time use and basic connection and configuration

When for the first use, the product must be installed by the engineer. If you (enterprise network administrator or responsible person) need to adjust the equipment during the use, please refer to the following instructions.

2.2.3 1 Set up wire connection

Please connect to this product following the instruction below.

2.2.3.1 Connect the uplink Ethernet interface

Connect the uplink Ethernet interface (WAN/ LAN port 1) and the operator's access information point with network cable. (work in Ethernet mode)

Figure 2-2 connects to uplink Ethernet (WAN)

2.2.3.2 Connect the LAN port

Connect the Lan ports(LAN 2-4) of the equipment with the network adapter of the user’s computer or other network equipment with network cable.

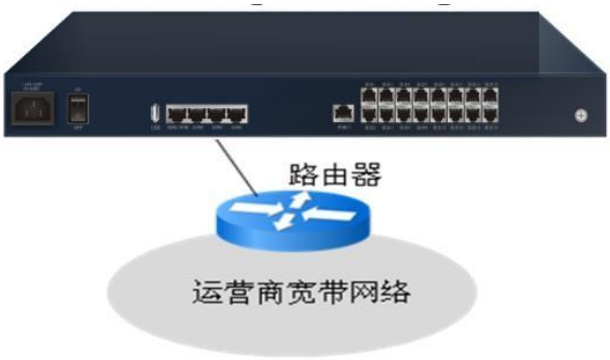


Figure 2-3 connect to LAN

2.2.3.3 Connects to telephone

Connect the analog FXS port and analog telephone with the telephone line with RJ-11 interface.

2.3.3.4 Connects to the power adaptor

Connect one end of the power adapter to the power interface of the product, and then insert the power cord plug into the power socket.

Input ac power supply range: 100V a.c. ~ 240V a.c. 50/60 hz

2.2.4 2 Turn on the power

After the connection completed ,turn on the power switch on the rear panel.

2.2.5 3 Check the electricity

After the installation and connection is completed, open the product. At this time, you can judge whether the product works normally by checking the status of indicator light. Please refer to "error! The reference source was not found.

2.3 Preparation configuration

This chapter will take you login and familiarize you with the Web setup page, using the basic functions of the product. This chapter takes the example of your computer using the Windows XP operating system, Internet Explorer browser. For other operating systems and browsers, please see their instructions and refer to this chapter's content configuration.

2.3.1 Preparation before configuration

Please confirm that the browser of the user's computer does not use the proxy server. The specific steps are as follows:

(1)Launch the browser, select" Internet" options in the tools menu bar, and then click the" connection "TAB to enter the Internet connection page as shown in figure 2-4.

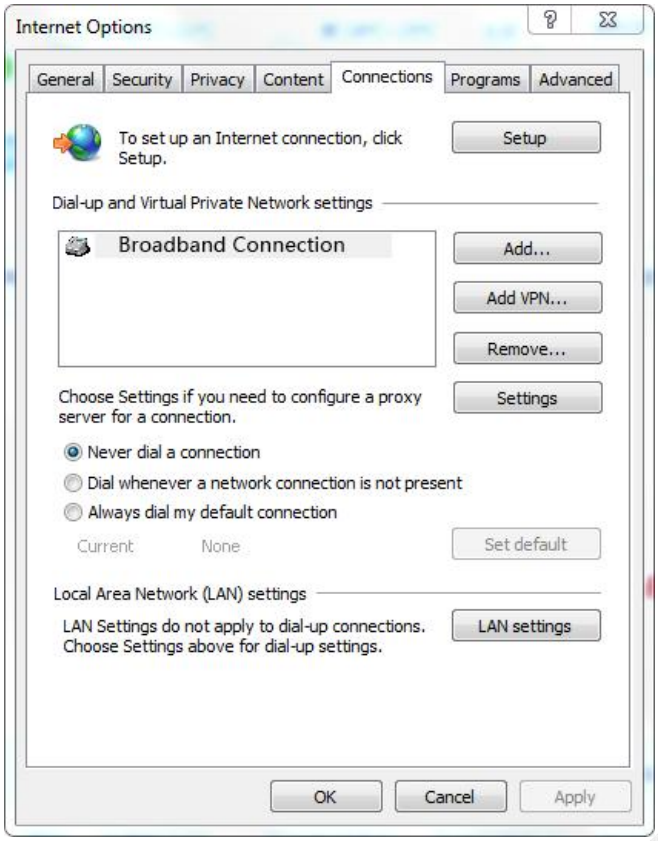


Figure 2-4 Internet connection

(2) On the Internet connection page, click LAN Settings, as shown in figure 2-5. Make sure that the radio box before "LAN USES proxy server" is not checked.

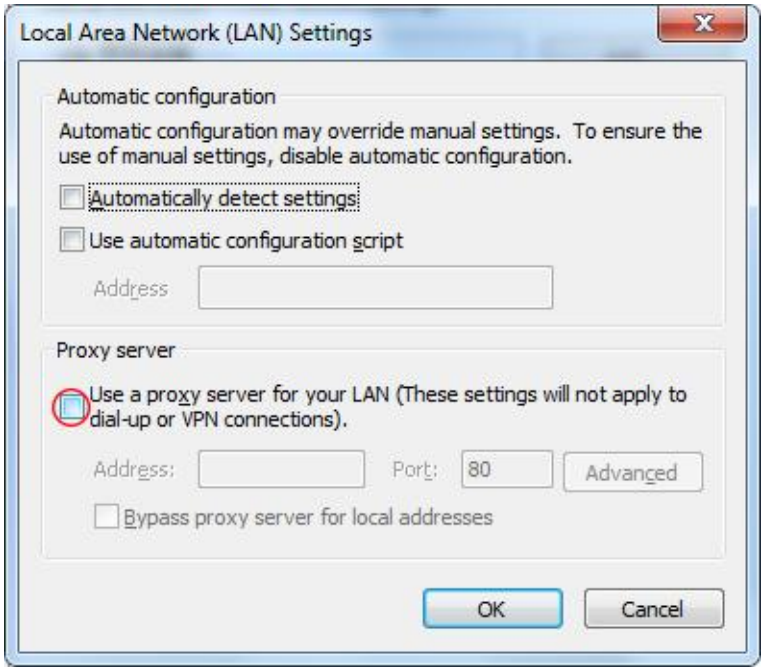


Figure 2-5 Set Proxy Server

Set the IP address of the user's computer

Before accessing configuration page, it is recommended to set the computer to "automatically obtain IP

address" and "automatically obtain DNS server address", and the IP address will be assigned by this product. If you need to specify a static IP address for your computer, you need to set the computer's IP address and the product's LAN port IP address in the same network segment (the device LAN)

The port default IP address is 192.168.200.1; The subnet mask is 255.255.255.0; The default gateway is 192.168.1.1.

(1) Select Internet protocol in the local connection properties window

(2) Then click the properties button and the Internet protocol (TCP/IP) properties pop up, as shown in figure 2-6

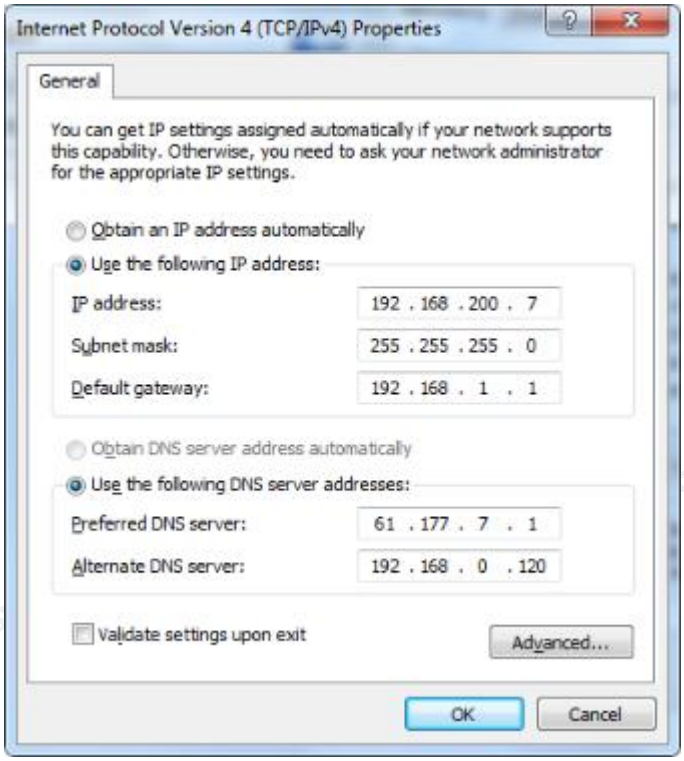


Figure 2-6 Internet protocol (TCP/IP) properties

(3) Set static IP address (optional)

In the Internet protocol (TCP/IP) properties dialog box, click use the following IP address to specify that the native IP address is in the same network segment as the device's LAN port address, that is For example, the IP address is 192.168.200.7, the subnet mask is 255.255.255.0, and the default gateway is set to 192.168.200.1.

(4) Automatic access to IP address (optional)

In the Internet protocol (TCP/IP) properties dialog box, click getting IP address automatically and get DNS server address automatically.

(5) click the ok button to confirm and save your Settings

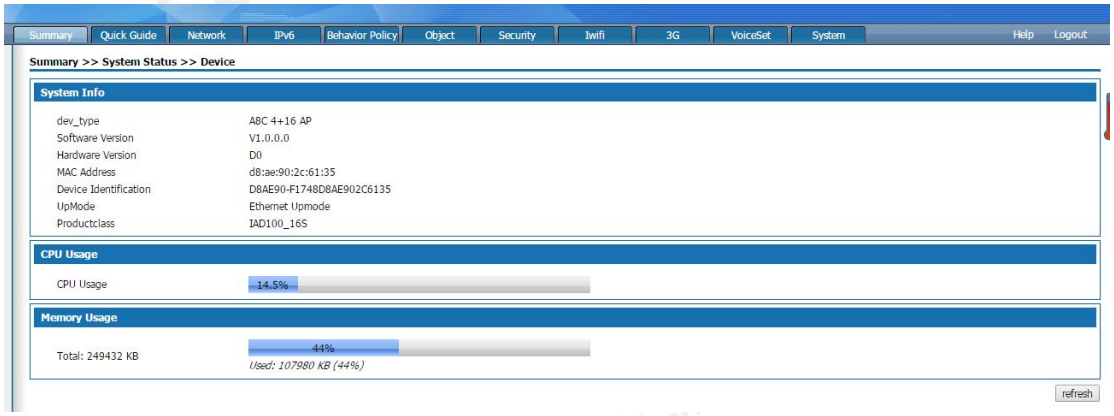
These Settings can be modified depending on the user's network requirements, but on first access to the device refer to the above configuration for your WEB configuration page.

Enter the configuration interface, the specific steps are as follows:

(1) Enter "http://192.168.200.1" in the address bar of the browser (192.168.200.1 is the default login IP address of the product), press enter, and the login window will pop up as shown in figure 2-7:

2-7 Log in page

(2) Choose the language English, Enter a user name and password in the login window and click the < login > button. After password verification, you can enter the configuration page of the product, as shown in figure 2-8: The default USER NAME is admin,and the default password is “admin” too.



2-8 Web Setting Page

You can see the function module on the top of the product configuration page, the navigation bar is on the left and the setting area on the right.

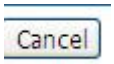
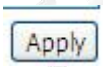
To exit the configuration interface, click < logout > on the far right of the navigation bar to exit the Web Settings page.

NOTE The timeout for the Web setup page is 5 minutes, and if no page Operation done within 5 minutes,it needs re-enter the user name and password validation.

If you close the browser without clicking logout, you exit after the timeout period,and no one can log in the equipment during.

2.3.2 Operation button description of the Web setting page

In the following chapters 6-11, we will introduce how to operate this product in detail. The main buttons of the product are described as follows.

Terms	Description
	After modifying the configuration information, click the < save > button to save the configuration information to the operation background.
	When you have finished clicking the save button, click the cancel > button to cancel the configuration information saved to the background of the operation.
	After clicking < save > button, confirm that the configuration information is correct, and click < apply > button to make the configuration information take effect.
	After adding a policy or modifying a policy, if you do not click the < Apply > button, the reminder that the configuration has not been applied will be displayed on the page. After clicking  , all the configuration information modified will take effect.

3.Device Summary

Summary includes system status and info statistic.

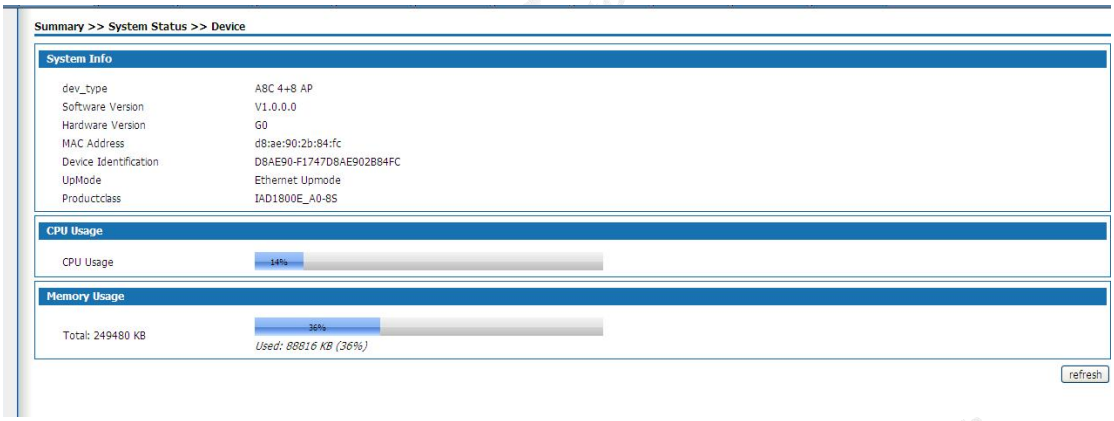
Before configuration, click "Summary " at the top of the page to enter the device overview page.

3.1 System status

System status includes Device, interface,WIFI,3G and Voice status.

3.1.1 Device

Select"Summary" and "system status" and "device" and enter in the device page as shown in picture 3-1.

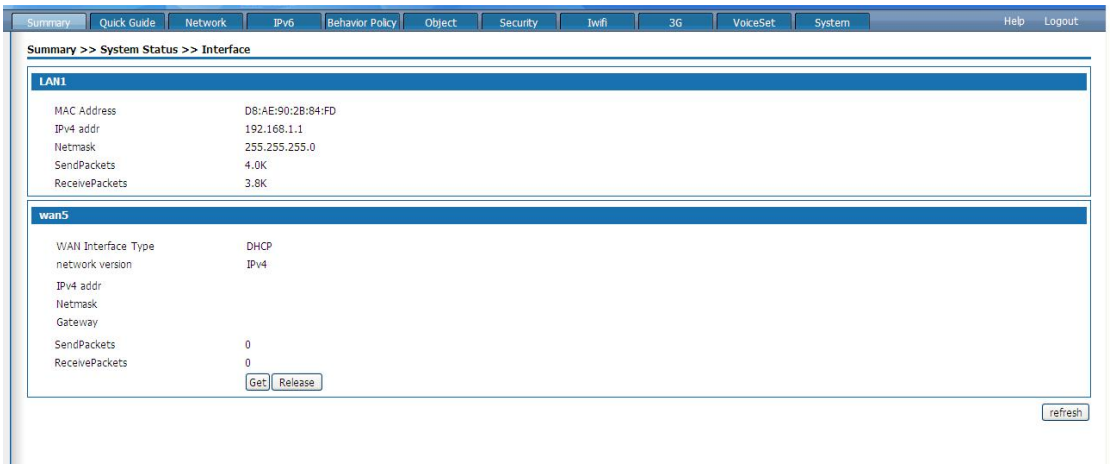


3-1 Device

The summary shows basic system information, CPU utilization, and memory usage. Click the < refresh > button to display the CPU and memory usage at the current time.

3.1.2 Interface Status

Select<Summary ><System status> and select <INTERFACE > entering the page as following



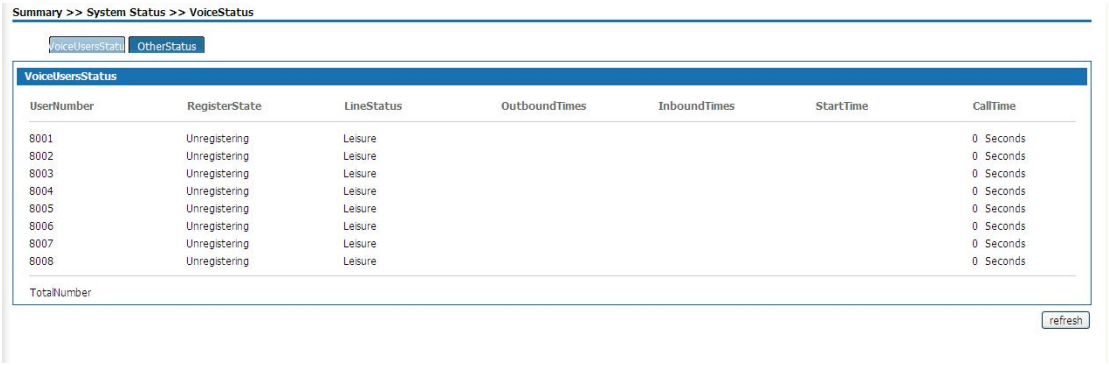
3-2 Interface status

The interface state shows the MAC address, IP address and subnet mask of the LAN port, the number of packets sent and received, the connection mode of the WAN port, the protocol type, IP address, subnet mask, gateway, and

the number of packets sent and received. Manual connect and disconnect buttons are provided for PPPOE dial-up lines. Click the < refresh > button to display interface information for the current time.

3.1.3 Voice status

Select"system status" then "voice status",you can see the current status of the voice users.



3-3 VOICE STATUS

3.2 Info Statistics

Info statistics includes DHCP client,interface, online user and ConnetNum.

3.2.1 DHCP client

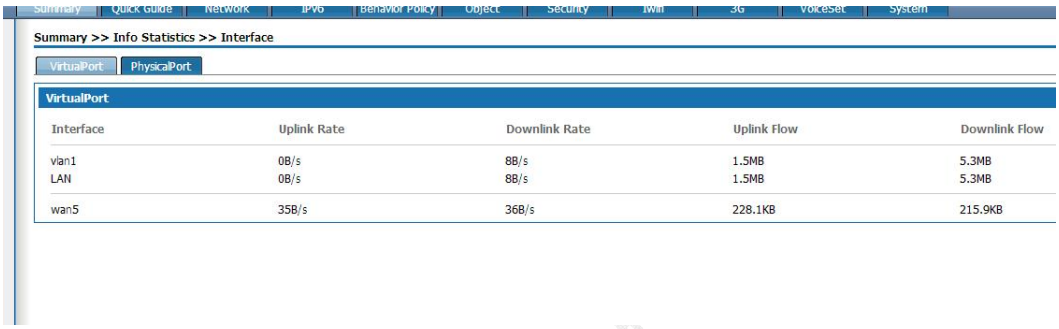
Select "Info statistics" >"DHCP client" ,the DHCP CLIENT page as following

3-4 DHCP client

DHCP status shows the user information of IP address obtained through the DHCP service of this product, including user name, user IP address and MAC address.

