VOIP ADAPTER USER GUIDE FTA5111

Version 1.0.0

Sep. 2021

Copyright

Trademark

Flyingvoice®, the logo and the name and marks are trademark of Flyingvoice Network Technology CO., LTD, which are registered legally in China, the United States, EU (European Union) and other countries.

All other trademarks belong to their respective owners. Without Flyingvoice's express written permission, recipient shall not reproduce or transmit any portion hereof in any form or by any means, with any purpose other than personal use.

Warranty

1. Warranty

The specifications and information regarding the products in this guide are subject to change without notice. all statements, information, and recommendations in this guide are believed to be accurate and presented without warranty of any kind, express or implied. users must take full responsibility for their application of products.

2. Disclaimer

Flyingvoice network technology co., ltd. makes no warranty of any kind with regard to this guide, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. Flyingvoice network technology co., ltd. shall not be liable for errors contained herein nor for incidental or consequential damages in connection with the furnishing, performance, or use of this guide.

3. Limitation of Liability

Flyingvoice and/or its respective suppliers are not responsible for the suitability of the information contained in this document for any reason. The information is provided "as is", and Flyingvoice does not provide any warranty and is subject to change without notice. All risks other than risks caused by use of the information are borne by the recipient. In no event, even if Flyingvoice has been suggested the occurrence of damages that are direct, consequential, incidental, special, punitive or whatsoever (Including but not limited to loss of business profit, business interruption or loss of business information), shall not be liable for these damages.

End User License Agreement

This End User License Agreement ("EULA") is a legal agreement between you and Flyingvoice. By installing, copying or otherwise using the Products, you: (1) agree to be bounded by the terms of this EULA, (2) you are the owner or an authorized user of the device, and (3) you represent and warrant that you have the right, authority and capacity to enter into this agreement and to abide by all its terms and conditions, just as if you had signed it. The EULA for this product is available on the Flyingvoice Support page for the product.

Patent Information

China, the United States, EU (European Union) and other countries are protecting one or more patents of accompanying products and/or patents being applied by Flyingvoice.

Technical Support

Visit www.flyingvoice.com for product documents and FAQ, or contact Flyingvoice by email at support@flyingvoice.com. We'll offer the help you need.

GNU GPL INFORMATION

Flyingvoice ATA firmware contains third-party software under the GNU General Public License (GPL). Flyingvoice uses software under the specific terms of the GPL. Please refer to the GPL for the exact terms and conditions of the license.

The original GPL license, source code of components licensed under GPL and used in Flyingvoice products can be downloaded online:

https://www.flyingvoice.com/download/gpl.html

Risk Warning Statement

This risk warning statement contains a summary of external network servers that FTA5111 will access under its factory settings in order to obtain necessary service support. If you want to prohibit these accesses based on security considerations, you can disable them through the web management page.

Number	Server Domain Name	Description	Factory Setting
1	https://prv3.flyingvoice.net:442	Flyingvoice Provision web management configuration server	Disable
2	http://acs3.flyingvoice.net:8080	Flyingvoice TR069 web management server	Disable
3	clock.fmt.he.net	NTP server	Enable
4	cn.pool.ntp.org	NTP Secondary server	Enable

Table of Contents

About This Guide

Thank you for choosing Flyingvoice FTA5111, which will allow you to make ATA call using your broadband connection.

This guide provides everything you need to quickly use your new ATA. Firstly, verify with your system administrator that the IP network is ready for ATA configuration. Also be sure to read the Quick Start Guide which can be found in your ATA package before you set up and use the IP ATA. As you read this guide, keep in mind that some features are configurable by your system administrator or determined by your ATA environment. As a result, some features may not be enabled or may operate differently on your ATA. Additionally, the examples and graphics in this guide may not directly reflect what is displayed or is available on your ATA screen.

Related Documents

The following types of related documents are available on each page:

- Datasheet
- Quick start guide

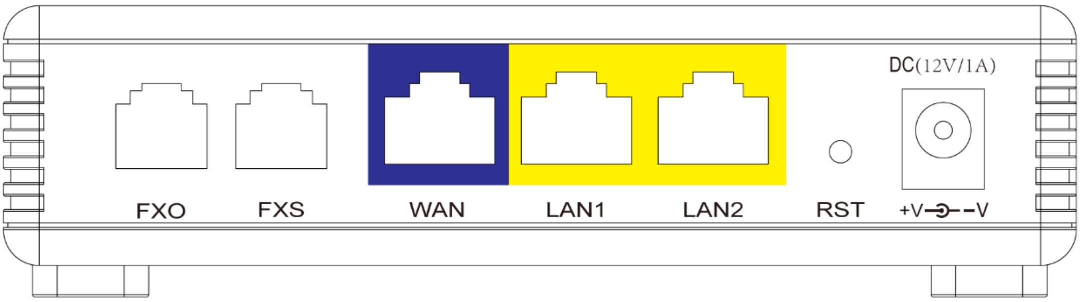
Getting Started with Your ATA

This chapter provides the overview of ATA hardware, and how to navigate your ATA for the best performance.