3.2.2 Interface

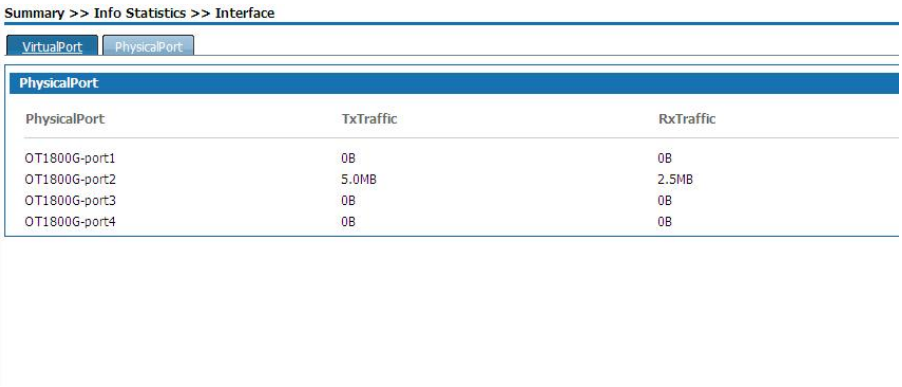
Select <Info Statistics> ><Interface> the interface page as following:



3-5 Virtual interface statistics

The virtual interface statistics show the upstream and downstream rates and traffic of the VLAN port and WAN sub-interfaces that have been enabled. If the WAN sub-interfaces are not enabled, the upstream and downstream rates and traffic of the WAN port will be displayed. Click the < refresh > button to display the virtual interface information for the current time.

Click on the < physical port > to bring up the page shown in figure 3-6.



3-6 Physical ports

Physical port statistics show the sending traffic, receiving traffic and connection status of the four physical ports of the device. Click the < Refresh > button to display the physical port information for the current time.

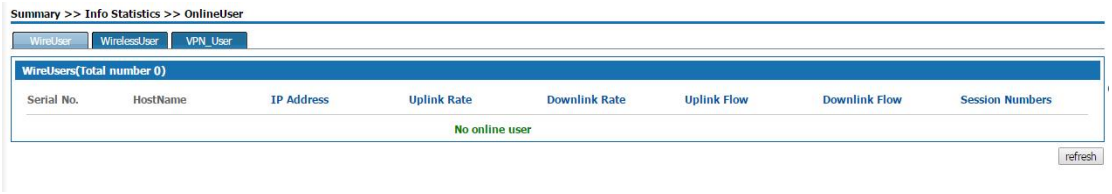
3.2.3 ON LINE USERS

Select<Summary> <INFO statistics > <online user statistics> and enter the <wired user statistics>page as shown in figure 3-7

3-7 Wireuser Statistics

The statistics of wired users can visually see the host name, IP address, upstream and downstream speed, upstream and downstream traffic, and the number of connection sessions of all wired users. Click the < Refresh > button to display the wired user information for the current time.

Click<wireless user> can shows the page as below



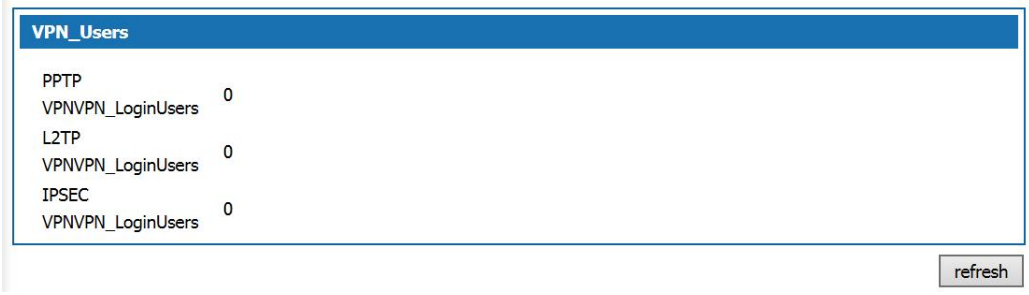
Wireless user statistics can visually see all wireless user host name, IP address, uplink and downlink speed, uplink and downlink traffic, connection session numbers. Click < Refresh > Button to display the wireless user information of the current time.

Figure3-8 Wireless user statistics

Click <VPN User >,the page as shown in Figure 3-9 is displayed.

In VPN User page, the number of the users who log in via PPTP VPN, L2TP VPN, and IPSEC VPN is displayed.

Click <Refresh> to display the information on number of VPN users logged in at the curLease Time.



3-9 VPN user statistics

4.Network configuration

The network setup module provides the basic configuration of this product, including WAN port setup, LAN port setup, and DHCP setup.

Before configuration, please click <Network> at the top of the page to enter the network configuration page.

4.1 Basic Setup

Basic Setup includes LAN Setup, Uplink mode settings,WAN Setup, DHCP setup.

4.1.1 Uplink mode setup

Select<Network> and <Basic Setup> then <Upmode>, and the <Upmode>page pops up as the following as figure4-1.

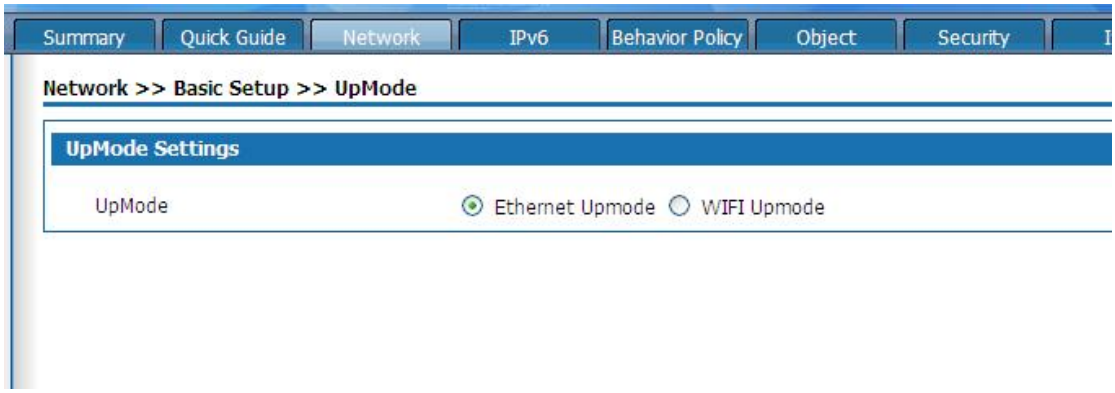


Figure 4-1 Uplink mode setting

Under ethernet upmode,the Wan port of the device serves as the uplink Ethernet interface, which supports the hybrid mode of TAG and UNTAG under the sub-interface mode.

4.1.2 LAN SETUP

Select “Network” and select<Basic Setup> and <Lan Setup>, the Lan settings page will display as follows:
Configure the IP address and subnet mask of the LAN port. The system has a default IP address of 192.168.200.1 and a subnet mask of 255.255.255.0.

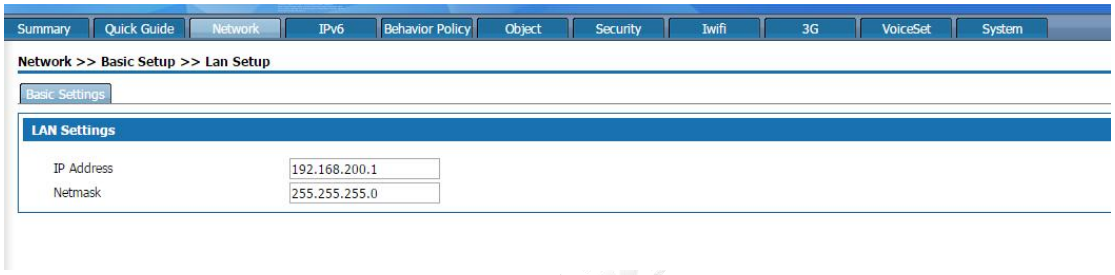


Figure 4-2 Lan Setup

After modifying the LAN port IP, you need to log in to the new device address to continue the configuration;

4.1.3 WAN setting

Select<Basic setup> and <Wan setup> and click the <Basic settings> tab, the WAN port setting page pops up as below:

4-3 basic settings of WAN mode

Wan port operation mode

Single WAN: work under <Ethernet uplink mode > or<WIFI uplink mode>

Single WAN(3G):Optional when using 3G connection network

Dual WAN(3G): Optional when using both Ethernet uplink and 3G networks or WIFI uplink and 3G networks

WAN interface mode: gateway: this product is used as an enterprise network exit routing device. It is generally deployed in the internal network exit of the enterprise. It assumes the internal user gateway of the enterprise internally and connects to the operator network externally through various links.

Bridge: this product is used as a bridge with filtering function. It is generally used when the enterprise already has the gateway equipment for Internet access. It can connect the equipment between the gateway and the Intranet to monitor and limit the staff's Internet traffic. Bridging mode allows easy access to the user network without changing the user network configuration. In bridge mode, the connection type defaults to a static address, which sets the Intranet address assigned to the device and allows the administrator to manage the device. The 3G interface does not support bridging mode.

The administrator's computer address and the management address set in bridge mode are required to be in the same network segment to manage the equipment.

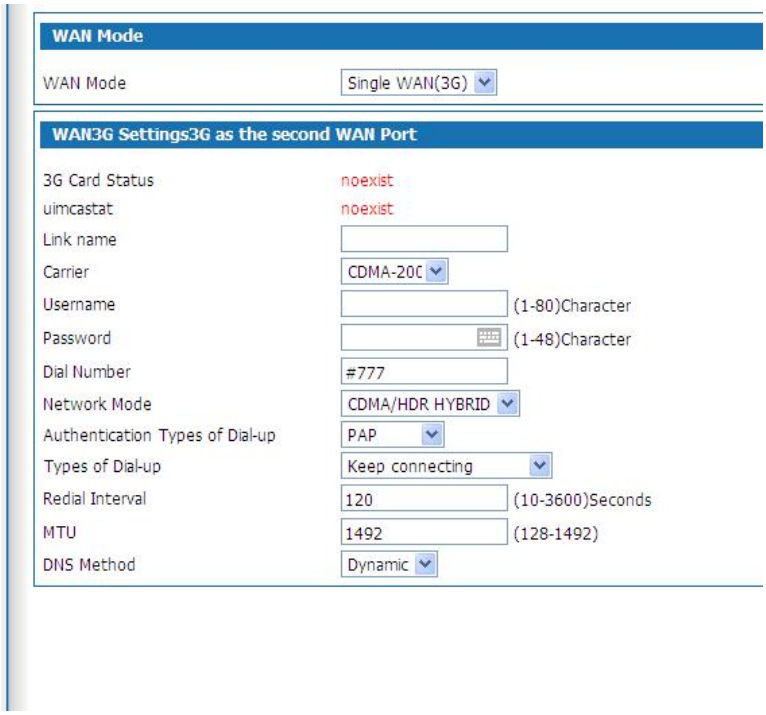
In bridge mode, the bridge contains a WAN port .Vlan can be bound via LAN/WAN

to join in the bridge, the added VLAN network segment for Internet access and flow control.

In the routing Settings, NAT Settings, port mapping, and IPsec policy Settings sections, the WAN interface of bridging mode will be masked.

3G card connection Settings:

Select single WAN(3G) or double WAN(3G) mode and the page as shown in figure 4-7 pops up.



4-4 3G card connection Settings

The setting of 3G card connection is as follows:

Interface Items	Instruction
3G Card Status	If 3G card connection is successful,it will display"exist",if no 3G card connection,it will display"noexist"
Uimcastat	If there is UIM card,it will display"exist"if no it will display"noexist"
Link name	Operator for 3G card
Username	Username for the 3G CARD,provided by ISP
Password	Password for 3G CARD,provided by ISP
Carrier	CDMA-2000 WCDMA TD-SCDMA Default CDMA-2000
Dial number	Provided for ISP
Network Mode	CDMA mode: refers to CDMA-1x mode, under which the maximum downlink rate is 153.6 KBPS. HDR mode: refers to 3G mode, under which the maximum downlink rate is 3.1Mbps CDMA/HDR HYBRID mode: it is compatible with CDMA and HDR. On which mode to choose, please consult the UIM card provider.
Authentication Types of Dial-up	PAP：Password Authentication Protocol

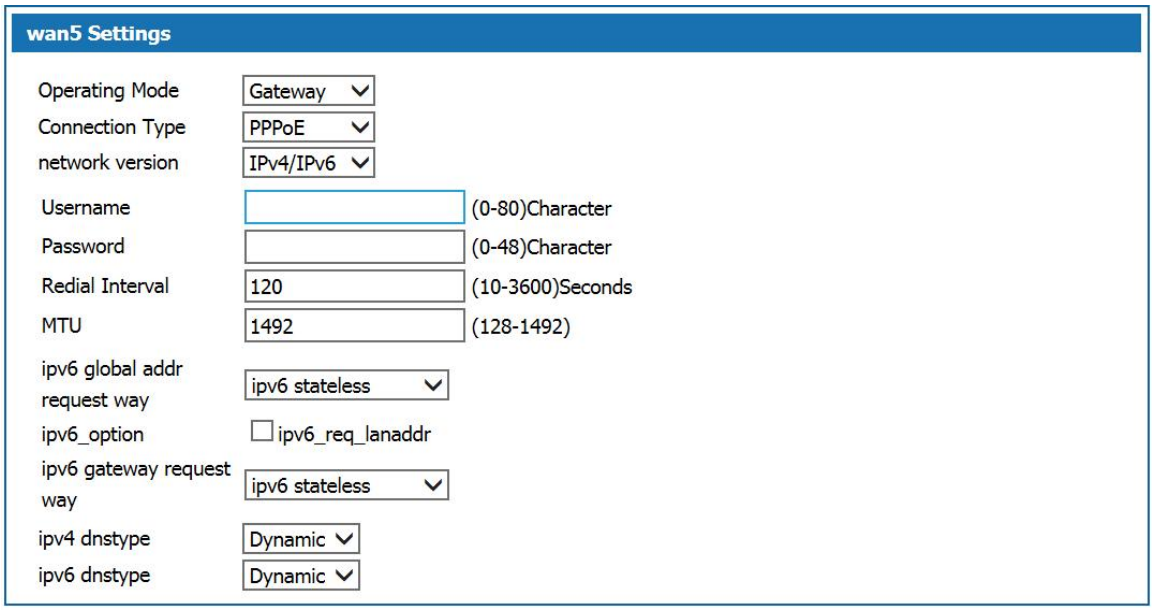
	CHAP：Challenge Handshake Authentication Protocol) MS-CHAP：Microsoft's version of the PPP challenge handshake authentication protocol AUTO: The authentication type needs to be the same with the PPP server, depending on which class is selected Please consult your ISP.
Types of Dial-up	Keep connecting: After successful dialing, it is always in the connection state. On demand connection: On-demand connection: when there is network traffic, the dial-up connection is triggered; Disconnect automatically when there is no network traffic. For example, when a user sends or receives mail, he starts to connect to the Internet by dial-up connection, and disconnects when he finishes sending or receiving mail.
Redial Interval	10-3600 seconds,default is 120 seconds,it is suggested to default value.
MTU	Maximum Transmission Unit Is the maximum units of data that can be transmitted in a given physical network. The value range is 128~ 1492, the unit is byte, the default is 1492, it is recommended to keep the default value.
DNS	DNS with dynamic fetch: the device automatically gets the DNS server address. Use the specified DNS: manually set the DNS server address.

Please insert 3G card into the USB port before configuration. The 3G card supports huawei EC122, huawei EC1261,Huawei EC156, zte AC580, zte AC582, zte AC583, zte AC2736.

WAN connection types include PPPOE, static IP, DHCP and IPoE:

- PPPOE dial-up to access to the WAN port address

Select "PPPOE" in the "Connection Type" drop-down box on the "Basic Settings " page as shown in Figure 4-5



4-5 PPPOE to access IP address

Select **"IPv4"** as the protocol type and enter the user name and password of the user's broadband account in the Username and Password fields. The interval of the redial and MTU are default. The IPv4 DNS mode can be selected according to the actual network configuration, options are"Dynamically obtained DNS"or manually specify the primary and secondary DNS server address.

Select **"IPv6"** as the protocol type and enter the user name and password of the user's broadband account in the user name and password fields. The interval of the redial and MTU are default. Configure the IPv6 global address obtain way, IPv6 option, the default method of obtaining IPv6 gateway. The Ipv6 DNS mode can be selected according to the actual network configuration, options are"Dynamically obtained DNS"or manually specify the primary and secondary DNS server address.

IPv6 Configuration Item Description:

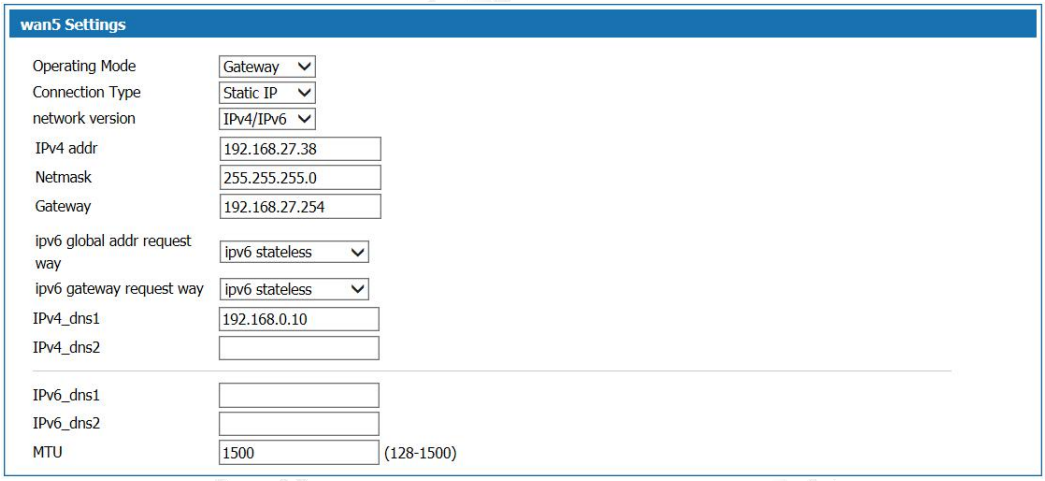
IPv6 Global Address Obtaining Method	No status Automatic configuration: Automatically generates an IPv6 address by the product based on the advertisement information of the remote router when the product first time connected to the network. Manual: Configure the IPv6 address and network prefix length in the text box below. DHCPv6: Obtain an IPv6 address through DHCPv6 with status.
IPv6 Options	Request LAN Prefix: If this option selected, the route advertisement options and DHCPv6 options in IPv6> Basic Configuration> LAN can be obtained by WAN Authorization.
IPv6 Default Gateway Obtaining	No status Autoconfiguration: Automatically generates an IPv6 Gateway address by the product based on the advertisement of the routing information sent by the

Method	peer end when the product first time connected to the network. Manual: Configure the IPv6 gateway address in the text box below.

Select IPv4 / IPv6 as the protocol type, configure IPv4 protocol and IPv6 protocol respectively. The device can access the network through both IPv4 and IPv6.

- Static IP

In the "Basic Settings" page, select "Static IP" from the drop-down list box as shown in Figure 4-6



4-6 Figure Static IP Page

Select "IPv4" as the protocol type. ISP will provide fixed WAN port IP address, subnet mask, gateway address and IPv4 DNS server address. Users should manually set these options.

Select the protocol type as IPv6 and set IPv6 global address and IPv6 default gateway access mode. Select the IPv6 DNS mode to use Dynamic DNS or manually specify the primary and secondary DNS server addresses. If the MTU is not set, There is a default value.

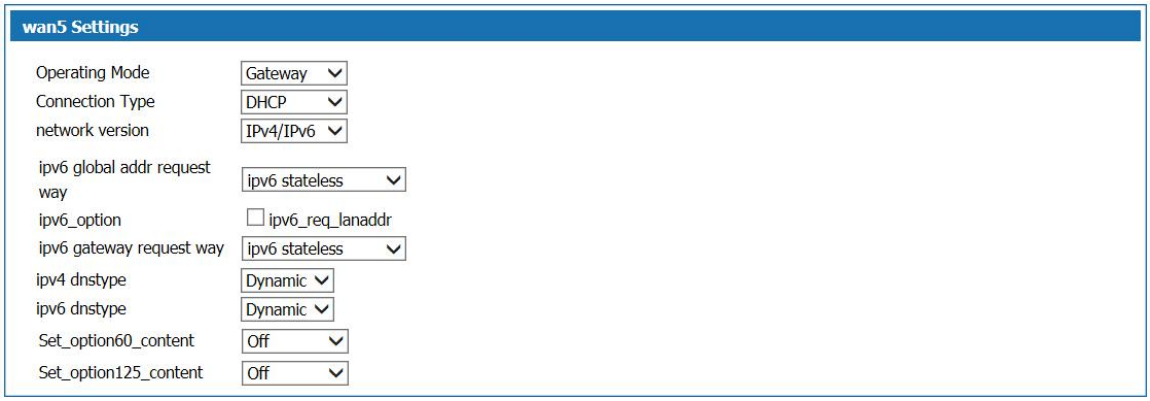
IPv6 Configuration Item Description:

IPv6 Global Address Obtaining Method	No status Automatic configuration: Automatically generates an IPv6 address by the product based on the advertisement information of the remote router when the product first time connected to the network. Manual: Configure the IPv6 address and network prefix length in the text box below.
IPv6 Default Gateway Obtaining Method	No status Autoconfiguration: Automatically generates an IPv6 Gateway address by the product based on the advertisement of the routing information sent by the peer end when the product first time connected to the network. Manual: Configure the IPv6 gateway address in the text box below.

Select IPv4 / IPv6 as the protocol type, configure IPv4 protocol and IPv6 protocol respectively. The device can access the network through both IPv4 and IPv6.

- DHCP way to obtain the WAN port address

Select "DHCP" in the "Connection Type" drop-down list on the "Basic Settings " page as shown in Figure4-7.



4-7 DHCP way to obtain IP

Select IPv4 as the protocol type. Select DNS using dynamic DNS. If you need to configure it manually, select Use specified DNS and enter the DNS server address provided by the ISP.

Select IPv6 as the IPv6 address and IPv6 default gateway. In IPv6 DNS mode, select Use DNS Dynamically. If you need to configure it manually, select Use Specified DNS. Then, Enter the DNS server address provided by your ISP.

IPv6 Configuration Item Description:

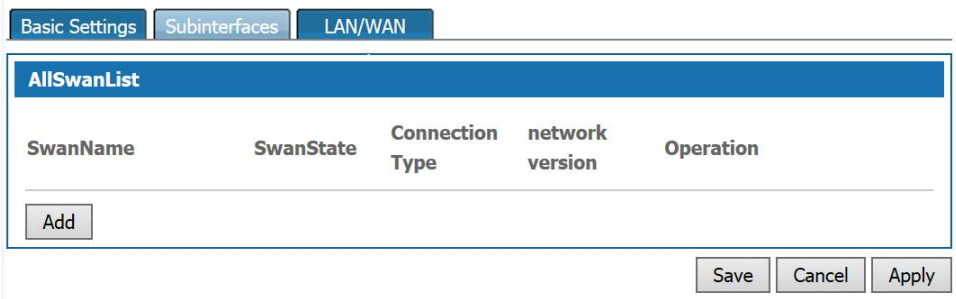
Business logo	The authentication information is exchanged according to the agreement with the routing device.
IPv6 Global Address Obtaining Method	No status Automatic configuration: Automatically generates an IPv6 address by the product based on the advertisement information of the remote router when the product first time connected to the network. Manual: Configure the IPv6 address and network prefix length in the text box below. DHCPv6: Obtain an IPv6 address through DHCPv6 with status.
IPv6 Options	Request LAN Prefix: If this option selected, the route advertisement options and DHCPv6 options in IPv6> Basic Configuration> LAN can be obtained by WAN Authorization.
IPv6 Default Gateway	No status Autoconfiguration: Automatically generates an IPv6 Gateway address by the product

Obtaining Method	based on the advertisement of the routing information sent by the peer end when the product first time connected to the network. Manual: Configure the IPv6 gateway address in the text box below.

Select the protocol type as "IPv4/IPv6", respectively configure the IPv4 and IPv6 protocols, the device can use both IPv4 and IPv6 to access the network

WAN subinterface

When multiple services, such as Internet, IPTV, and VoIP services, need separate WAN ports as their own channels, multiple WAN subinterfaces should be enabled to configure LAN / WAN bonding. Select “Basic Setup> WAN Setup” and click the “Subinterfaces” tab. The page as shown in Figure 4-8 is displayed.



4-8 WAN Subinterfaces page

Click <Add> to pop up the page for adding a WAN sub-interface as shown in Figure 4-9.

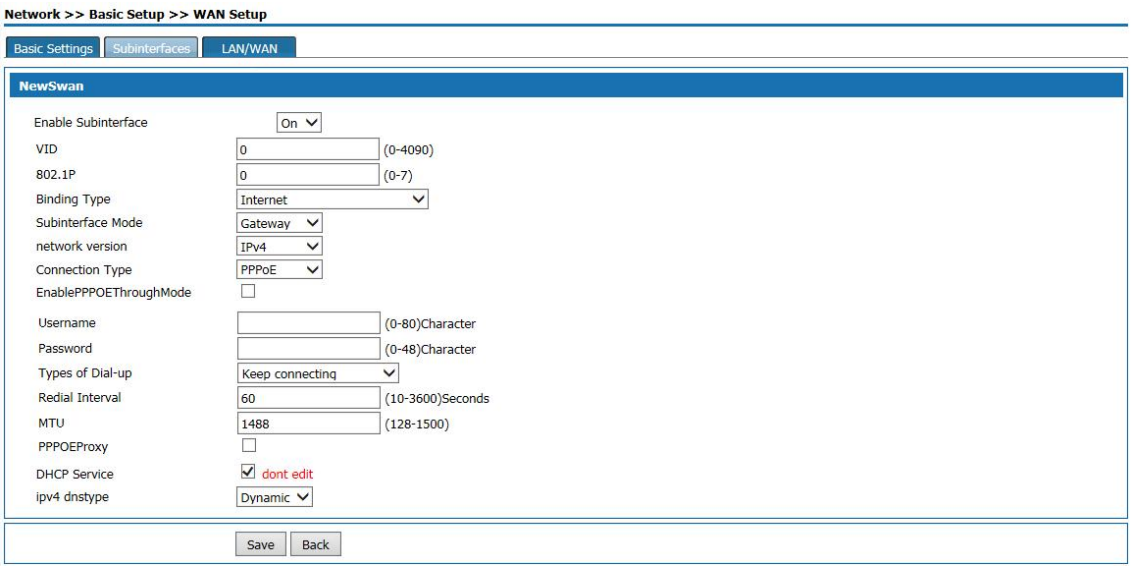


Figure4- 9 WAN Subinterfaces Configuration

WAN Subinterfaces Configuration description：

Item	Description
Enable Subinterface	Enable subinterface option or not
VID	Negotiate with the WAN port switch equipment in consensus
802.1P	Negotiate with the WAN port switch equipment in consensus
Binding Type	• Internet：The sub-interface for Internet access； • Management：This subinterface is used to manage the channel. When this type is set, the subinterface will be hidden in the LAN / WAN binding part； • IPTV：This sub-interface is for IPTV channel； • Management-Internet：This type is compatible with Internet access and management;； • Voice：This sub-interface is used for voice channel； • Management-Voice：This type is compatible with management and voice;； • Voice-Internet: This type is compatible with voice and Internet access；

Item	Description
	• Management-Voice-Internet: This type of compatible management, Internet access and voice； • Other：Other types.
Subinterface Mode	Options: Gateway, Bridge
Connection Type	Options include static IP, DHCP, PPPOE, configuration method is same with the one of WAN port.

Enable "Subinterface" mode, the WAN port "Basic Settings" will not be available.

LAN/WAN Binding

In WAN Subinterface mode or Bridge mode, the connection between VLAN network segment or LAN port and WAN side port can be achieve by adding a LAN / WAN binding.

Select “Basic Setup> WAN Setup” and click the “LAN / WAN” tab. The page shown in Figure 4-10 is displayed.

Figure4- 10 LAN/WAN Binding

VLAN binding: Select "VLAN binding" mode, and select from the drop-down box to bind the enabled VLAN with WAN subinterface.

Port binding: Select "Port binding" mode, and select from the drop-down box to bind the two internal network ports on the LAN side of the device withthe WAN subinterface.

When "Port binding" is selected,the "VLAN Settings", "Port VLAN Settings" and "VLAN Isolation" under "Basic Setup> LAN Setup" will be hidden.

4.1.4 DHCP Configuration

Select “Basic Setup> DHCP”. The DHCP Settings page is displayed as shown in Figure 4-11.

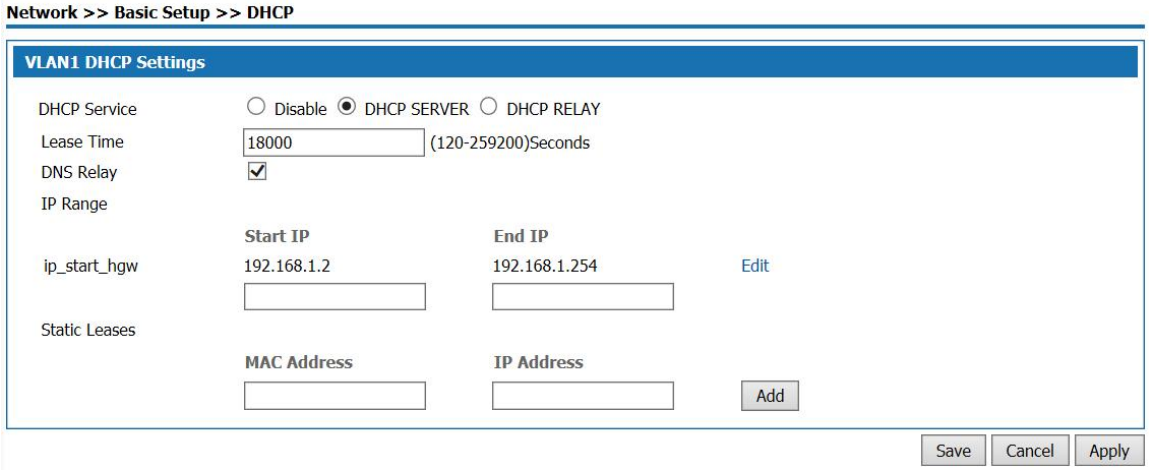


Figure4- 11 DHCP SERVER Configuration

- ..... When DHCP service is select as ” Disabled”, the DHCP function on the LAN port is disabled.
- ..... DHCP service is select as "DHCP SERVER", a page pop-up shown as Figure 4-11. This product acts as a DHCP (Dynamic Host Configuration Protocol) server and assigns IP addresses to computers in the LAN.

DHCP SERVER Configuration：

Table 4- 2 DHCP SERVER Configuration

Item	Description
Lease Time	Enter the lease time of the assigned IP address for computer, after the lease time, the computer must re-apply for an address (usually a computer will automatically apply). Unit: second, the default value is 18000 seconds.
IP Range	The DHCP server IP address pool configuration requires that the IP address of the LAN is on the same network segment. You can add multiple IP address pools to set the initial IP and end IP addresses of the address pool.
IP/MAC Address Binding	Add MAC and IP address bindings to meet the fixed IP needs of some machines. When the product receives a DHCP client request for an IP address, it first looks for the binding table. If the computer is in a binding table, it assigns the corresponding IP address to the computer.

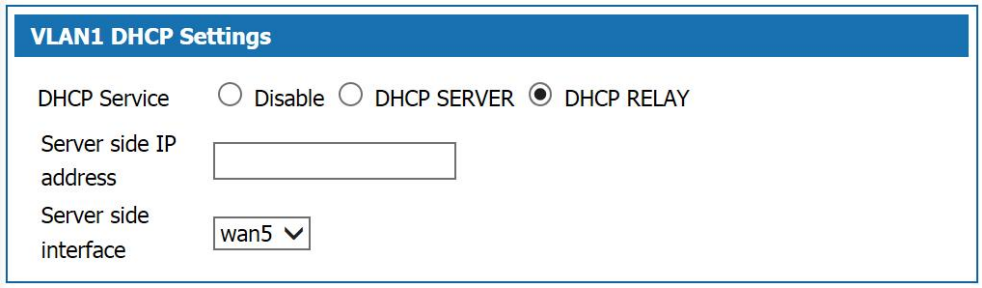


Figure4-12 DHCP RELAY Configuration

- DHCP Service: Select "DHCP RELAY" to open page shown in Figure5-11. If the DHCP client and DHCP server are not on the same physical segment, the DCHP Relay Agent (Relay Agent) is required. In this case, the LAN acts as a DHCP RELAY proxy to communicate with DHCP servers on other subnets to allocate IP addresses to DHCP clients.
- DHCP RELAY Configuration Description：

Table 4-3 DHCP RELAY Configuration

Item	Description
Server side IP Address	IP address of DHCP server connected
Server side interface	The interface that connect DHCP RELAY with DHCP server

4.2 Advanced options

Advanced options include DDNS Settings, static routing, dynamic routing, DNS Relay Settings, NAT, port mapping, virtual domain names, ALG, network usb flash drives, local subinterfaces, and multicast Settings.

4.2.1 DDNS Settings

The resolution between fixed domain name and dynamic IP address is realized. When the IP address of WAN port changes, this product will automatically initiate an update request to the designated DDNS server, and DDNS server will update the corresponding relationship between domain name and IP. Select "advanced options >DDNS" and enter the "DDNS Settings" page as shown in figure 4-13.

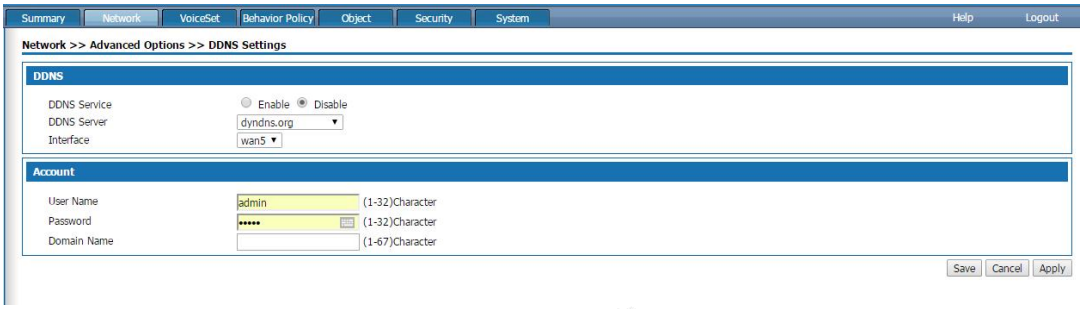


Figure 4-13 DDNS setting

The DDNS setting instructions are as follows:

Table 4-3 DDNS setting

Terms	Instruction
DDNS update	Enable or disable the DDNS service, the default value is enabled
Service type	Choose a provider of domain name services,currently the product only support www.3322.org
Username	The user name of register DDNS service.
password	The password of register DDNS service.
Domain name	Domain name bound to the WAN port IP address of the product.

4.2.2 Static Route

After defining the LAN port address, WAN port address and gateway, the device will automatically generate the interface network segment route and a default routing, with these routes,basic service needs can be meet in normal circumstances. Select" Advanced Options> Static Route". The "Static Route" page is displayed as shown in Figure 4-14.

Figure 4-14 Route setting page

Add route configuration description：

Table 4- 4 Add Routing

Item	Description
Name	User defined route name.
Destination IP	The destination address need to reach, it could be network address or host address.
Gateway	The IP address of the next router to pass before the data reaches the destination address.
NetMask	The destination address subnet mask to be reached.
Network Type	Select the static route out interface, including the LAN port and WAN port.

4.2.3 Dynamic Route

Dynamic routing means that the router can automatically set up its own routing table and adjust it according to the actual situation. The routing information exchange between the product and the docking device is realized based on RIP routing protocol. Route: network >advanced options>dynamic route, the page pops up as following:

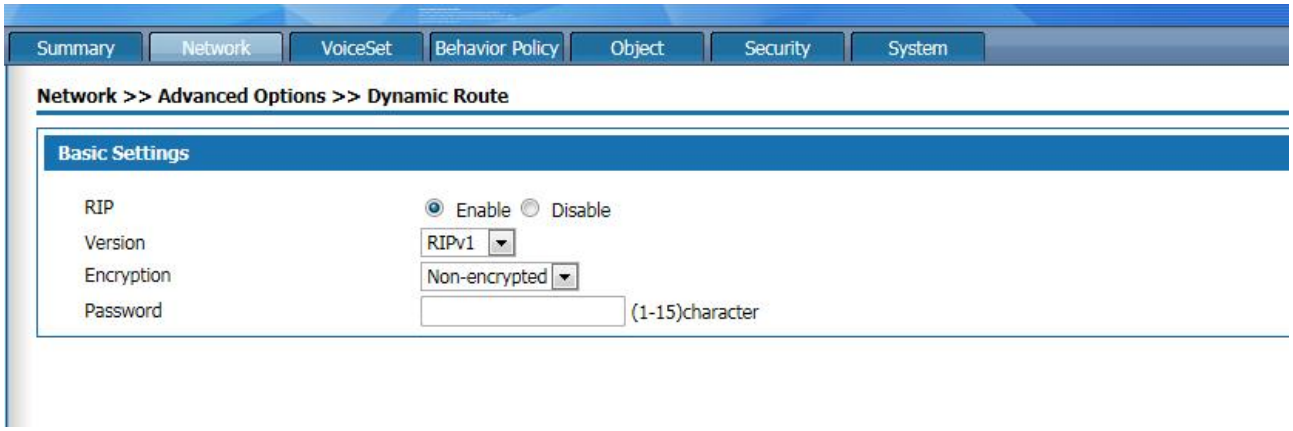


Figure 4-15 Dynamic Route

Items	Description
RIP	Click “enable” to enable Routing Information Protocol
Version	Consistent with docking routing devices, optional "default", "RIPv1" And "RIPv2". Select "default" to automatically negotiate with the docking routing device.
Encryption	Select “ RIPv1” ,no need to encrypt. Select “RIPv2”,negotiated with the docking device whether to encrypt or not.The device supports plaintext encryption and MD5 encryption. Set the encrypted password in the password box below.

4.2.4 NAT setting

Network Address Translation (NAT) enables multiple computers in the LAN to access the Internet through a small number of public IP addresses and save public IP addresses. As LANs are isolated from the Internet, NAT can also provide some assurance of Security. Select “Advanced Options> NAT”, and enter the NAT Configuration page as shown in Figure 4-16.

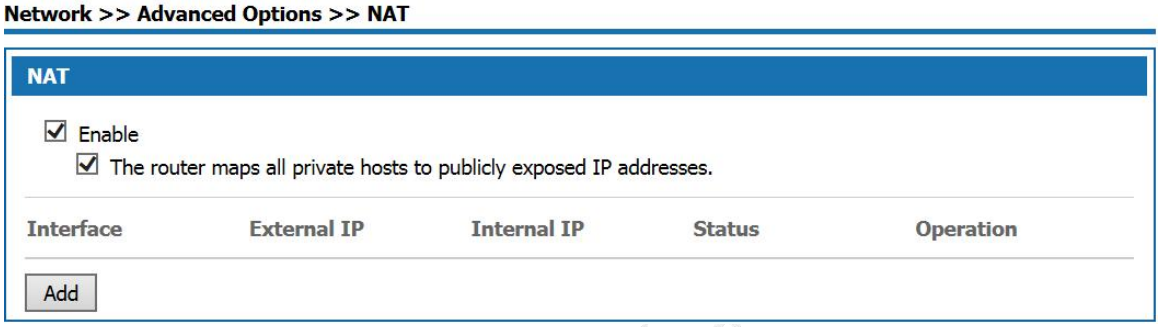


Figure 4-16 NAT SETTING

NAT setting description as following:

Table 4-16 NAT setting

Item	Description
Enable	Select“Enable” to activate NAT service
The router maps all private hosts to publicly exposed IP addresses	Select this item to enable NAT function, all the internal network IP address converted into WAN port IP address through the NAT function to ensure that users access the Internet. The NAT rule added later by the user takes precedence over this rule.