Hardware Overview

Topics

FTA5111 Hardware



NO.	Item	Description
1	DC (12V1A)	Power adapter interface
2	LAN1-LAN2	Local Area Network interface, connect RJ45 cable
3	WAN	Wide Area Network interface, connect RJ45 cable
4	FXS	FXS port, connect RJ11 cable
5	FXO	FXO port, connect RJ11 cable

LED Indicator

The LED indicator indicates the call, message and ATA's system status.

LED	LED Status	Description
Power	ON(GREEN)	Powered on

	OFF	Powered off
WAN	ON(GREEN)	Connected (Data), running as active WAN
	On Blinking (GREEN)	Connected (Registered)
	OFF	Disconnected/Power off
FXS	ON(GREEN)	Connected (Registered)
	On Blinking (GREEN)	Connected (Data)
	OFF	Disconnected/Register fail
FXO	ON(GREEN)	Connected (Registered)
	On Blinking (GREEN)	Connected (Data)
	OFF	Disconnected/Register fail

Hardware Installation

Before configuring your ATA, please see the procedure below for instructions on connecting the device in your network.

1. Connect analog phone to FXS Port with a RJ11 cable.
2. Connect the WAN port to your ISP’s ATA/switch with a RJ45 cable.
3. Connect one end of the power cord to the power port of the device. Connect the other end to the wall outlet.
4. Check the device LED to confirm network connectivity.

Warning

Please do not attempt to unsupported power adapters and do not remove power during configuring or updating the device. Using other power adapters may damage the device and will void the manufacturer warranty.

Warning

Changes or modifications not expressly approved by the party responsible for compliance can void the user's authority to operate the equipment.

This equipment has been tested and found to comply with the limits for a Class B digital device, pursuant to Part 15 of the FCC Rules. These limits are designed to provide reasonable protection against harmful interference in a residential installation. This equipment generates, uses and can radiate radio frequency cause harmful interference to radio communications. However, there is no energy and, if not installed and used in accordance with the instructions, may guarantee that interference will not occur in a particular installation.

If this equipment does cause harmful interference to radio or television reception, which can be determined by turning the equipment off and on, the user is encouraged to try to correct the interference by one or more of the following measures:

- Reorient or relocate the receiving antenna.
- Increase the separation between the equipment and receiver.
- Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.
- Consult the dealer or an experienced radio/TV technician for help.

Documents

Name	Content	Location	Language
Quick Guide	Basic functions and customization	Package	CN/EN
		Flyingvoice Official website	CN/EN
User Guide	Web setting and advanced functions	Flyingvoice Official website	CN/EN

Basic Features

You can use the ATA to make a place and answer calls, ignore incoming calls, transfer a call to someone else, conduct a conference call and perform other basic call features.

Topics

ATA initialization

After the ATA is powered on, the following steps will be performed:

1. Please make sure that the network cable connected to the adapter can access the Internet normally, and the adapter is in DHCP mode by default

2. Please connect the LAN port of the device to the computer. After the connection is successful, the computer will obtain the IP of 192.168.1.x and can access the Internet normally

Note: If the ATA cannot obtain the network configuration through the DHCP server, please perform the basic network settings in section 2.3 on page 11.

ATA Status

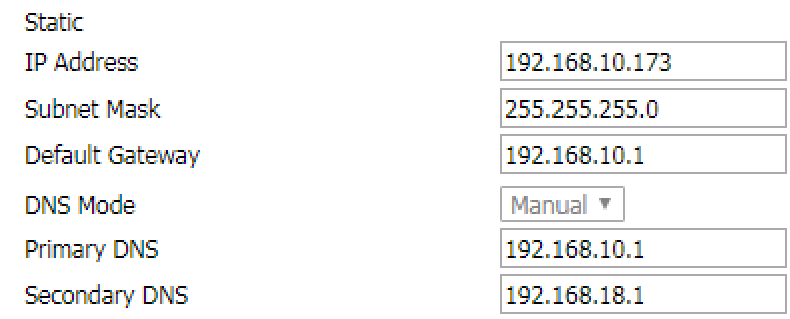
You can check the ATA status through the adapter web interface. The status information of the adapter includes:

1. Network status (currently active uplink status, etc.)
2. IPv4 address length is 32 bits
3. Device information (product name, hardware version, firmware version, product serial number, MAC address)
4. Account information (registered information for SIP account)