Click <Add> button to open the “Add NAT Configuration”page as shown in Figure 4-17

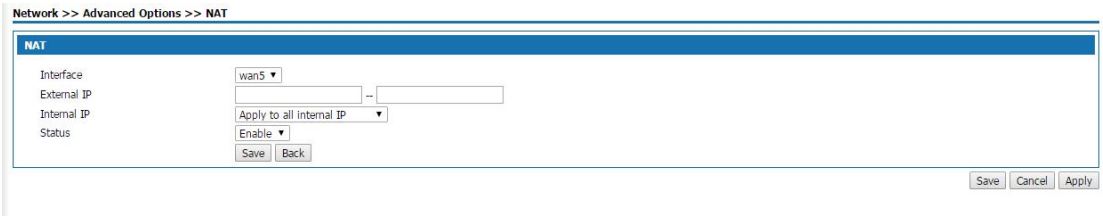


Figure 4-17 Add NAT Configuration

Add NAT Configuration：

Table 4- 17 Add NAT Configuration

Item	Description
Interface	Select WAN port.or wan sub interface port. NAT configuration added is valid when the WAN port address is static, otherwise it shows no static interface.
Extranet IP	IP address range used after address translation, the address range must be in the same network segment as the above network interface.
Intranet IP	Intranet IP address need to be translated. Select "Apply to all Intranet IP"， all Intranet IP are translated to the extranet IP through NAT function,select "Apply to the specified Intranet IP." Set the intranet addresses that need NAT to translated in the following text box .
status	Optional, Enable or Disable.

4.2.5 Port Mapping

Port mapping is used to map the WAN side IP of the device to the specific server IP of the Intranet. When accessing the Intranet specific server IP, just access the WAN side IP.

Choose “Advanced Options> Port Mapping”, and enter the “Port Mapping” page shown in Figure4-18.

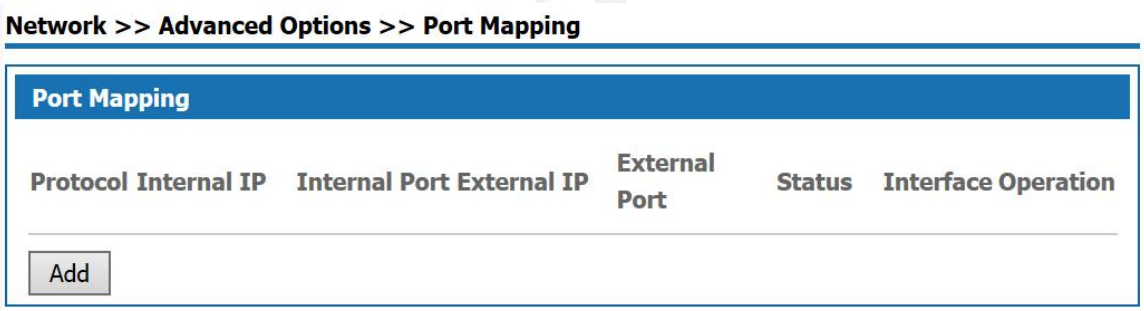
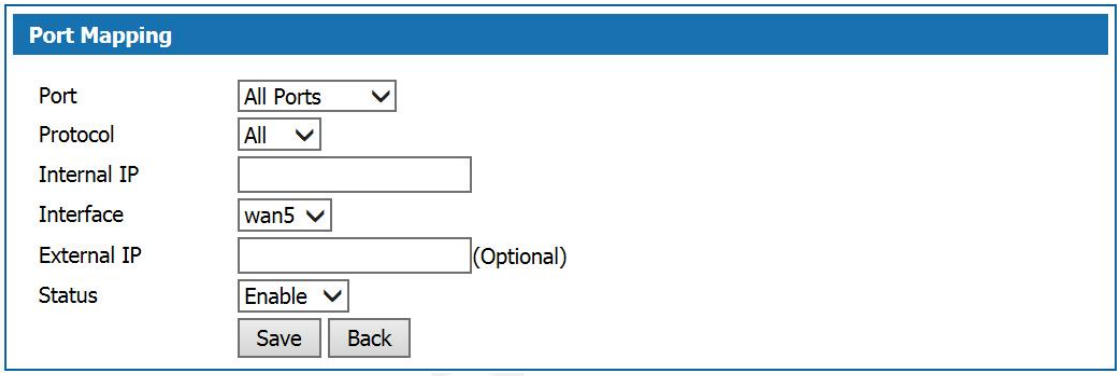


Figure 4-18 Port Mapping Configuration

Click <Add> button to open Add Port Mapping page shown in Figure 4-18.



Figur4-18 Add Port Mapping

Add Port Mapping Description：

Table 4-18 Add Port Mapping

Item	Description
Port	Any ports：In this mode, all ports will be mapped. Designated port： Users need to configure the “Intranet port” and ”Extranet port”.
Protocol	The data connection protocol used when port mapping，options include All,TCP or UDP.
Internal IP	The intranet IP that need port mapping
Internal Port	When selecting designated port,the internal port to be mapped externally,for example,www port is 80,ftp port is 21.
Interface	WAN port、WAN 3G or User Defined are available.
External IP	Network Interface selected as “ External IP”, set the IP address of the extranet used by the port mapping, which must belong to the NAT address pool.
External Port	When selecting "specify port", set the external network service port of the port mapping, such as WWW port 80, FTP port 21, and generally keep the same with the internal network port.
Status	Optional, Enable or Disable.

4.2.6 Host name setting

Virtual domain Settings allow users to set the domain name to access the corresponding Intranet IP address. Select Network >Advance options> Host name, the page will pops up as the figure 4-19.

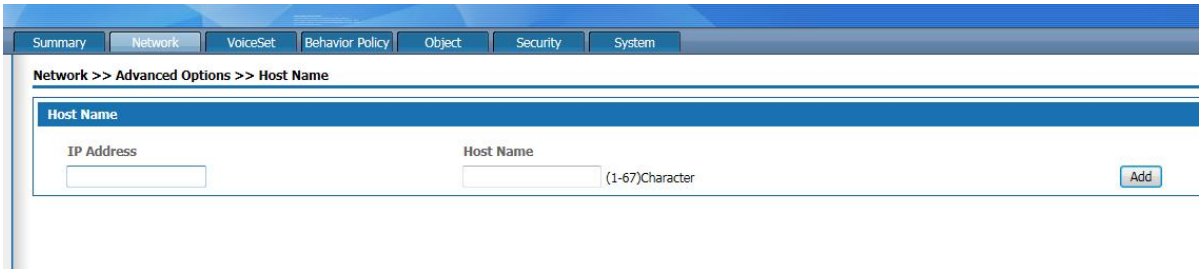


Figure 4-19 Host name setting page

Host name setting description as following:

Table 4-19 Host name setting description

Interface	Instruction
IP address	Intranet IP address
Host name	Set the host name of the intranet IP,the length is 1-67 characters

4.2.7 ALG setting

The ALG(Application Layer Gateway) is a type of firewall made by a an augmented firewall or computer network Application or firewall containing of security components for NAT.Enable ALG function to realize private network traversal function of SIP, FTP, H323, L2TP, RTSP, IPSEC and PPTP protocols.

Select "advanced options >ALG" and enter the "ALG" page as shown in figure 4-20

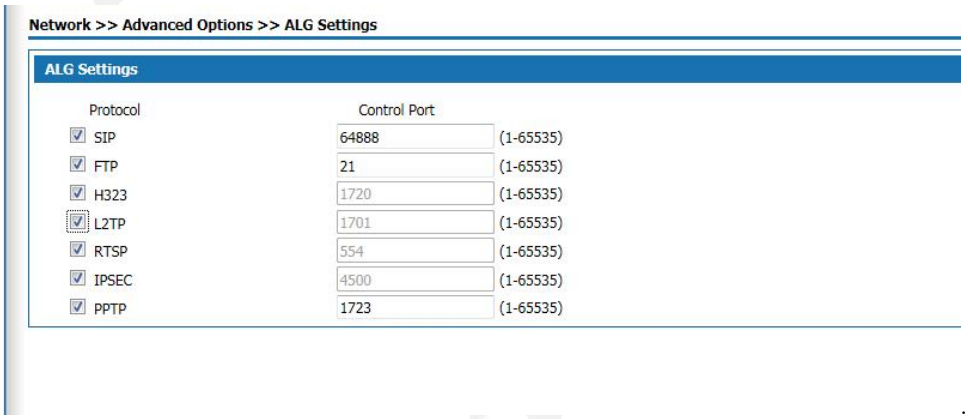


Figure 4-20 ALG setting

Select the radio box to enable ALG for the corresponding protocol.

4.2.8 Network U disk

The network U disk allows the files on the storage device attached to the USB interface of this product to be Shared automatically. Select "advanced option > network usb drive" and enter the "network usb drive" page as shown in figure 4-21.

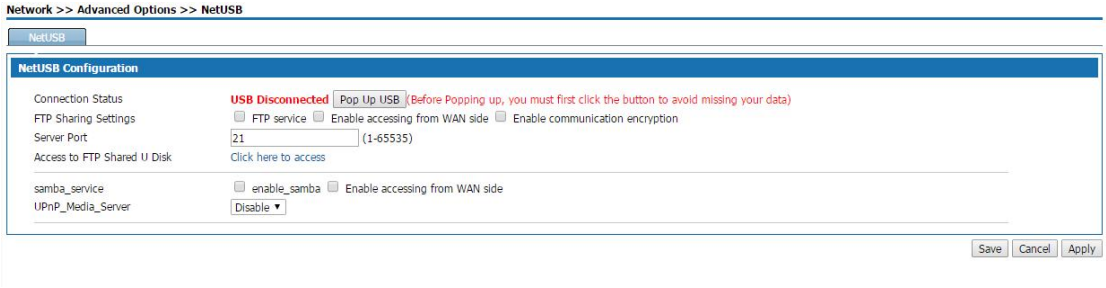


Figure 4-21 Network USB configuration

The setting instructions of network usb flash drive are as follows:

Table 4-21 network U disk Settings

Terms	Description
USB connection status	The product's USB interface is attached to the storage device, showing "USB connected"; otherwise, it shows "USB not connected". Before pulling out the USB drive, please click < pop up the USB drive > button, and then pull out the USB drive after the status update is "USB is not connected".
FTP setting	
FTP Sharing Settings	Select “FTP service”,the intranet users can access to the usb device by entering “ftp://local lan port address” in the browser. Select “Enable accessing from WAN side”,it is allowable for the WAN side users to access usb device by entering “ftp://product local wan port address” on the browser. “Enable communication encryption”: select this to enable the communication encryption.
Server port	FTP server port,generally set “21”
Access to FTP Shared U Disk	Click accessing here ,it can visit the shared u disk.

Terms	Description
Samba service setting	
Enable samba service	Select the radio box to enable the samba service. On Windows, the Intranet user clicks "start > run" and enters "\\ device LAN port IP address \usbshare" to access the network usb drive.
Enable accessing from WAN side	Select the radio box to allow users on the WAN side to access the network usb drive. In Windows system, the Intranet user clicks "start > run" and enters "\\ device WAN port IP address \usbshare" to access the network usb drive.

4.2.9 Local subinterface

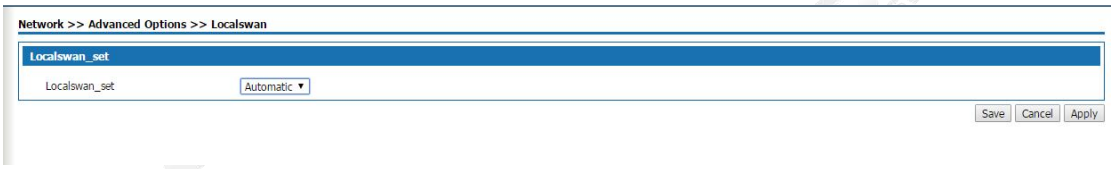


Figure 4-22 Network USB configuration

4.2.10 IGMP PROXY

Select advanced options> IGMP Proxy setting,the page pops up as figure 5-21

Figure 4-22 IGMP Proxy setting

This product supports IGMP proxy and IGMP listen function,click the radio box to enable the function. The proxy

interface is the interface connect with IGMP router,which can be WAN 5 or WAN sub-interface according to the drop-down box.

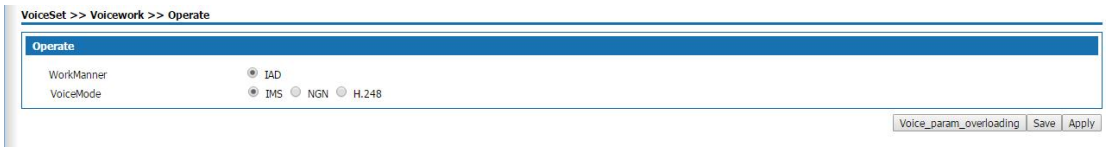
5.Voice Configuration

Voice configuration includes operate,SIP user set,SIP server set, Digitmap ,Codec set,IAD global set and Suppservice.

Before voice setting, please click "voice set" at the top of the page to enter the voice setting page.

5.1 Operate mode setting

Select<Voiceset> <Voicework> and <Operate> enter into the page as shown below:



5-1 Operate mode setup

The working mode is "IAD", and this product is used as integrated access device.

Select IMS in voice mode, click < voice_parameter_overloading >, and configure the parameters of device docking with IMS network; Select NGN network in the voice mode, click < voice_ parameter_overloading >, and configure the parameters of device docking with NGN network; Select H. 248 protocol for the voice mode, click < voice_parameters_overloading >, and configure the parameters for the device to interface with the MGC gateway.

5.2 SIP USER SET

When selecting "IMS" or "NGN" in the voice mode, select <Voice set>and <Voice work>then click the tab<SIP USER SET>" and enter the "SIP user setting" page as shown in figure 5-2.

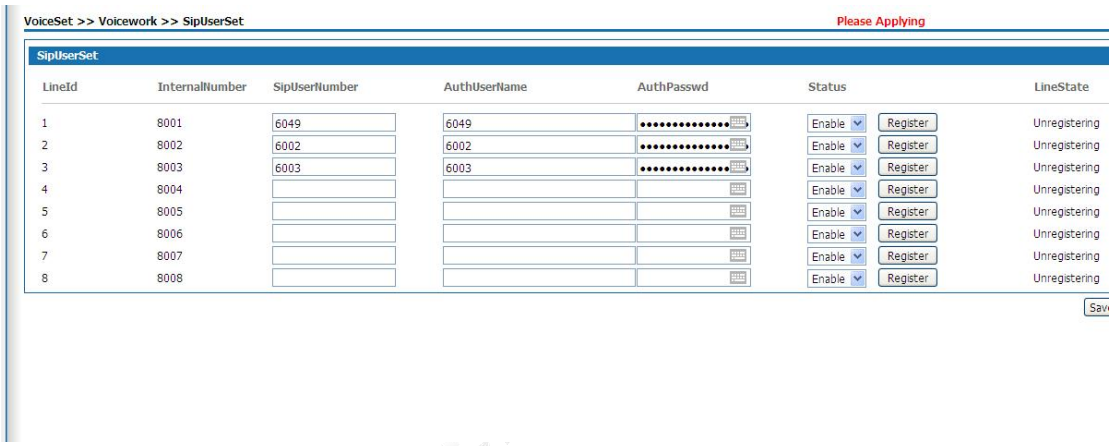


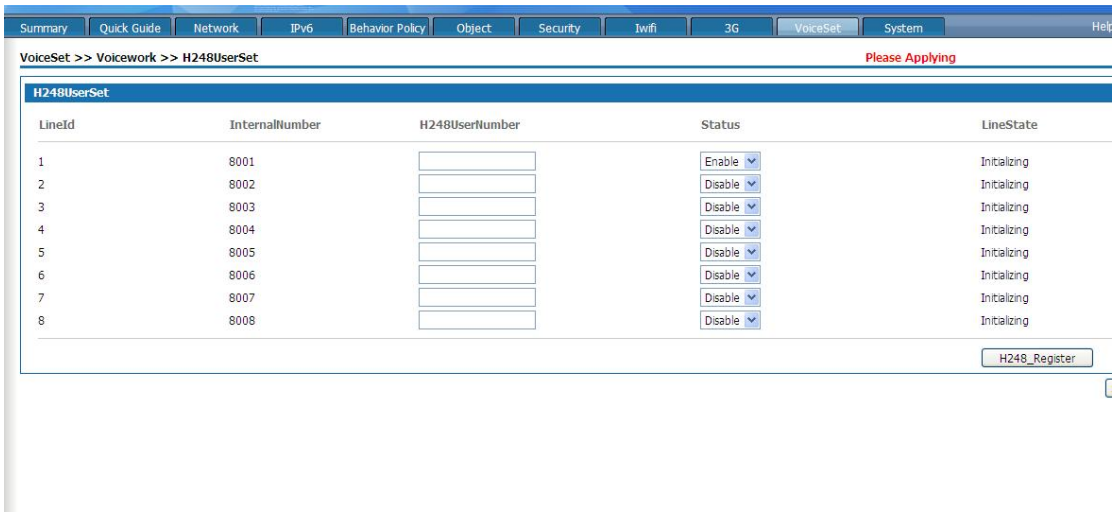
Figure 5-2 SIP user set

This product provides 8 FXS ports, 8 analog phones can be hung under the maximum support, 8 users can be added, the page has been configured with the internal number of 8 users. The user here is SIP user, go to analog channel.

Item	Description
Line ID	The analog channel for user,the system has default value.
Internal number	The user's internal number, the system has a default value, can not be modified
SIP user number	The SIP user number assigned to the user, and the SIP user number is used to dial each other between the IAD analog user and the external user.
Auth User name	Fill in the SIP registration server to identify the user name. After registration, the IP address of the user can be located.
Auth Password	Fill in the password of the registered authenticated user. The default value is “Aa111111”
Status	Select "enable" to enable the line; Select disable to disable the line.
Register	Click < register > to register with the SIP registration server.To set up the SIP server please see <Voicework> <SIP server set>
Linestatus	When the line is Disabled, display "Disabled"; When the line is enabled, "UP" will be displayed after successful registration; Registered failure show "Unregistering".

Generally speaking, there are two forms of docking with operators. One is direct docking, that is, no need Account number and password, only need to know the other party's IP address and port, directly invited the called number to the service operator; One is to register with the service server first and then send the invitation. In this way, authentication is enabled and the account and password are verified.

When choose “H.248” as voice mode,select <Voice work> and <H.248 USER SET> entering the H.248 user setup as the following page



Page 5-3 H.248 user setup

This product provides 8 FXS ports, 8 analog phones can be hung under the maximum support, 8 users can be added, the page has been configured with the internal number of 8 users. The users here are H. 248 users and go through the analog channel.

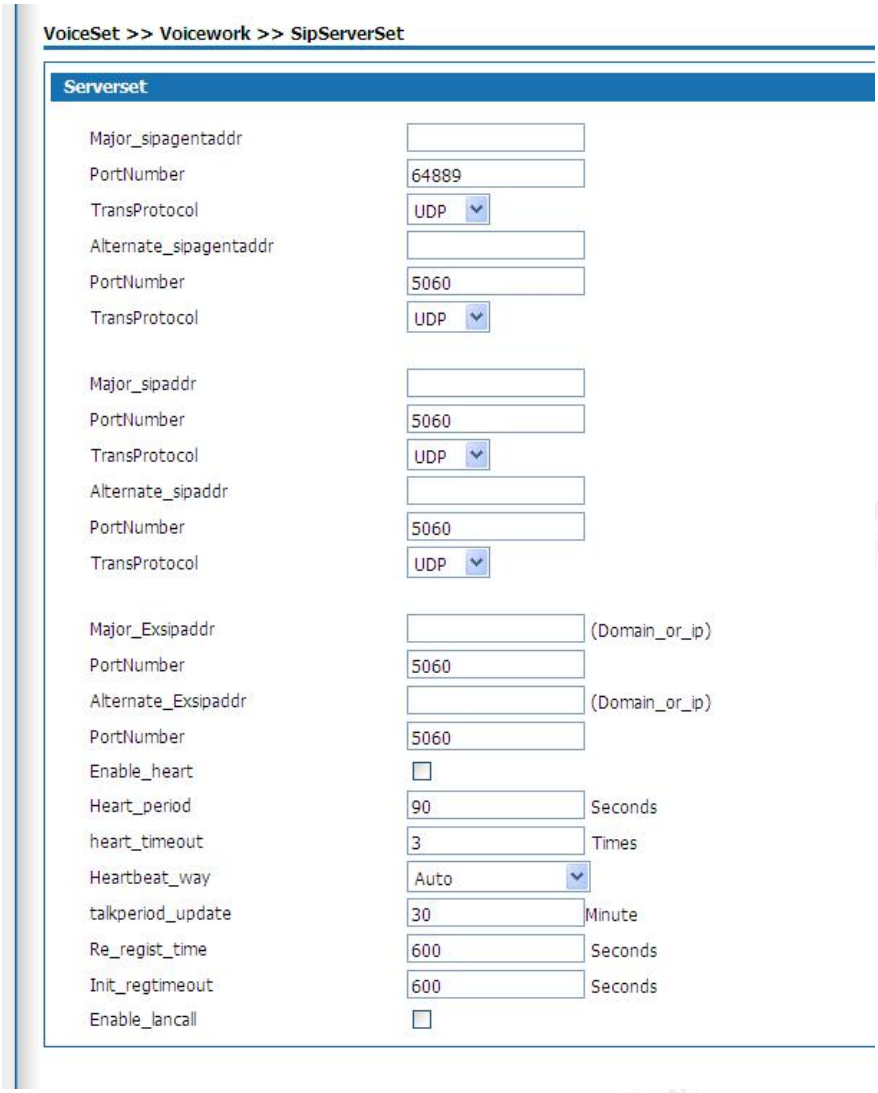
Items	Description
Line ID	This user is using an emulated channel, and the system has default values.
Internal Number	The user's internal number, the system has a default value, can not be modified
H.248 user number	Set the name of H. 248 user node. If the endpoint identification prefix is "A" in the parameter setting of H248, the H. 248 user can be set as A0-A7 respectively.
Status	Select "enable" to enable the line; Select disable to disable the line.
Register	Click < H248_register > to register with the MGC gateway. To set up the MGC gateway, see "working mode > H. 248 parameter Settings".
Line state	When the line is disabled, "Initializing" is displayed;When the line is enabled, after registration, show "Registering";Registration failed, shows "Unregistering"

Generally speaking, docking with the operator has two forms. One is direct docking, that is, no need Account and password, just need to know the other party's IP address and port, directly invited the called number to the service operator; One is to register with the service operator first and then send the invitation, which requires

authentication and account and password verification.

5.3 SIP server set

When selecting "IMS" or "NGN" in the voice mode, select <Voice set ><Voice work><SIPserver set> and enter the "SIP server setting" page as shown in figure 5-4.



Page 5-4 SIP server set

SIP server description as below:

Interface Items	Description
Major SIP agent address	Set the major SIP registration server IP address.
Port number	Set the major SIP server port number.
Trans protocol	Select the transport protocol that transports the SIP message and negotiate with the opposing device.
Alternate_sipagentaddr	Alternate SIP registration server address
Port number	Set the alternate SIP server port number.
Trans protocol	Select the transport protocol that transports the SIP

	message and negotiate with the opposing device.
Master SIP proxy server address	Set the IP address of the primary SIP proxy server.
Port number	Set the primary SIP proxy server port number.
Trans protocol	Select the transport protocol that transports the SIP message and negotiate with the opposing device.
Alternate_sipaddr	Set the IP address of the standby SIP proxy server.
Port number	Set the port number of the standby SIP proxy server.
Trans protocol	Select the transport protocol that transports the SIP message and negotiate with the opposing device.
Major_Exsipaddr	Set the main SIP external proxy server address.
PortNumber	Set the port number of main external SIP proxy server.
Alternate_Exsipaddr	Set the alternate SIP external proxy server address.
PortNumber	Set the port number of the alternate SIP external proxy server.
Enable_heart	Sets whether heartbeat between device and soft switch is enabled.
Heart_period	Set the heartbeat period,default value is 180s.
heart_timeout	Set the number of heartbeat timeout, the default value is 3 times, If the soft-platform is for 3 times without response, the device will be re-registered with the soft exchange
Heartbeat_way	The device provides four heartbeat modes of "Auto", "option_passive", "register_active" and "option_active".
talkperiod_update	Set the session cycle update time to 30 minutes by default.
Re_regist_time	If the device fails to register with the soft switching platform, the time for registration retry will be 600 s by default.
Init_regtimeout	Set the period of time after the device is successfully registered to the soft exchange, that is, the registration needs to be re-registered, and the default value is 600s.
Enable_lancall	

5.4 H248 parameter setting

This product can be used as MG to configure the address, domain name, port and other information of MG and MGC respectively. After MG successfully registers with MGC, MG and MGC will negotiate relevant configuration parameters.The MGC instructs the MG to detect a pick event at a terminal that can receive or initiate a call.

When the voice mode is “H.248”,select the <voicework> and<Paramset>,then the "H248 parameter setting" page pops up as shown in figure 5-5.

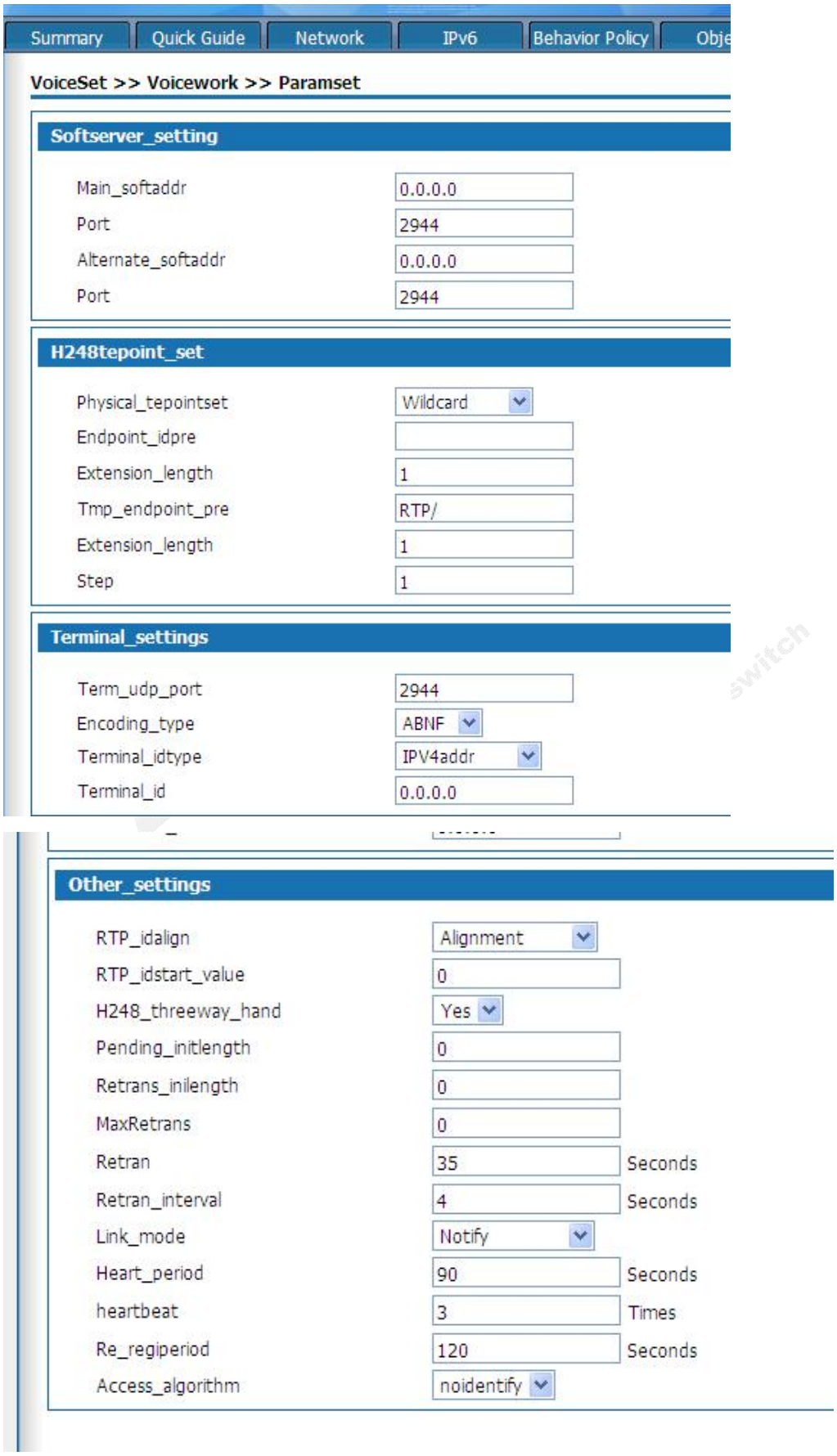


Figure 5-5 H248 parameter setting

Items	Instructions
Soft switch server setup	
Main_softaddr	Sets the IP address of the primary MGC.
Port	Set the main MGC port. The default value is 2944.
Alternate_softaddr	Set the IP address of the standby MGC.
Port	Set the standby MGC port.The default value is 2944
H.248 endpoint setting	
Physical endpoint Settings	Wild card and one_by_one
Endpoint_idpre	Set the physical endpoint prefix, generally the default value "A", provided by the MGC side.
Extension_length	Sets the number of digits to be added after the endpoint identification prefix; The default value of "0" means incrementing numerically.
Tmp_endpoint_pre	Set the temporary endpoint prefix, generally the default value "RTP/", provided by the MGC side.
Extension_length	Sets the number of digits added after the temporary endpoint identification prefix; The default value of "0" means incrementing numerically.
Step	Set the increment step of the RTP suffix number.
Terminal settings	
Term_udp_port	Set the terminal UDP port number. It is recommended to keep the default value of "2944".
Encoding_type	The device supports two types, "ABNF" and "ASN.1".
Terminal_idtype	The device supports three types “IPV4addr” ”Domain name””Device name” It should be keep the same with the MGC side.
Terminal_id	Input terminal ID,allocated by MGC side
Other settings	
RTP_idalign	Alignment and Non_alignment,it is the same configuration with the MGC side.
RTP_idstart_value	Sets the starting value of the temporary endpoint identity, which is generally the default value "0".
H248_threeway_hand	Set whether the H. 248 protocol requires three handshake authentication.
Pending_initlength	Set the Pending timer initial duration. It is recommended to keep the default value 0.
Retrans_inilength	Set the initial duration of the Retrans timer, and it is recommended to keep the default value 0.
MaxRetrans	Set the maximum number of retransmissions of messages. It is recommended to keep the default value 0.
Retran	Set the message retransmission time, and it is

	recommended to keep the default value.35S.
Retran_interval	Set the message retransmission interval. It is recommended to keep the default value.4Seconds.
Link_mode	“Notify”“ServiceChange”and “Audit” or no three modes
Heart_period	Configure h. 248 heartbeat cycle, which is the time set after the first successful registration of the device. After the device sends the heartbeat message to the soft exchange in the heartbeat cycle, the device will stop itself after receiving any message sent by the soft exchange.
heartbeat	Set the heartbeat detection times, the default value is 3 times.If the soft exchage doesn’t reply after 3times, the device will register again to the soft exchange.
Re_regiperiod	When the device fails to register with the soft switch server, then try to register again.the default interval is 120 s.
Access_algorithm	The device provides "MD5", "no identy" and "other" three access authentication algorithms, and the default value is "no identy".

5.5 Configuration sample

User number：+8651280910482，Authentication user name:+8651280910482@ims.js.chinamobile.com, Authpassword:14785236

IMS soft switch platform: 120.195.9.148

Connect one phone to RJ11 interface .

Select work manner IAD and voice mode “IMS”

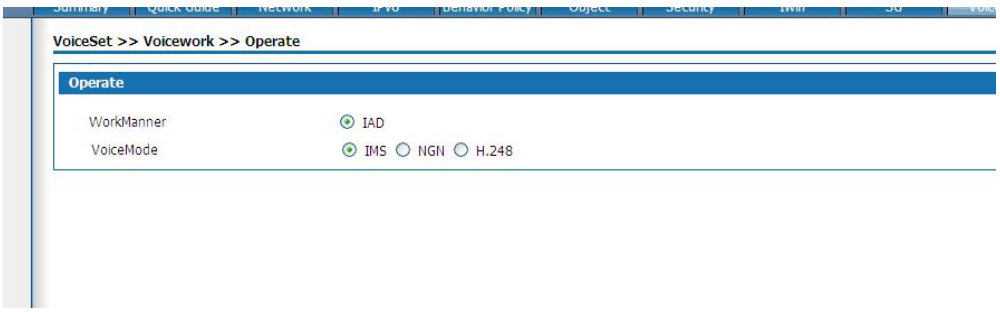


Figure5-6 Sample setting

Click<voice parameters overloading> to change specified parameters,click<save>to save the configuration,click <apply> to apply the configuration.

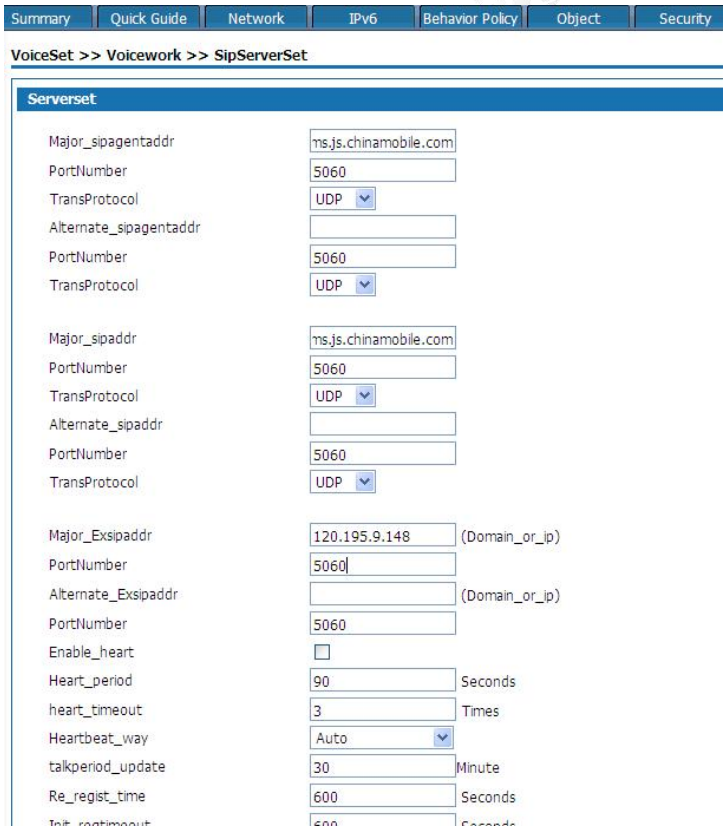
Set the SIP server

Set the main SIP register server IP address and main SIP proxy server IP address to be

“ims.js.chinamobile.com”.Main SIP external proxy server IP address “120.195.9.148”.The port number is “5060”,the transport protocol”UDP”,other keeps the default value as below.

The user number register to IMS soft switch platform.

The SIP user number is “+8651280910482”， The authentication user name is “+8651280910482@ims.js.chinamobile.com”,the authentication password “14785236”.Select “enable”and click <save> to save the configuration then click <apply> to make the configuration effective.Click < register > to register with IMS network. After successful registration, the line status shows "UP", and now the phone can be used through IMS channel when the device hangs down.



When the device hangs down the phone it supports tripartite communication, use the tripartite communication function normally and then passing the beat fork action can add users to join the call, the device can support up to five users to talk at the same time.

5.6 Codec setting

Select<Voice set><Voice work> and<Codec set>,the page pops up as following 5-9

Figure 5-9

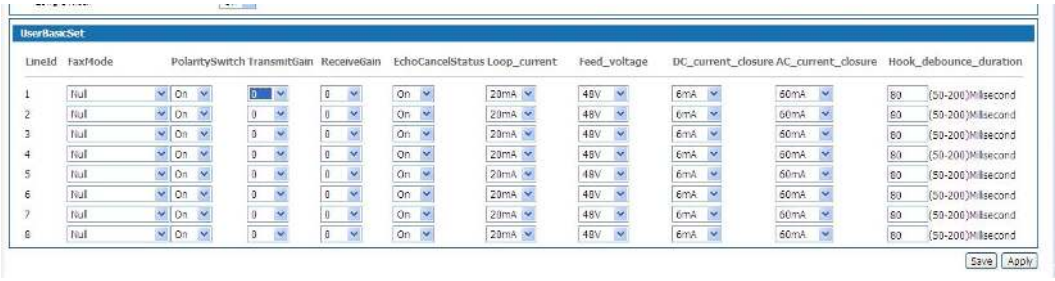
Configure the codec orders of the device,it should be negotiated with the opposite device in the order of priority encoding and decoding 1, 2, 3, 4 and 5.

5.7 IAD GLOBAL SET

Select <Voiceset><Voicework> and <IAD globalset>,then the page pops up as the following

Globalsetting

GC_domain		
Voicecall_ims_port	9060	(0~65535)
Voicecall_sip_port	5060	(0~65535)
ims_dscp	0	
Voicecall_rtp_port	10000 ~ 20000	(0~65535)
audio_dscp	0	
packet_time	20	Millisecond
TOS	0	
Same_phonetime	Off	
Call_display_mode	FSK	
FaxT38	Disable	
FaxT30	Enable	
FaxWayT30	ALL	
Voicefax	Disable	
DspInputGain	0	
dsp_dtmt_volume	-3	
dsp_clear_echo_enable	Enable	
DspClearEcho	64	
Media jitter buffer(ms)	150	
DspComfortVoice	Disable	
dsp_compress_mute	Disable	
whether_subscription	Disable	
Subscription cycle(s)	3600	
whether_supportprack	Yes	
whether_bifurcation	Yes	
whether_early_sessionssion	No	
DTMF_mode	Inband	
voip_sendponder	Yes	
start_digit_timer	10	
inter_digit_timer_short	2	
inter_digit_timer_long	3	
PlayHangTime	60	
PlayBusyToneTime	40	
NoAnswerTimer	60	
fxs_pch_time	90 - 500	(90~500)
Digiphone_code	58426	
Digiphone_second_code	58427	
hot_line	*53#	
Receive 183 + 180 Without P-Early-Media	Not play ring-back tone locally	
SipUserNum	0	
Short Switch	Off	
Long Switch	Off	
Voice Single Switch	Off	
Sip caller display header	PAI	
IMS is send unreg	No	
SIP FFRTP	Off	



5-10 Global set

Item	Instruction
Global set	
GC_domain	Government and enterprise gateway domain name
Voicecall_ims_port	The default value is 9060, which can also be negotiated with opposite devices.
Voicecall_sip_port	The default value is 5060which can also be the same with the opposite device,and the port range suggested is 1000-10000
ims_dscp	Sets the signaling DSCP priority value
Voicecall_rtp_port	The RTP port is generally set between 10000 and 20000
audio_dscp	Set the RTP DSCP priority value.
packet_time	Set how often the codec chip samples the voice packet and sends it as an IP message; The common packing time is 20ms and 30ms.
TOS	Set the TOS priority value.
Same_phonetime	With this option enabled, the phone time is synchronized with the device's time.
Call_display_mode	The device provides "FSK" mode.
FaxT38	Whether to enable or disable the T38 fax mode
FaxT30	Enable or disable FAX T30
FaxWayT30	The device provide “ALL” and “other”two mode
Voicefax	Enable or disable voice fax
DspInputGain	The volume of the voice of the initiating caller. The value range is -14db ~ 6db, volume gradually increased, default is "0db".
dsp_dtmt_volume	The volume of the user's keystroke sound during a call. The value range is -63db ~ 0db, and its volume increases gradually. Default identified as "-3db".
dsp_clear_echo_enable	Enable echo suppression control to eliminate the echo transmission on the peer.
DspClearEcho	Enable echo suppression control, set the suppression time, value 8 ~ 128ms, default value is "64ms".
DspComfortVoice	Enabling a comfortable background sound, the device has the technology to generate a comfortable background sound. With mute compression enabled, the

	device generates a mute packet during the mute period, saving bandwidth and making both parties comfortable.
dsp_compress_mute	Enable mute compression, detect the mute in the call stage and process it to save network bandwidth and reduce time delay; If mute compression is disabled, a normal sound signal is generated and transmitted even if mute is detected.
whether_subscription	When docking with the opposite device, some businesses require subscription. It is recommended to choose subscription.
whether_supportprack	When a phone call is dropped, the device sends the invite to the opposite platform Whether to send prack value after message; It is recommended that the default value be "yes".
whether_bifurcation	If the item above whether select prack select yes, this item is valid. If select yes,the branch value sent to the opposite platform by IAD can be different,it is suggested to keep the default value “ yes”
whether_early_sessionssion	Degualt value “NO”
DTMF_mode	Set the sending mode of DTMF, which is used to configure the way of dialing when the phone is sent. Info, inband and rfc2833 are provided, and the default is "rfc2833".
voip_sendponder	Select "yes", press "#" to send "#", select "no", press "#" without sending "#".
start_digit_timer	If the user does not dial the number for a certain period of time, the busy signal will be heard
inter_digit_timer_short	The current number dialed by the user can match a certain rule in the number graph, but the user may continue to dial, resulting in a match with different number graph rules. At this time, the device will not immediately send the number, but enable the short inter-bit timer time to wait for receiving more Numbers.
inter_digit_timer_long	If the current number dialed by the user needs at least one number to match any rule in the number graph, the interbit timer value is the interbit long timer time. Set the interbit timer time. When the set time is exceeded, the number will be sent out.
PlayHangTime	Set hurried hang off sound broadcast time, and over the time there will be no signal.
PlayBusyToneTime	Set the time for playing the busy tone. After the time is expired, the reminder tone will be listened to.