Basic Network Setting

Static IP

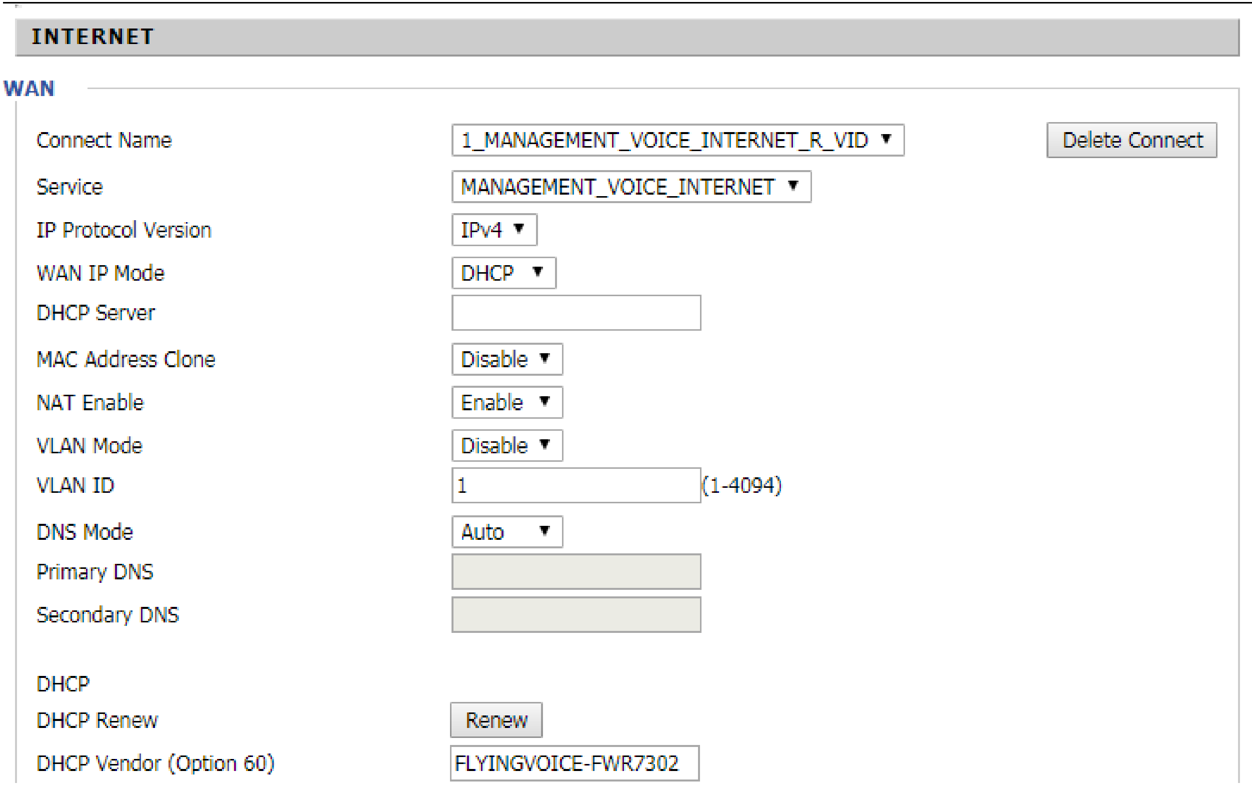
This configuration may be utilized when a user receives a fixed public IP address or a public subnet, namely multiple public IP addresses from the Internet providers. In most cases, a Cable service. provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you can assign an IP address to the WAN interface.



Field Name	Description
IP Address	The IP address of Internet port
Subnet Mask	The subnet mask of Internet port
Default Gateway	The default gateway of Internet port
DNS Mode	Select DNS mode, options are Auto and Manual: 1. When DNS mode is Auto, the device under LAN port will automatically obtain the preferred DNS and alternate DNS 2. When DNS mode is Manual, the user manually configures the preferred DNS and alternate DNS information
Primary DNS Address	The primary DNS of Internet port
Secondary DNS Address	The secondary DNS of Internet port

DHCP

The ATA has a built-in DHCP server that assigns private IP address to each local client.
The DHCP feature allows to the ATA to obtain an IP address automatically from a DHCP server. In this case, it is not necessary to assign an IP address to the client manually.

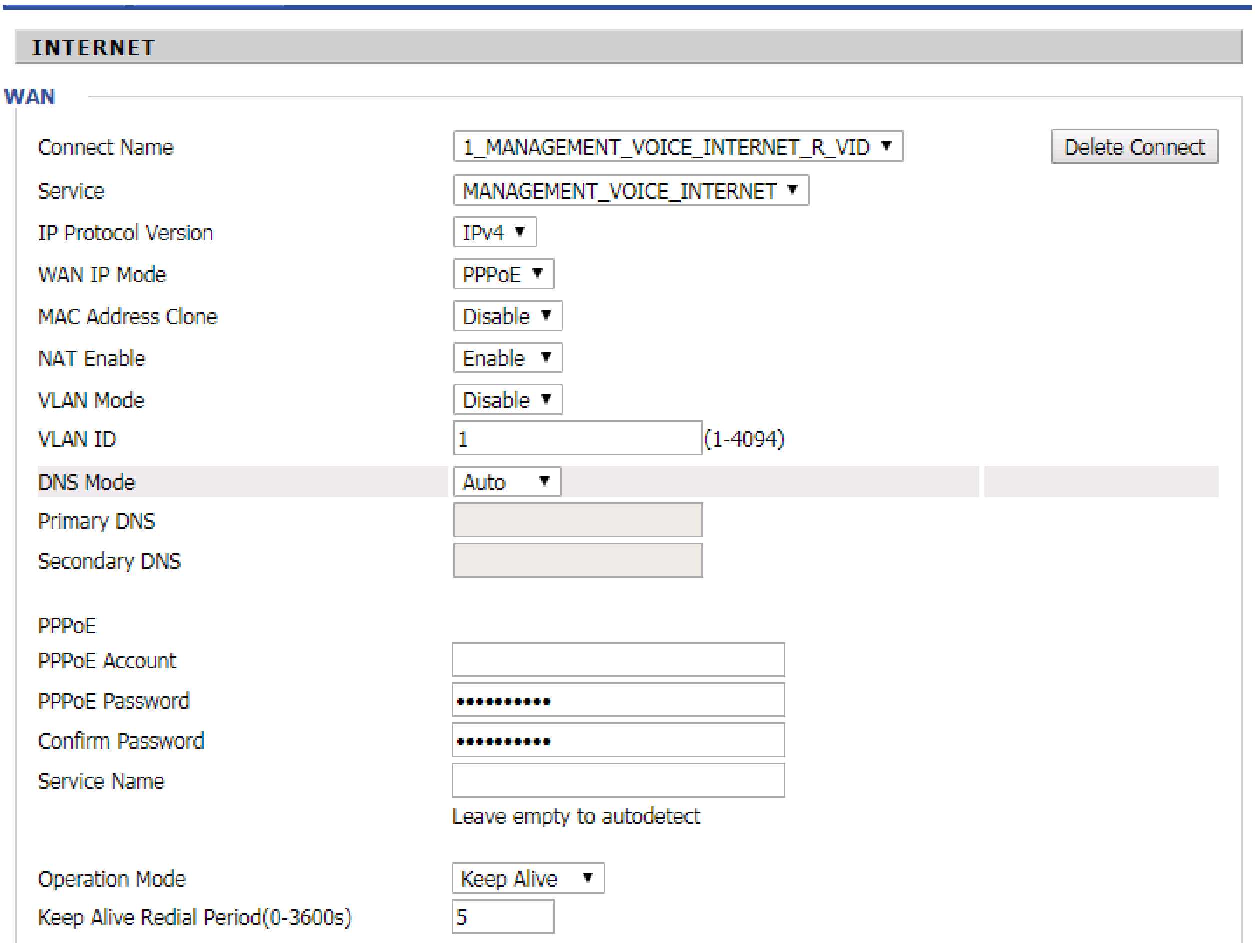


Field Name	Description
DNS Mode	Select DNS mode, options are Auto and Manual: When DNS mode is Auto, the device under LAN port will automatically obtain the preferred DNS and alternate DNS. When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS.
Primary DNS Address	Primary DNS of Internet port.
Secondary DNS Address	Secondary DNS of Internet port.
DHCP Renew	Refresh the DHCP IP address.
DHCP Vendor (Option60)	Specify the DHCP Vendor field. Display the vendor and product name.

PPPoE

PPPoE stands for Point-to-Point Protocol over Ethernet. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection.

PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.