NoAnswerTimer	After the user dials,set how long there is no answer and play the prompt tone.
fxs_pch_time	Judge the patting fork action of the user, and it is considered to be the patting fork action within the set time range, and it is considered to hang up if the time exceeds the set time. It is recommended to keep the default values.
Digiphone_code	58426
Digiphone_second_code	58427
hot_line	*53#
SipUserNum	SIP user increased
Short switch	Use to turn on the switch between short number switch,the internal number can be dialed within the IAD.
Long Switch	Use to turn on the switch between long number swtich, SIP user number can be dialed by external device with this switch on.
Basic information	
FaxMode	Select the fax mode, “T.30 pass through” “T38” or “no”
PolaritySwitch	Select whether to enable polarity reversal. Enable this function. When the phone is connected, provide a reverse polarity signal.the phone billing starts billing, the default value is “off”,reflects not turn on this function.
TransmitGain	The transmission gain of the line is selected to adjust the strength of the transmitted signal. The effective parameter setting range is from -8 db to 8 db. The default value "0 db" does not change the signal strength.
ReceiveGain	The receiving gain of the circuit is selected to adjust the strength of the received signal. The effective parameter setting range is from -8 db to 8 db. The default value "0 db" does not change the signal strength.
EchoCancelStatus	Select whether to enable echo suppression.

5.8 Digitmap

The dialing rule is the number acquisition rule descriptor, which is used to detect and report the dialing events received by the terminal. The main purpose of using dialing rules is to improve the efficiency of this product to

send called code, that is, when the called number dialed by the user conforms to one of the dialing schemes defined in the dialing rules, this product will immediately send this called number.

Select the <Voiceset> and <Digitmap>,the digitmap page is as following

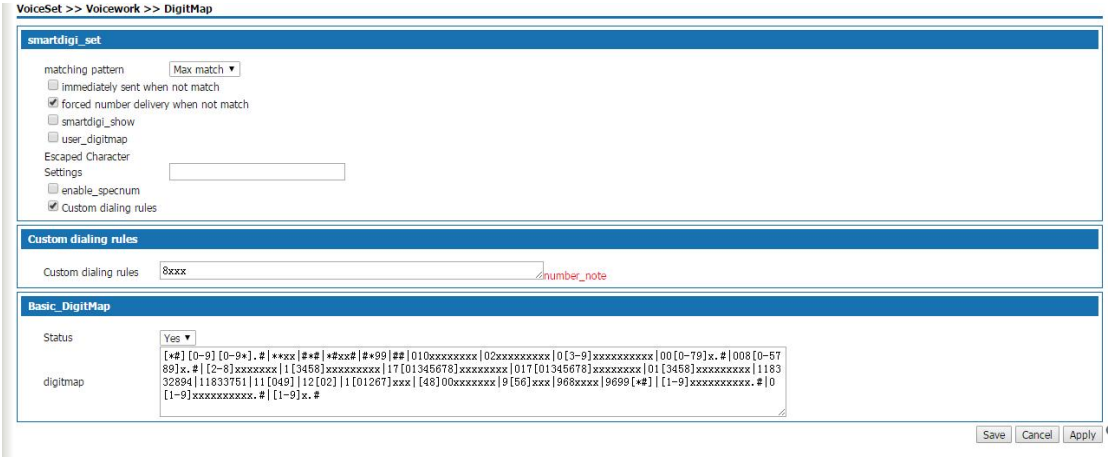


Figure5-8 Digitmap

Please refer to the page description for the description of dialing rules. The system default rules are as follows:

Item	Description
Enable or not	Select "yes" to enable the number graph rule; Select "no" to disable the number graph rule.
digitmap	When the called number dialed by the user conforms to the dialing rule defined by the number graph rule, the product will send the called number immediately.
immediately sent when not match	With this option enabled, when the called number does not match the defined number, the called number is sent directly.
Maximum matching pattern	The current number dialed by the user can match one of the rules in the number graph. At this time, the device will not immediately send out the number, but enable inter-bit short timer time to wait for receiving more Numbers. If the number exceeds the inter-bit short timer time without dialing, it will send out the number. If the user continues to dial and matches a number graph rule, the number is immediately sent out. If this is not enabled, the number will be sent the first time the number that the user dialed matches exactly the number graph rule. Maximum matching mode is recommended.

5.9 Suppservice

Supplementary services are used to display the existing services of users, which are parameters of tr069. These

parameters belong to the data subscribed to the core network, that is, they can only be used if the core network can support these services.

Select "working mode > supplementary service" and the page as shown in figure 5-11 pops up.

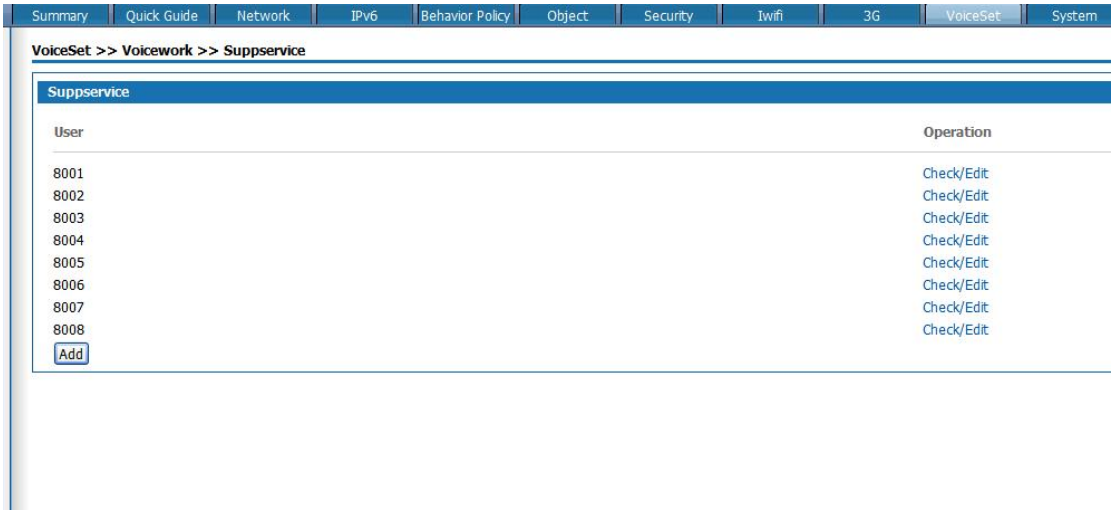


Figure 5-11 supplementary service

Select “check/Edit” the page it will pop up the page as following 5-12

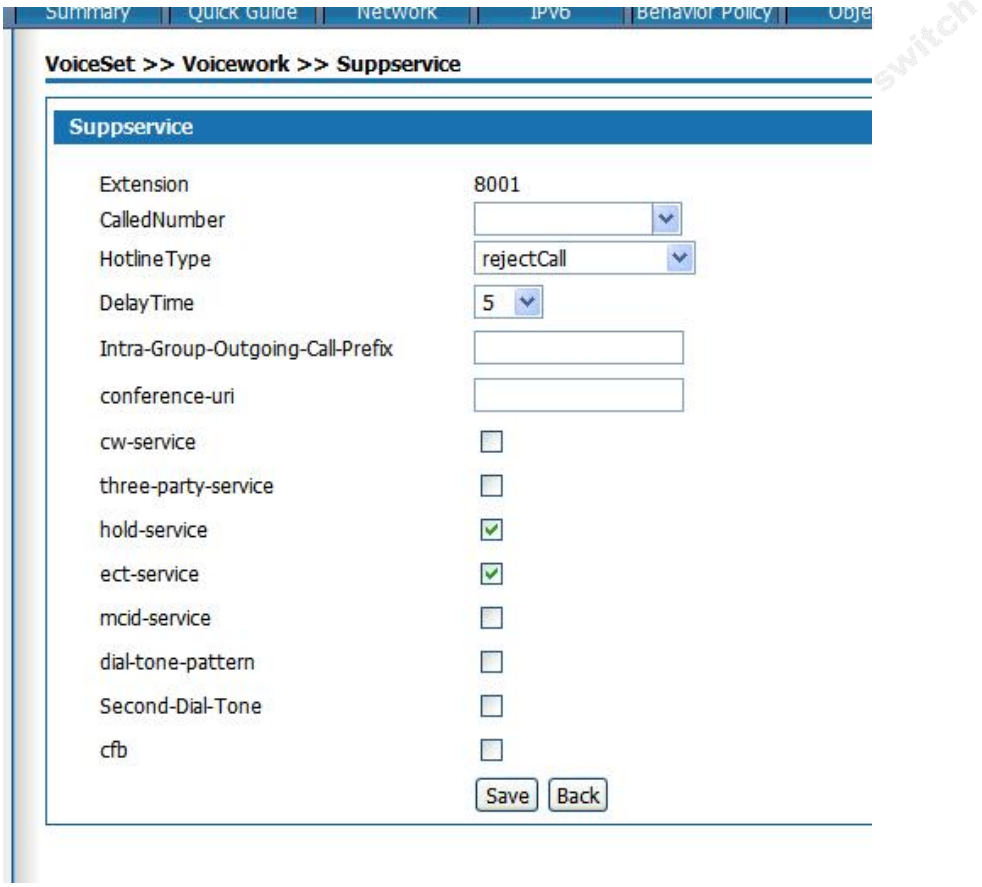


Figure 5-12

Interface items	Instruction
Extension number	Displays the extension number of the phone.
CalledNumber	The called number when hotline.

HotlineType	Rejectcall: the hotline is not activated Immediatelyhotline: refers to the user will not hear the dialing tone after the phone is picked up,it will immediately sent to the called number; Delay hotline: if the user does not dial the number within the delay time after picking up the phone, it will automatically transfer to the called number.
Intra-Group-Outgoing-Call-Prefix	If it is blank,that is no subcription to the business.It there is prefix number ,that is subscription to the business.The user can dial the outgoing-call-prefix to match the outgoing call rule. If there is a secondary dial tone service, plays the secondary dial tone.
Conference-uri	If there is value,it means subscription to the business. If there is blank,the service is not subscribed.
Cw-service	Cw-service (call waiting) shows empty, that is, no subscription to the service; Show checked, subscribe to business.
Three-party-service	Three-party-service shows empty, that is, no subscription to the service; Show checked, subscribe to business.
hold-service	The Hold-service box is empty, that is not subscription to the service.Show checked, subscribe to business.
ect-service	The ect-service box is empty, that is not subscription to the service.Show checked, subscribe to business.
mcid-service	The mcid-service box is empty, that is not subscription to the service.Show checked, subscribe to business.
dial-tone-pattern	The dial-tone-pattern box is empty, that is not subscription to the service.Show checked, subscribe to business.
second-dial-tone	The second-dial-tone box is empty, that is not subscription to the service.Show checked, subscribe to business.
cfb	The cfb box is empty, that is not subscription to the service.Show checked, subscribe to business.

6.Network security

Network security module includes basic Settings, firewall, ARP and DDos.

Before configuration, please click "security" at the top of the Web page to enter the network security page.

6.1Basic setting

Select<Security> and <basic setting> then the basic setting will pop up as following.

Figure 6-1 Basic setting

The basic setting as following

Items	Instruction
only_lan	If the administrator is allowed to log in the web management page of this product from LAN port, the default value is off.
only_wan	If the administrator is allowed to log in the web management page of this product from WAN port, the default value is off.
Permit Configuration From WLAN	If the administrator is allowed to log in the web management page of this product from WLAN port, the default value is off.
Enable Firewall	Firewall enabled or not, the default value is enable
Respond to PING on WAN	If the device on the Internet is allowed to ping the WAN port address of this product, the default value is off.
Lan ping	If the device on the internet is allowed to ping the Lan port address of the IAD product,the default value is off.

6.2 ACL access control

ACL access control is applicable to users in enterprises, governments, schools and other industries. Users can create diversified security policies based on the functions of ACL access control. Select "network security >ACL access control" to enter the page of "ACL access control" as shown in figure 6-2.

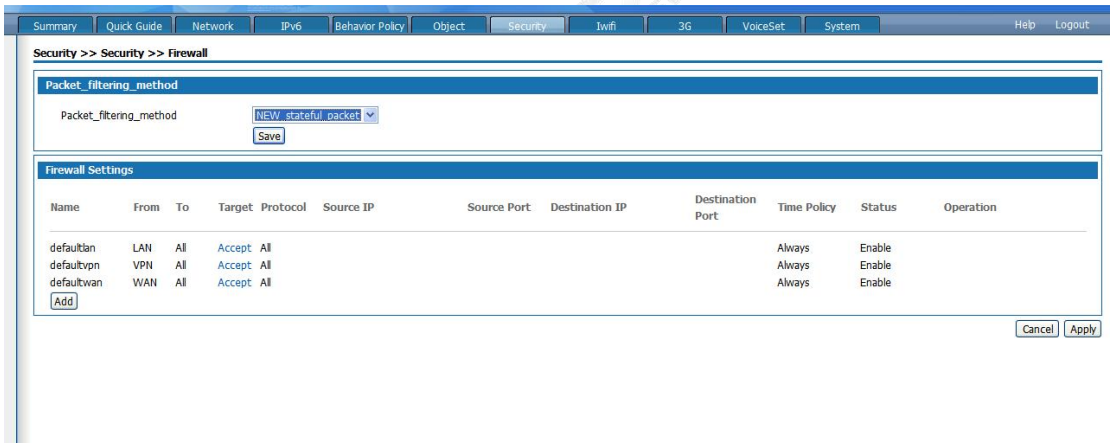
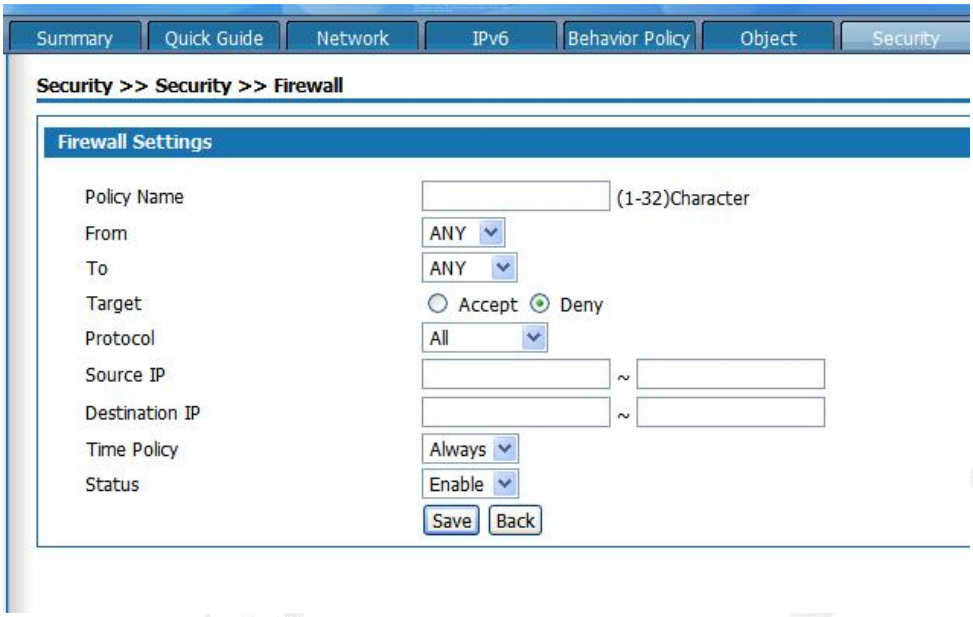


Figure6-2 Firewall

ACL access control policies for packets derived from the basic interface have been predefined in this product. Users can modify the policy target by clicking the target item.

Click the < add > button and enter the page of "add ACL access control rules" as shown in figure 6-3.

Add ACL access control rules as follows:



6-3 Add ACL control

Item	Instruction
Policy Name	Policy name,1-32 character
From to	From the source interface to the destination interface of the packet. Optional ANY, LAN, WAN,ANY Interface.
Target	Set the action of packet matching this rule: Accept:allows matching packets to pass. Deny:disallows matching packets from passing
Protocol	Set the protocol needs to control: TCP UDP, TCP+UDP,...SSH AND ALL
Source IP	Set the source IP address that matching this packet rule.When the users doesn't set the data,any source IP will apply to this rule.

Souce IP port number	Set the source port number matching this packet rule,the value range is 0~65535.This rule applies to any port number when this parameter is not set by the user.
Destination IP	Set the destination IP address that matching this packet rule.When the users doesn't set the data,any destination IP will apply to this rule.
Destination port number	Set the destination port number matching this packet rule,the value range is 0~65535.This rule applies to any port number when this parameter is not set by the user.
Time Policy	Set the time the rule is valid and select it from the drop-down box. "Always" means that any time is in play. For setting time policy, see <object > <schedule.>

After the rule is successfully added, the rules will be matched in the order from top to bottom. The user can change the order of the access control rules through the < up > and < down > buttons.

6.3 ARP DEFENSE

ARP attack prevention function is mainly to prevent a large number of invalid ARP request packets in the local area network (LAN) from filling the ARP table items of the device, so that the normal computer cannot access the device or the situation of the external network. This function should be combined with IP/MAC binding. After enabling this function, the system will only process ARP packets that conform to IP/MAC binding rules and discard other ARP packets directly, so as to achieve the function of preventing malicious ARP attacks. Therefore, before enabling the ARP anti-attack function, it is necessary to bind the legal IP/MAC address in the IP/MAC binding table.

6.3.1 The IP/MAC binding

Select <network security ><ARP defense> and enter the "IP/MAC binding" page as shown in figure 6-4.