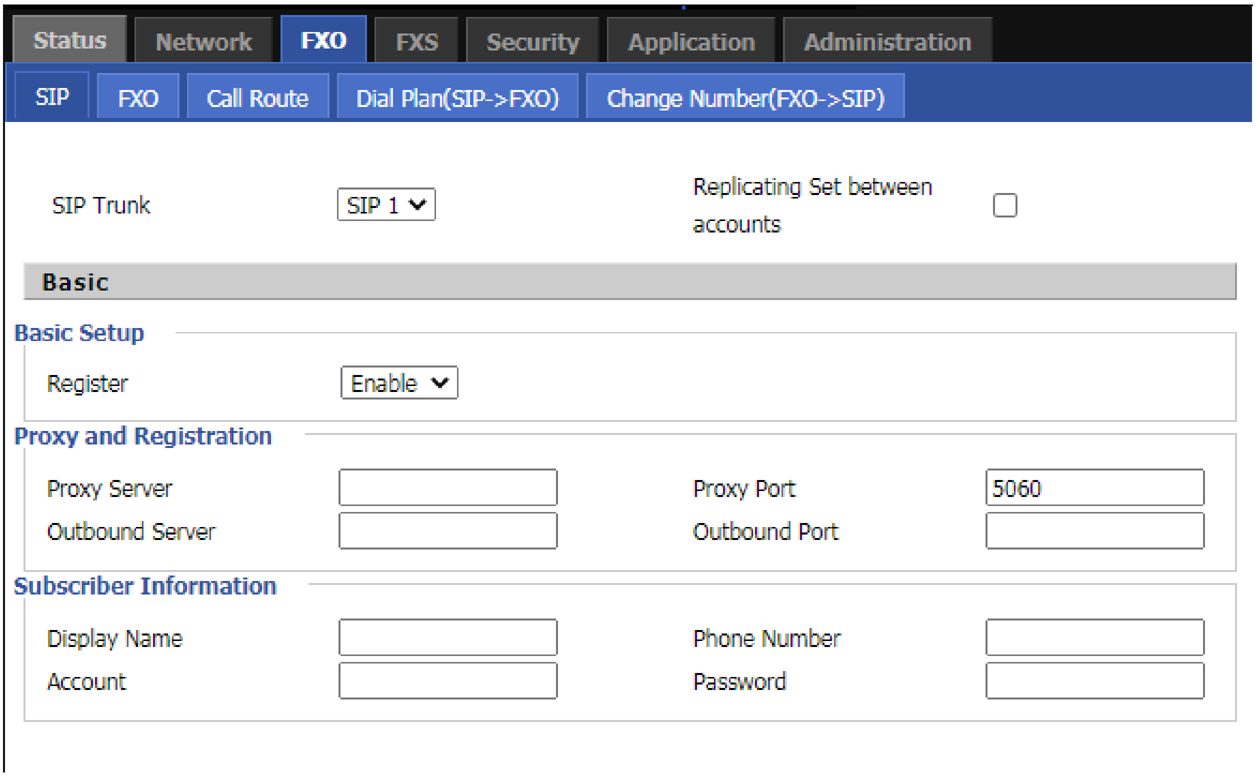
Field Name	Descriptio
PPPoE Account	Enter a valid user name provided by the ISP.
PPPoE Password	Enter a valid password provided by the ISP. The password can contain special characters and allowed special characters are $, +, *, #, @ and !. For example, the password can be entered as #net123@IT!$+*

Confirm Password	Enter your PPPoE password again.
Service Name	Enter a service name for PPPoE authentication. If it is left empty, the service name is auto detected.
Operation Mode	Select the mode of operation, options are Keep Alive, On Demand and Manual: When the mode is Keep Alive, the user sets the “keep alive redial period” values range from 0 to 3600s, the default setting is 5 minutes; When the mode is On Demand, the user sets the 'on demand idle time' value in the range of 0-60 minutes, the default setting is 5 minutes;  When the mode is Manual, there are no additional settings to configure.
Keep Alive Redial	Set the interval to send Keep Alive messaging.
PPPoE Account	Assign a valid user name provided by the ISP.

Configuring SIP trunk

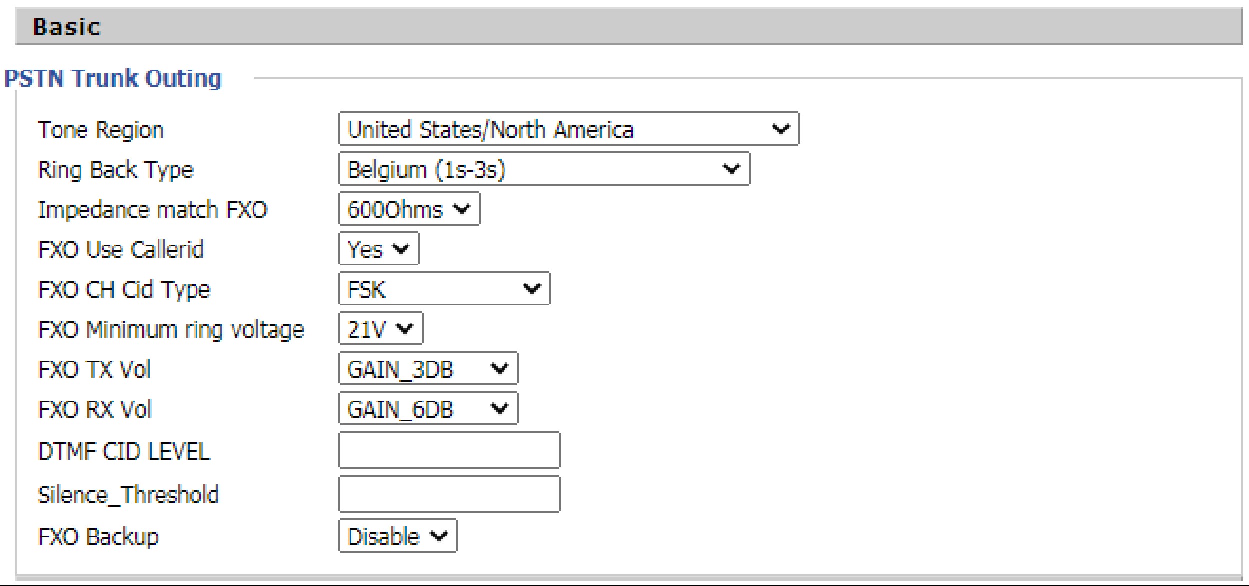
FTA5111 support forward call between SIP trunk and FXO.

SIP trunk register



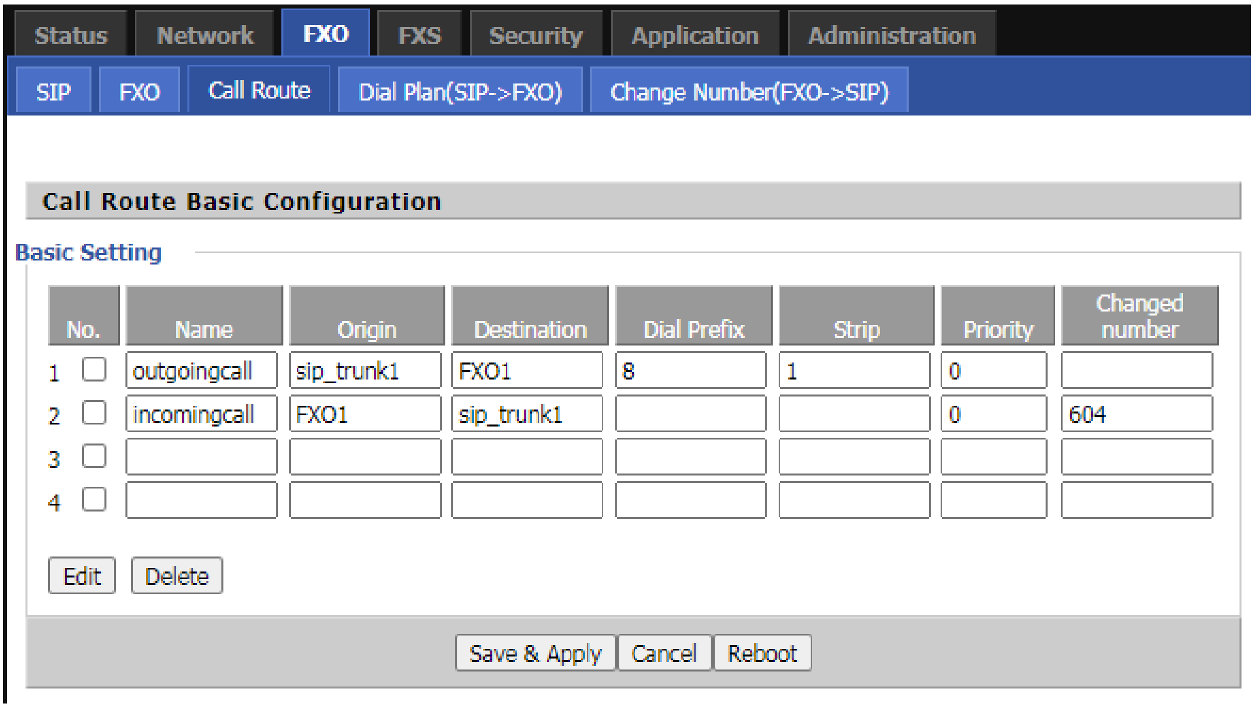
Procedure	
1.	Navigate to the FXO/SIP Account web page.
2.	Input the SIP Server address and SIP Server port number (from server provider) into parameters: Proxy Server and Proxy Port.
3.	Input account details received from your administrator into Display Name, Phone Number and Account details.
4.	Type the password received from your administrator into the Password parameter.
5.	Press Save button in the bottom of the web page to save changes.
6.	Press Reboot button in the bottom of the web page to make setting effective.
7.	Navigate to Status page check register status.

PSTN setting

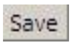


Field Name	Description
Tone Region	Used to match gateway's tone region setting for DTMF CID detect
Ring Back Type	Used to match gateway's ring back type for DTMF CID detect
Impedance match FXO	FXO impedance setting
FXO Use Callerid	FXO CID enable/disable
FXO CH Cid Type	FXO CID type setting: FSK or DTMF
FXO Minimum ring	FXO ring voltage setting
FXO TX Vol	FXO volume gain setting
FXO RX Vol	FXO volume gain setting
DTMF CID LEVEL	DTMF energy setting, when DTMF CID LEVEL > Silence_Threshold, device will detect DTMF CID number
Silence_Threshold	Device default energy setting
FXO Backup	FXO backup setting, enable, FXO1 and FXO2 are backup for each other