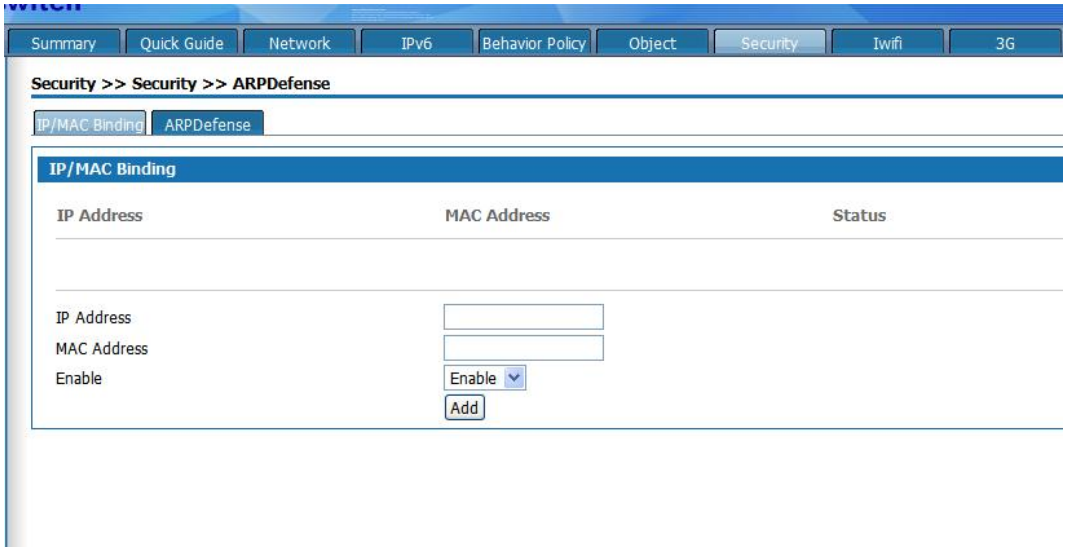


Figure 6-4 IP/MAC binding

Click the < import from system> button from the system, and the device will automatically learn the IP/MAC binding information in the ARP list, which will be displayed on the IP/MAC binding page.

You can also manually add IP/MAC binding information by setting the IP address and MAC address, and then click the < add > button to add IP/MAC binding information to the IP/MAC binding page.

The LAN computer IP/MAC binding table can be easily obtained by importing it from the system. However, due to ARP aging and other reasons it can not guarantee the import of all computer information. It is recommended that after importing through this method, check whether the computer you want to bind is in the binding table. If not, please Add it manually.

6.3.2 ARP Defense

Click<ARP DEFENSE> enter the ARP defense page as following

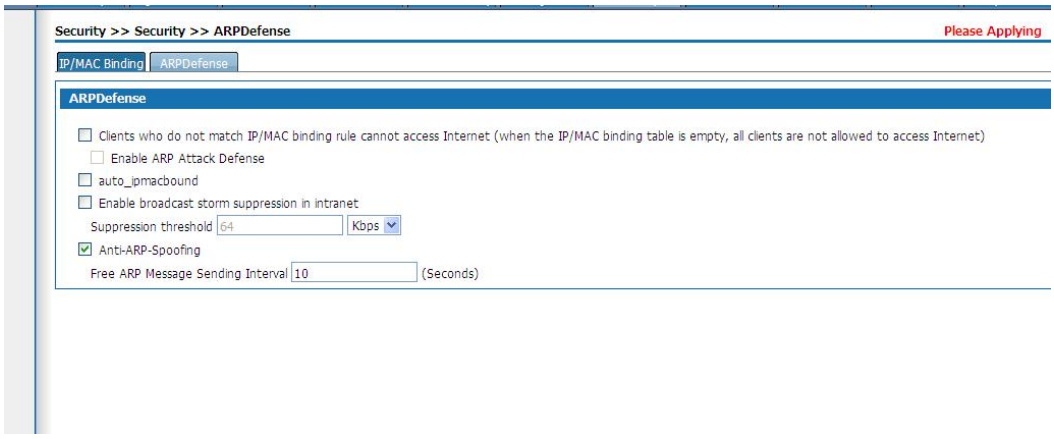


Figure6-5 ARP DEFENSE

The ARP anti-attack configuration is described as follows:

Clients who do not match IP/MAC binding rule cannot access Internet (when the IP/MAC binding table is empty, all clients are not allowed to access Internet)	Set whether users in the IP/MAC list have access to external networks. Check that only addresses enabled in the IP/MAC list can access the external network.
Enable ARP Attack Defense	Select Clients who do not match IP/MAC binding rule cannot access Internet can enable ARP attack defense. When enabled, ARP packets that do not match the IP/MAC list are discarded.
auto_ipmacbound	Select the radio box to enable automatic binding.
Enable broadcast storm suppression in intranet	After selecting the radio box and enabling the broadcast storm suppression function, the suppression threshold can be set. When the broadcast traffic exceeds the threshold, the system will discard the broadcast message.
Anti-ARP-Spoofing	Select the radio box and enable the ARP anti-spoofing function. By sending free ARP regularly Message to update all users' ARP tables to prevent ARP spoofing. Send free ARP message interval: default is 10 seconds.

Enable "disable clients that do not comply with IP/MAC binding rules from accessing the external network",please confirm that the IP/MAC binding table has been bound with the necessary IP/MAC information. Without any binding information, the device cannot be logged in from the WAN/LAN port.

6.4 DDOS defense

Intrusion protection provides protection against DDOS attacks, can achieve the dynamic filtering of malicious traffic, prevent large traffic based on a variety of protocol DDOS attacks, effectively ensure the stable operation of the network. Select "network security >DDOS" and enter the page of "DDOS protection" as shown in figure 6-6.

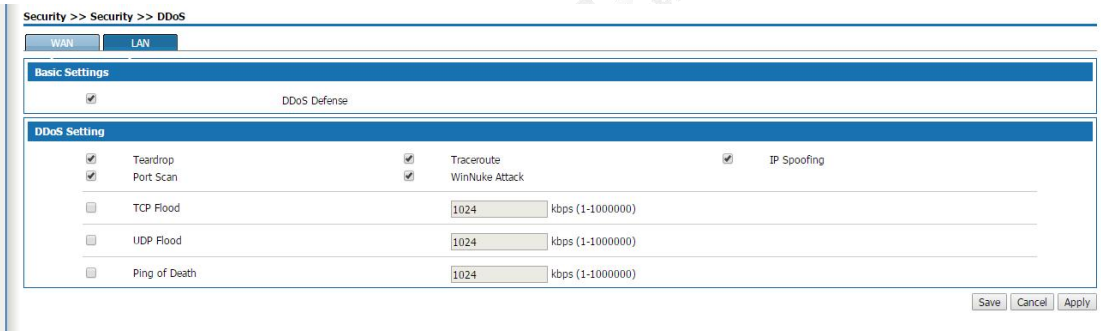


Figure 6-6 DDos defense

WAN setting page is used to protect external network users from DDoS attacks on devices; The LAN setup page is used to protect the device from DDoS attacks by Intranet users. Select "enable DDoS protection function" to

enable this function. It is recommended to turn on all preventive functions without special requirements. Open the TCP Flood attack defense, UDP Flood attack defense and ping Of Death attack defense, you can set the connection limit according to the traffic Of the server under normal circumstances, generally keep the default value.

7.System management

Before configuration, please click "system management" at the top of the page to enter the system management page.

System management to manage the hostname, time, password, backup and recovery, upgrade, remote management, restart, recovery of factory values, diagnostic tools, Bypass Settings and logs.

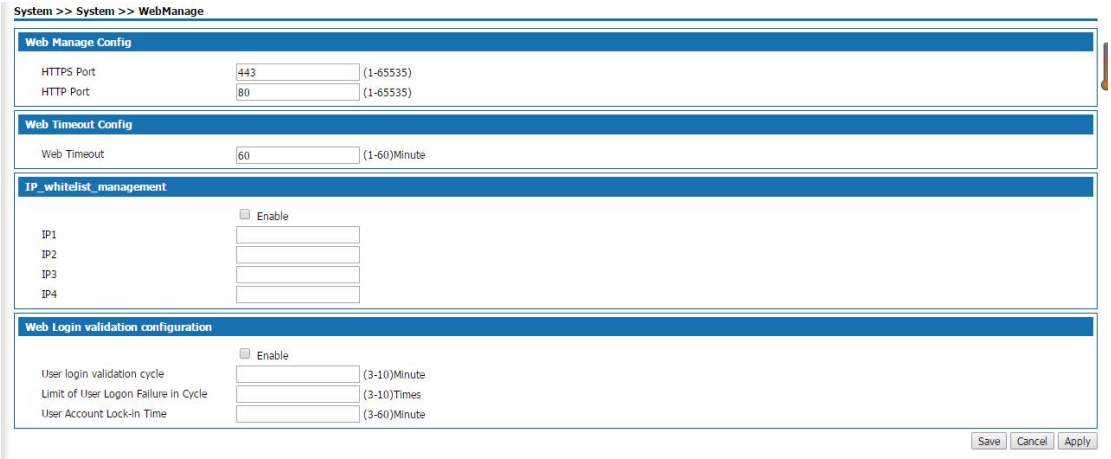
7.1 Basic setting

Select "system management > basic Settings" and enter the "basic Settings" page as shown in figure 7-1.

Figure 7-1 Basic setting

7.2 Web manage

Select “system management> Web Manage” and enter the web manage page as following



7.2 Web manage

The system has a default HTTP port of 80 and an HTTPS port of 443. You can modify the WEB administration port as you like, but generally you don't need to. The device was not operated on during the administrative timeout, and you need to log in the device again to continue the configuration.If whitelist is enabled, only computers with whitelist IP addresses are allowed to manage the WEB

7.3 Backup and restore configurations

If you have backed up the system setting information before, you can restore the current setting to the previous backup setting to ensure the normal operation of the product and reduce the loss caused by the loss of information when the system setting information of the product is lost due to wrong operation or other circumstances. Backup system setup information also helps with failure analysis.

Select “System management> Maintain” entering the “maintain”page as figure 7-3.

7-3 Backup and restore configurations

The operation for backup configuration to PC is below:

In “maintain”page select the backup to PC,enter< the file name to save> and click<Backup> button,it pops up the file download dialog box.In the”file download” dialog,click <saving>button and it pops up “save as ” dialog box. In “save as” dialog box select the information route then click saving button to save backup.

Result: The configuration information was successfully saved to the computer and the device can be recovered later through the configuration file

Backup configuration information to USB operation:

Insert the USB device into the USB port of the device, and the USB connection status is displayed as USB connected. On the configuration maintenance page, select backup to USB, click the < backup > button, and start

Result: After the successful backup to USB, it will pop up the page as following

Figure 7-4 configuration successfully

NOTE Please do not modify the backup configuration information file. The configuration file is encrypted. It cannot be restored to the device after modification.

Local import configuration:

Select<maintain> page click the <browse> button ,then it pops up the “select file “dialog box.In select file dialog

box, find out the backup file,click<open> button.In <maintain>page ,select<restore> button, then it will appear the succesful page as following

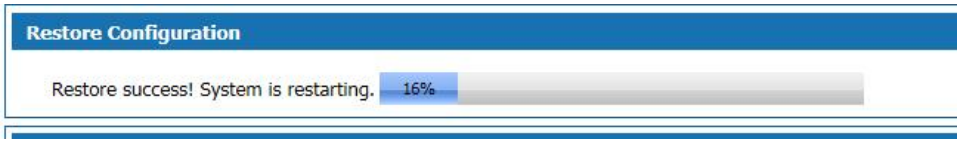


Figure 7-5 backup restore successful

Result:The system restarts and returns to the imported configuration information state.

USB import backup configuration process as follow:

After selecting the configuration file in USB, click the < restore > button to display the page of "setup information restored successfully" as shown in figure 7-5. After system restart, restore to the imported configuration of setup information.

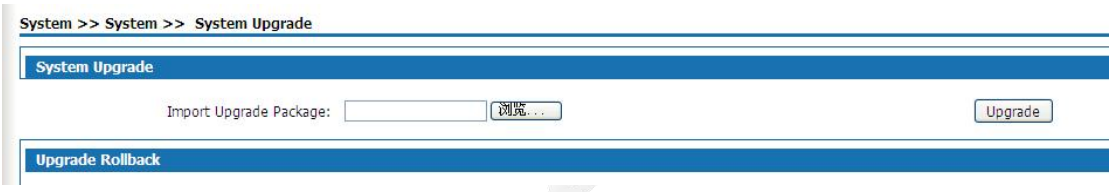
NOTE After the configuration information is restored, the current configuration information is lost. If you lose your current configuration information, take care to make a backup.

Restore installation configuration:

Click < start > to save the installation configuration to the device to display the save time of the configuration; Click < start > to restore the saved configuration information. After restoring the configuration, all the configuration information from the last installation configuration save time to the current time will be lost. Please pay attention to the backup.

7.4 Upgrade

Users of this product can contact the manufacturer to obtain the latest version and upgrade the system to obtain more functions and more stable performance. Select "system management > upgrade" to enter the "system upgrade" page as shown in figure 7-6.



Version upgrade operation is as follows:

Click the "browse >" button on the "upgrade" page, and the "select file" dialog box will pop up. In the "select file" dialog box to find the latest version of the file, click < to open the > button; Click the "upgrade >" button on the "upgrade" page, and the system will start to upgrade. The upgrade process will take some time. Please wait patiently.

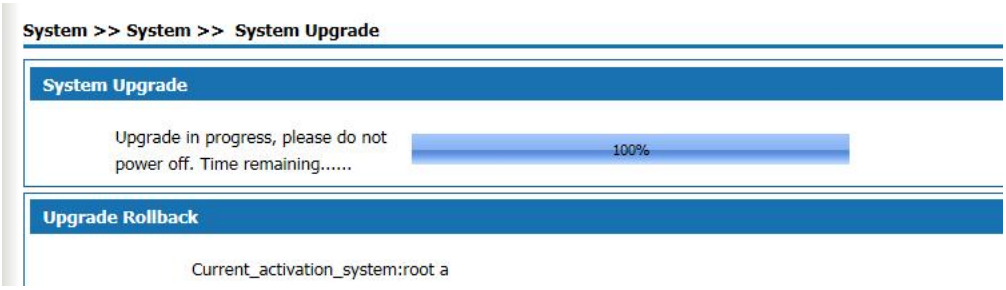


Figure 7-7 system upgrade successful

Result:

The system is restarted and upgraded to the latest version.

During the upgrade process, the system indicator light shows red slow flashing. After the upgrade is successful, the device is restarted.The system indicator light shows green quick flashing. After the login page pops up, if it works normally, the system indicator light shows green slow flashing.

7.5 SNMP SETTING

SNMP(Simple network management protocol) is the most popular network protocol currently.Through this protocol it can realized the visit and management of management device to managed device.SNMP protocol is based on the management of server and client.The background network management server serves as SNMP server, and the foreground network equipment serves as SNMP client. The background and foreground shares the same MIB management library and communicate through SNMP protocol.

Select<system management> enter into <SNMP> page as following

:

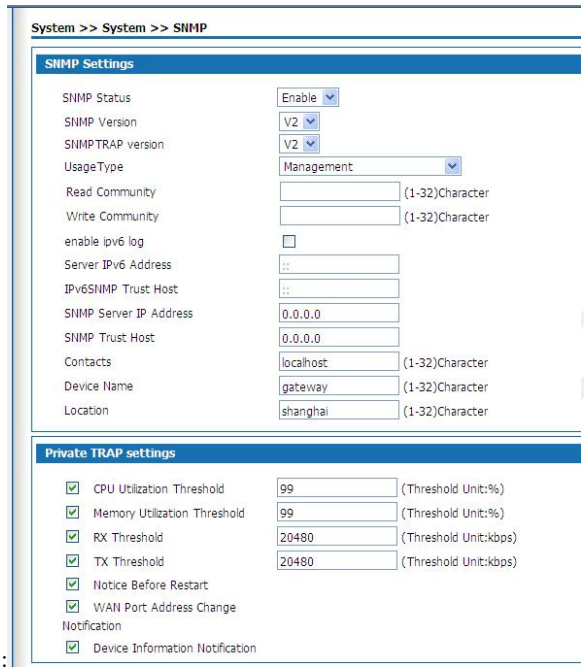


Figure 7-8 SNMP setting

SNMP setting as below:

Interface item	Instruction
SNMP setting	
SNMP Status	SNMP is optionally enabled or disabled, with the default being enabled.
SNMP Version	SNMP Version can be VI V2 V3 default value is V3
SNMPTRAP version	V1 V2 V3
UsageType	Default Management
Read Community	When the SNMP version selects "SNMPV1&V2", set the password used for read-only access.
Write Community	When the SNMP version selects "SNMPV1&V2", set the password to be used for read and write access.
enable ipv6 log	Checked
Server IPv6 Address	The IP address of the remote SNMP server, that is, the reception address of the TRAP. The default value is 192.168.3.193.
IPv6SNMP Trust Host	The trusted IP address,which means only the specified management device can visit this device.If not setting this term,then it will have no restriction on the management device IP address.
SNMP Username	When the SNMP version"SNMPV3",set the SNMP user name.
Encryption	When SNMP version select"SNMPV3",Set the SNMP Authentication algorithm: ● DES:CBC-DES（Data Encryption Standard) ● AES：Advanced Encryption Standard
Authentication Methods	When SNMP version selects "SNMPV3",Two authentication protocols are used in USM ● MD5:HMAC-MD5-96 ● SHA:HMAC-SHA(Secure Hash Algorithm)-96 Default :MD5
Encryption Password	When the SNMP version selects "SNMPV3", set the encryption code of SNMP user, which is used to encrypt the transmission message between the device and the management device, so as to avoid being overheard. Value range: 8-64 bit string.
Authentication Password	When "SNMPV3" is selected in SNMP version, the authentication secret code of SNMP user is set to verify the legitimacy of message sender and avoid the access of illegal users. Value range: 8-64 bit string.

Private TRAP Setting	
CPU Utilization Threshold	Send TRAP alarms when the device CPU usage exceeds the threshold. Enabled by default, the default value is 99.
Memory Utilization Threshold	Send TRAP alarms when the device memory usage exceeds the threshold. Enabled by default, the default value is 99.
RX Threshhold	Send TRAP alarms when the network interface incoming traffic exceeding the threshold. Enabled by default, the default is 20480.
TX Threshhold	Send TRAP alarms when the network interface outgoing traffic exceeding the threshold. Enabled by default, the default is 20480.
Notice Before Restart	The device runs the reboot command, send TRAP alarms before the device restarts. Enabled by default.
WAN Port Address Change Notification	TRAP alarm is sent when WAN port address change, TRAP content includes the new WAN port IP address. Enabled by default.
Device Information Notification	Send TRAP alarm when WAN address change, reboot device, access device or SNMP program is started. Enabled by default.

7.6 TR069 Configuration

TR-069 (CPE Wide Area Network Management Protocol) provides a common framework and protocols for managing the configuration of user network devices in next generation networks. The device can be centrally and remotely managed via ACS (Auto Configuration Server) on the network side.

Select “System > TR-069” to enter the “TR-069” page, as shown in Figure 7-9.

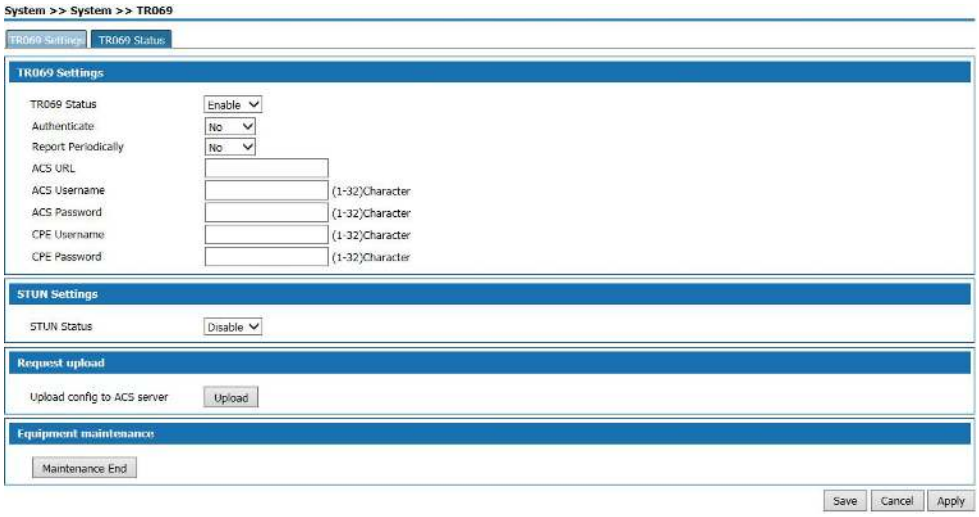


Figure7- 9 TR-069 Settings

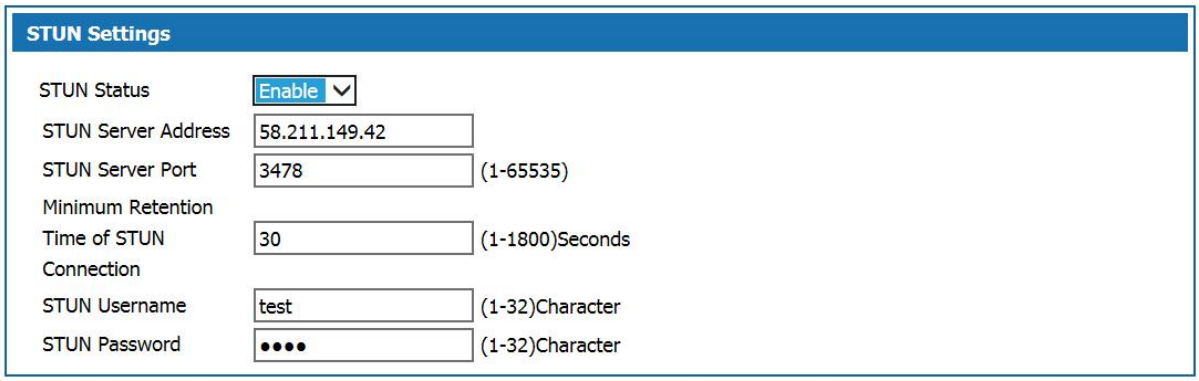


Figure7- 10 Settings

TR-069 Settings Description：

Item	Description
TR069 Settings	The Setting items are described below.
TR-069 Status	TR-069 Status Options "Enable" or "Disable", Enable by default.
Authenticate	Optional, Yes or No, the default is No.
Report Periodically	Select "No", not report periodically, Select "Yes" and set the interval of periodic report in the text box below.
ACS URL	The URL used when connecting to the ACS (Auto-Confi CPE (Customer Premise Equipment) guration Server), using the CPE WAN Management Protocol. This parameter should be set in valid HTTP or HTTP URL form.
ACS UserName	The user name of CPE when the CPE is connected to the ACS using the CPE WAN Management Protocol. The username is valid only when the CPE uses HTTP-based authentication. Value range: 1 ~ 32 characters.
ACS Password	CPE Password used at the time of authentication when connecting to the ACS using the CPE WAN Management Protocol. The password is valid only when the CPE uses HTTP-based authentication. Value range: 1 ~ 32 characters.
CPE Username	Authentication user name used by the ACS to initiate a connection request to the CPE. Value range: 1 ~ 32 characters
CPE Password	The authentication password used by the ACS to

Item	Description
	initiate a connection request to the CPE. Value range: 1 ~ 32 characters
STUN Settings	When this product is in a private network, it uses the datagram protocol to establish a port mapping on the product that interacts with the ACS through the STUN (Simple Network Address Translation) mechanism, so that the ACS can configure and manage the product. By default, STUN status is “Disable”. After selecting “Enable”, the page shown in Figure 10-10 is displayed. The configuration items are described as follows.
STUN server address	Address of the STUN server
STUN Server Port	The port number of the STUN server.
Minimum Retention Time of STUN Connection	The minimum holding time for the client to establish a connection with the STUN server.
STUN Username	User name used to log in to the STUN server.
STUN Password	Password for logging in the STUN server.
Request Upload	Click <Upload> to request to upload the device configuration to ACS server, The sending result of the request will pop-up on the right side.

The CPE refered in this manual is the 1800 device. ACS server address is provided by the telecommunications, make sure the port number and URL address must be correct.

7.7 Reboot

Select “System > Reboot”. The Reboot page is displayed as shown in Figure 7-11.

Figure7- 11 Reboot Page

Click <Confirm Reboot> to reboot the system.

- Do not power off during resboot.
- Network communication will be temporarily interrupted during resboot.

7.8 Restore Factory Default

Run Restore Factory Default, all the setting information of the product will be deleted and return to the factory default configuration status. This function is generally used when the equipment is changed from one network environment to another different network environment. The device is restored to the factory default configuration and then reset to better suit the current networking.

Select "System > Restore" and go to " Restore" page as shown in Figure7-12.

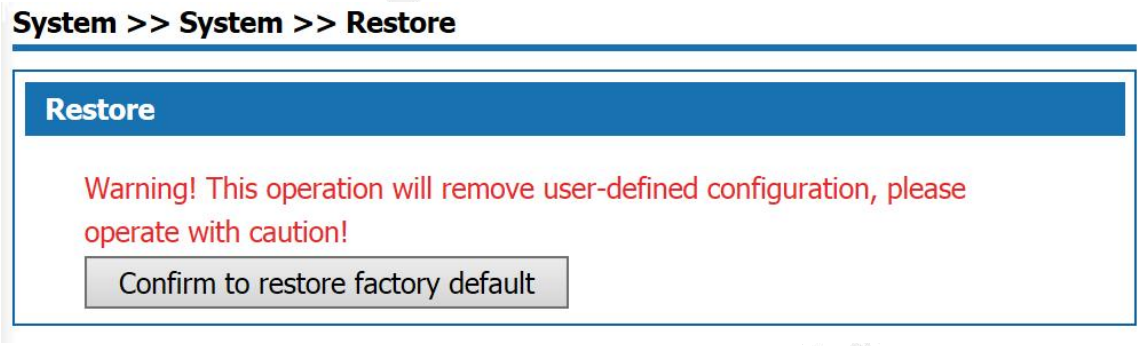


Figure7- 12 Restore Factory Default

- User will lose configuration when restore to the factory default. Please backup before the restore.
- After restoring to the factory default, the system will resboot.

Step 2 Select the diagnostic tool needed and enter the IP addr or Domain Name of the destination device in the Diagnostic Address text box.

Step 3 Click the “Run”button to start the debug.

Result The result will be displayed in the text box below.

7.9 System Debug

This product provides four kinds of diagnostic tools which include ping communication test, TraceRoute (route tracking), httpGet and DnsQuery. The Ping function is used to test whether the connection between the product and other network devices is normal or not. The TraceRoute function is used to test whether the link between the product and a computer or network device is normal. The HttpGet function is used for testing whether users of this product can access the Internet normally or not; DnsQuery function is used to test whether the server is valid.

Step 1 Select “System > Debug” to enter “Debug” page as shown in Figure 7-13.

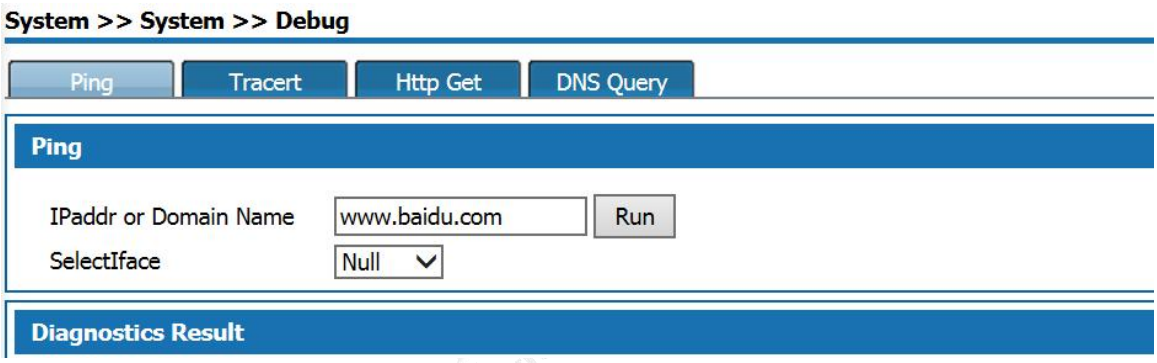


Figure7- 13 Debug

Step 2 Select the diagnostic tool needed and enter the IP addr or Domain Name of the destination device in the Diagnostic Address text box.

Step 3 Click the “Run”button to start the debug.

Result The result will be displayed in the text box below.

7.10 Time Settings

Select “System > Time Settings” to enter “Time Setting” page as shown in Figure 10-14.

There are two ways to set the system time. Obtain time through internet and manually set the system time. By default, the product obtains the time through NTP server.

Network Time Protocol (NTP) is used to provide time synchronization between routers, switches, and workstations. The function of time synchronization is to look at the related event records of multiple network devices to help analyze more complicated faults and security incidents.

NTP server to obtain time in two ways:

- When the product is connected to the Internet, it automatically obtains the time from the default NTP server of the device (this method is adopted by default).
- Enter the specified NTP server address, the product obtains the time from the specified NTP server.

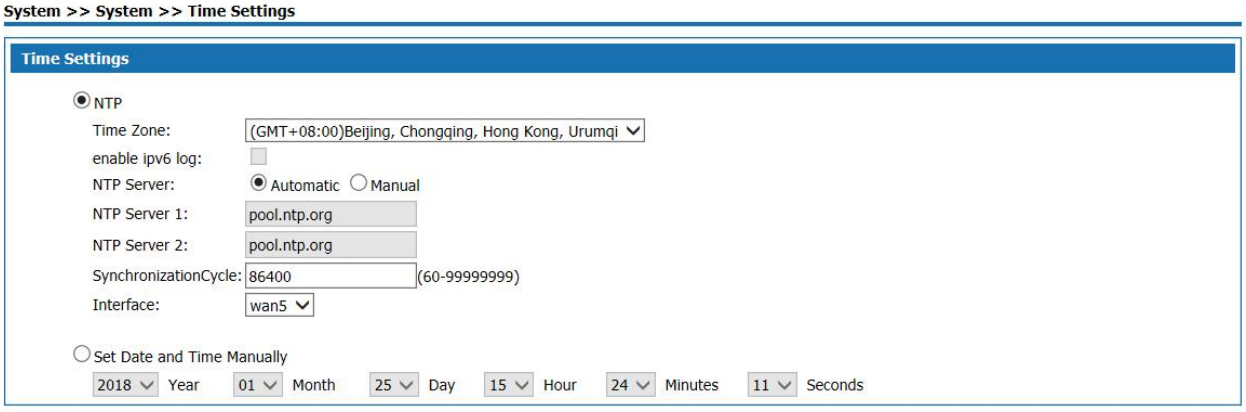


Figure7- 14 Time Settings

System Basic Configuration Page description:

Table 7- 3 Time Configuration

Item	Description

Item	Description
Enable NTP Time Zone	Check to enable NTP service function. The default value is Enable.
Time zone	Select the time zone of the product, the default is GMT + 08: 00 China standard time.
Time server	Automatic: Update the time from the default NTP server. Manual: If you need to set other NTP server, select "Manual", set NTP server, the product will update time from the specified NTP server. The default is automatic.
NTP Server 1 / NTP Server 2	In manual mode, you can manually set 2 NTP servers
Manually set the date and time	After selecting, manually set the time, turn off the NTP service function. The default is disabled.

7.11 Log Manage

Select “System > Log Manage” to enter “Log Manage” page as shown in Figure 7-15.

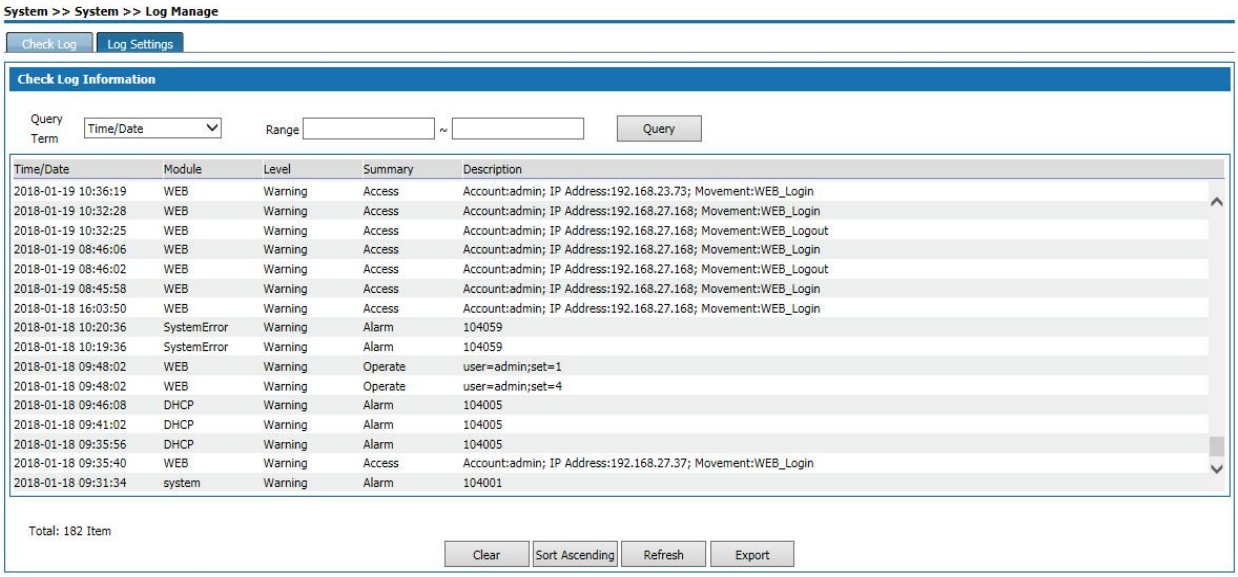


Figure7- 15 Log Manage—Check Log

Check Log description as follows:

Table 7- 4 Check Log Information

Item	Description
Query items	The system provides five query items: Time / Date, Module, Level, Summary,

Item	Description
	Description. Select a query item, set the content need to query. If select "Time", set the time range in the Time Range box and click <Query>, the query result will be shown in the following list.
Log information list	The log information displayed is five query items: Time / date: when the log occurred; Module: the log module; Level: The level of the log, including the five levels which are "warning", "err", "crit", "alert", and "emerg". Summary: The type of the log. “Alarm” is the alarm log. “Access” is the access log. “Operate” is the operation log. “URL-Filter” is the URL filtering log. “Flow” is the traffic log. Description: Displays the log information to analyze the operation.
Button Description	Clear: Click <Clear> to clear all the log information. Positive sequence display: Click the “Positive Sequence” button, the log information is displayed in chronological order, and the button is changed to “Reverse Order display”. Refresh: Click the “ Refresh” button to display the latest log information.

In the log page, users can specify the log information to be displayed in "Log Information View" or set the remote log sending function. Click the [Log Settings] tab to enter page shown in Figure 7-16.

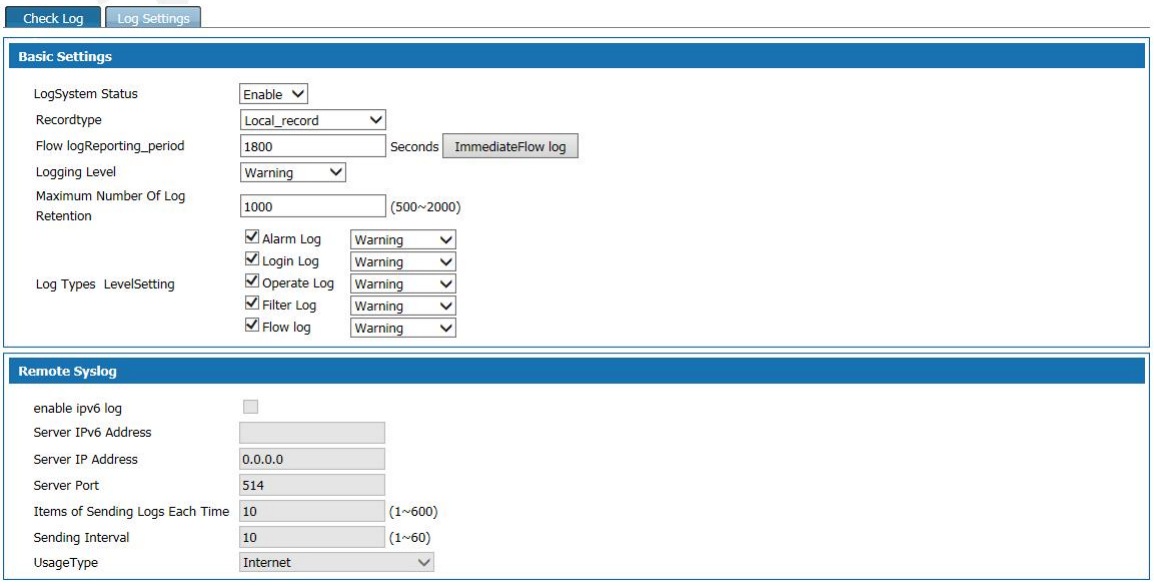


Figure7- 16 Log Manage - Log Settings

Log Settings page:

Table 7- 5 Log Settings

Item	Description
Basic Settings: Specify the log information to be displayed.	

Item	Description
RecordType	Specify the log type to be displayed. Select the radio button to display the corresponding log information.
Logging Level	Select to display the log information level, including "warning", "err", "crit", "alert", "emerg" five levels, the level of severity increases in order. Logs greater than or equal to the setting level are displayed.
Maximum number of log reservations	Set the maximum number of log reservations, the value range: 500 ~ 2000. When the number of system log reaches the set value, it will automatically delete the old log information according to the time of sending the log.
Remote Syslog: Set log upload information of remote server.	
Enable IPv6 Log	Check the radio button to enable IPv6 log function.
Server IPv6 address	IPv6 address of server which receives upload logs.
Server IP address	IP address of server which receives upload logs.
Server Port	Server-defined port which receives log upload. Value range: 0 ~ 65535 integer. Default: 514.
Items of sending logs each time	The number of logs sent to server each time. Value range: 1~ 600 integer.

8.Account Management

Before configuration,please select “Object” on top of the page,then enter into the object management page.

8.1 Object Management

Add users to user management and give users relevant business rights. When using the network U disk, SMS, VPN service, users with corresponding rights shall conduct identification, and the service can be used after the authentication. Select "object management > account" and enter the "object management" page as shown in figure 8-1.

Figure 8-1 account management page

Click the < add > button, and the "add account management" page pops up as shown in figure 8-2.

Figure 8-2 add account management

Add user management Settings as described below:

Interface items	Instruction
User Name	Set the user name
Password	Set the password
Retype	Retype the password
User level	Select "user admin" and log in the device as an ordinary user to configure the device; Select “business” and login to the device to see only the business configured for that account.
Services	The services the users can use, select the radio box can be.
Web permission	Select "enable" can log in the device through the Web

	management page; Select "disable" and "this user has no access to the page" pops up.
Status	Select "enable", the user can normally use; Select disable. This user is currently unavailable.

9.Product problem analysis

Why is the POWER indicator not on?

Answer: Check that the power adapter matches.

Please check whether the power connection is valid. Please check whether the power switch is on.

Why is the Ethernet (ETH) indicator not on?

Please check the network connection is correct or not.

Please check the network connection is reliable or not.

Why isn't the LAN indicator on the computer on?

Please check whether the type of cable from this product to the computer is correct.

Please check if the network connection is valid. Please check whether the computer network card indicator light is on. Please check whether the network card works normally:

The way to do this is to look at the device name under "network adapter" in Windows device manager. Whether with “?” Or "!" Symbols. If yes, please reinstall the device after deleting it, or change the network card to a new slot. If the problem persists, please replace the network card.

How to restore factory default Settings?

The steps to restore the factory default configuration are as follows:

Find the "RESET" button in the front panel of this product. Press the "RESET" button with the needle and hold it for more than 3 seconds, then release it.

Further Inquiry ?

During the use process,if you meet any configuration and using problem of the product,please dial to the customer service 0757-82288116 email to service@lvswitches.com for information.

In the contact process, you need to provide the equipment identification (the equipment identification can be obtained on the bottom label of the product, in the form of "XXXX XXXX XXXX").