Call Route



Procedure

1. Navigate to the FXO/Call Route web page.
2. Add call route: call is from SIP trunk1, need forward to FXO1, please refer to call route 1 like picture.
3. Please note: when setting call route from SIP trunk to FXO, change number is not mandatory, but the call from FXO to SIP trunk, you must input change number, this means the call from FXO only could forward to change number.
4. Press 

button in the bottom of the web page to save changes.
5. Press 

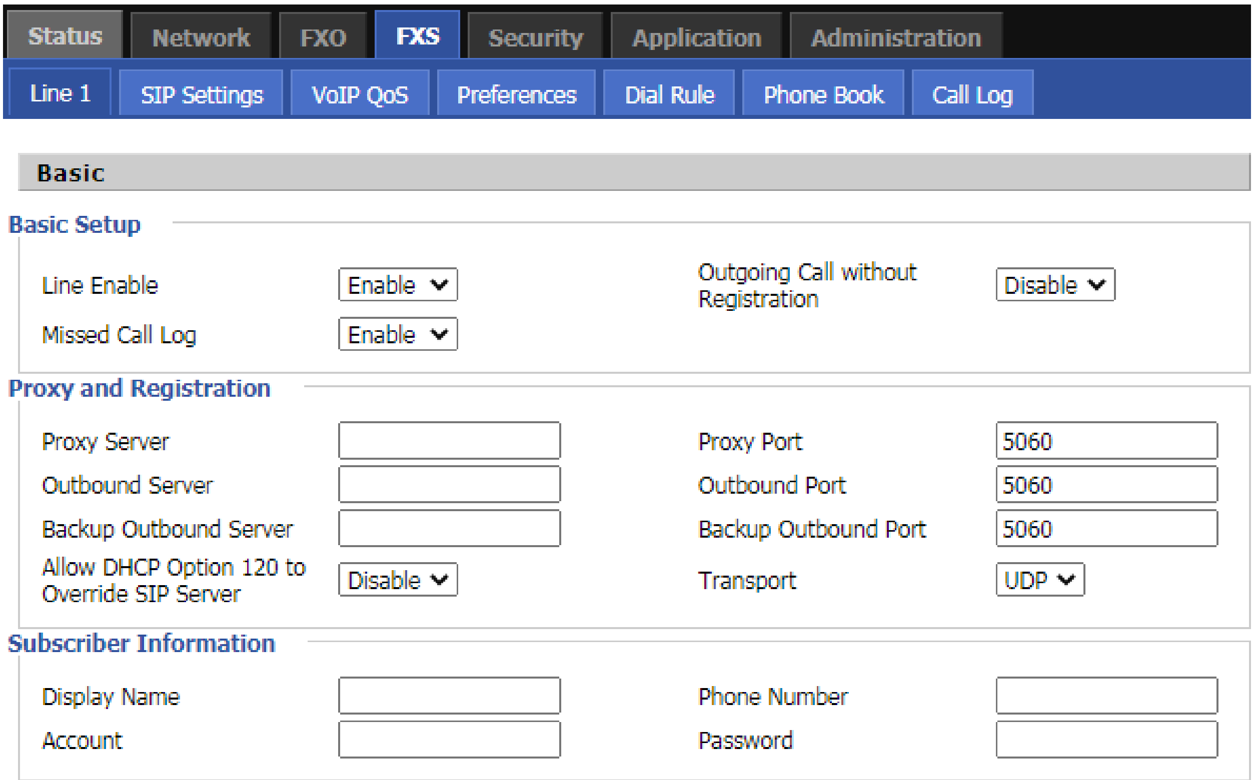
button in the bottom of the web page to make setting effective.
6. Navigate to Status page check register status.

Configuring FXS

SIP Accounts

The device support 2 FXS ports to make SIP (Session Initiation Protocol) calls. Before registering, the device user should have a SIP account configured by the system administrator or provider. See the section below for more information.

Configuring SIP via the Web Management Interface



Procedure
1. Navigate to the FXS1/SIP Account web page.
2. Input the SIP Server address and SIP Server port number (from server provider) into parameters: Proxy Server and Proxy Port.
3. Input account details received from your administrator into Display Name, Phone Number and Account details.
4. Type the password received from your administrator into the Password parameter.
5. Press Save button in the bottom of the web page to save changes.
6. Press Reboot button in the bottom of the web page to make setting effective.
7. Navigate to Status page check register status.

Basic Calls

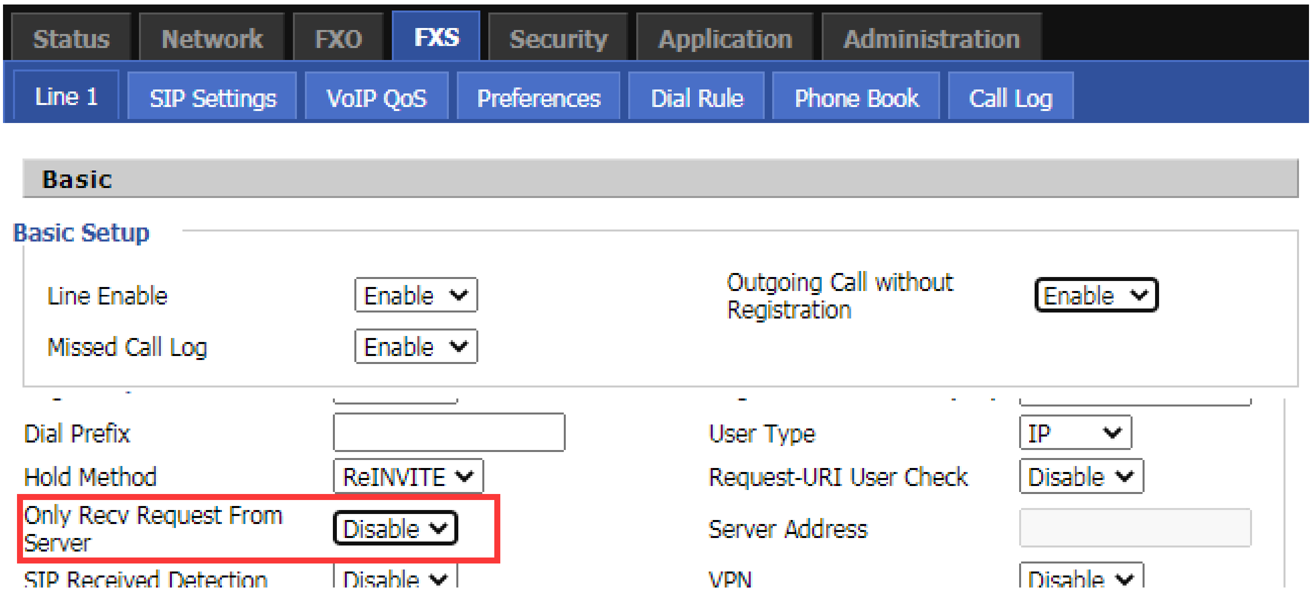
To make basic calls:

- Caller and callee register to same SIP server.
- To make a call, caller pick up the analog phone or turn on the speaker on the analog phone, caller will hear dial tone.
- Then input callee's phone number with # at the end.
- Callee will start ringing, pick up to answer the call.
- For example: caller number is 601, callee is 601, caller press 601#, callee will start ringing.

Directly IP calls

Direct IP calling allows two analog phones to talk to each other without SIP server.

- Please make sure both ATA which analog phone connected could ping each other from WAN port.
- Enable Outgoing Call without Registration in FXS--SIP Account page.
- Disable Only Recv Request from Server in FXS--SIP Account---SIP Advanced Setup part.
- Caller pick up the analog phone or turn on the speakerphone on the analog phone, input the callee's IP address directly, with the end "#".
- Callee will start ringing, pick up to answer the call.



Call Hold

- During a call connection, party A pressing the "*77" to put the call on hold, then part A will hear the dial tone and the party B will hear hold tone at the same time.
- Party A pressing the "*77" again to release the previously hold status and resume the bi-directional media.

Blind Transfer

- Assume that call party A and B are in a conversation, party A wants to transfer this call to C.
- Party A dials "*98" to get a dial tone, then dial party C's number.
- Party A can hang up. Party C will start ringing, pick up will talk to part B.

Attended Transfer

- Assume that call party A and B are in a conversation. A wants to transfer this call to C.
- Party A press "*77" to hold the party B, when hear the dial tone, A dials C's number, then party A and party C are in conversation.
- Party A press "*98" to transfer to C, then B and C will be in a conversation.
- If the transfer is not completed successfully, then A and B are in conversation again.

Conference

- Assume that call party A and B are in a conversation. A wants to add C to the conference.
- Party A dials "*77" to hold the party B, when hear the dial tone, A dial C's number, then party A and party C are in conversation.
- Party A dials "*88" to add C, then A and B, and C will be in a conference.

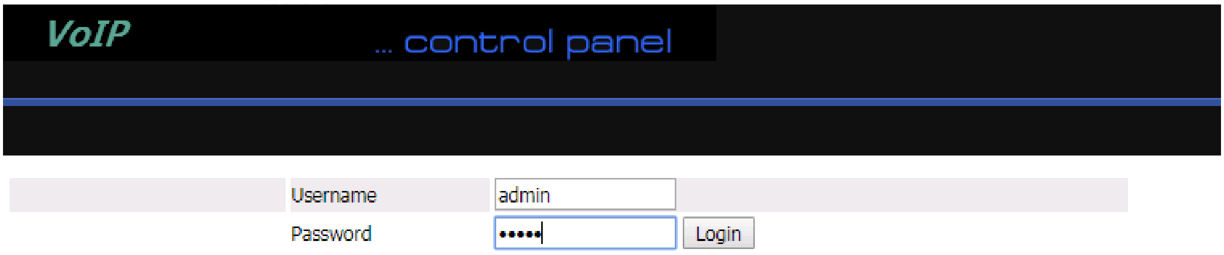
Advanced Web Configuration

This chapter guides users to execute advanced (full) configuration through admin mode operation.

Topics:

Login
Status
Network
FXO
FXS
Security
Application
Administration

Login

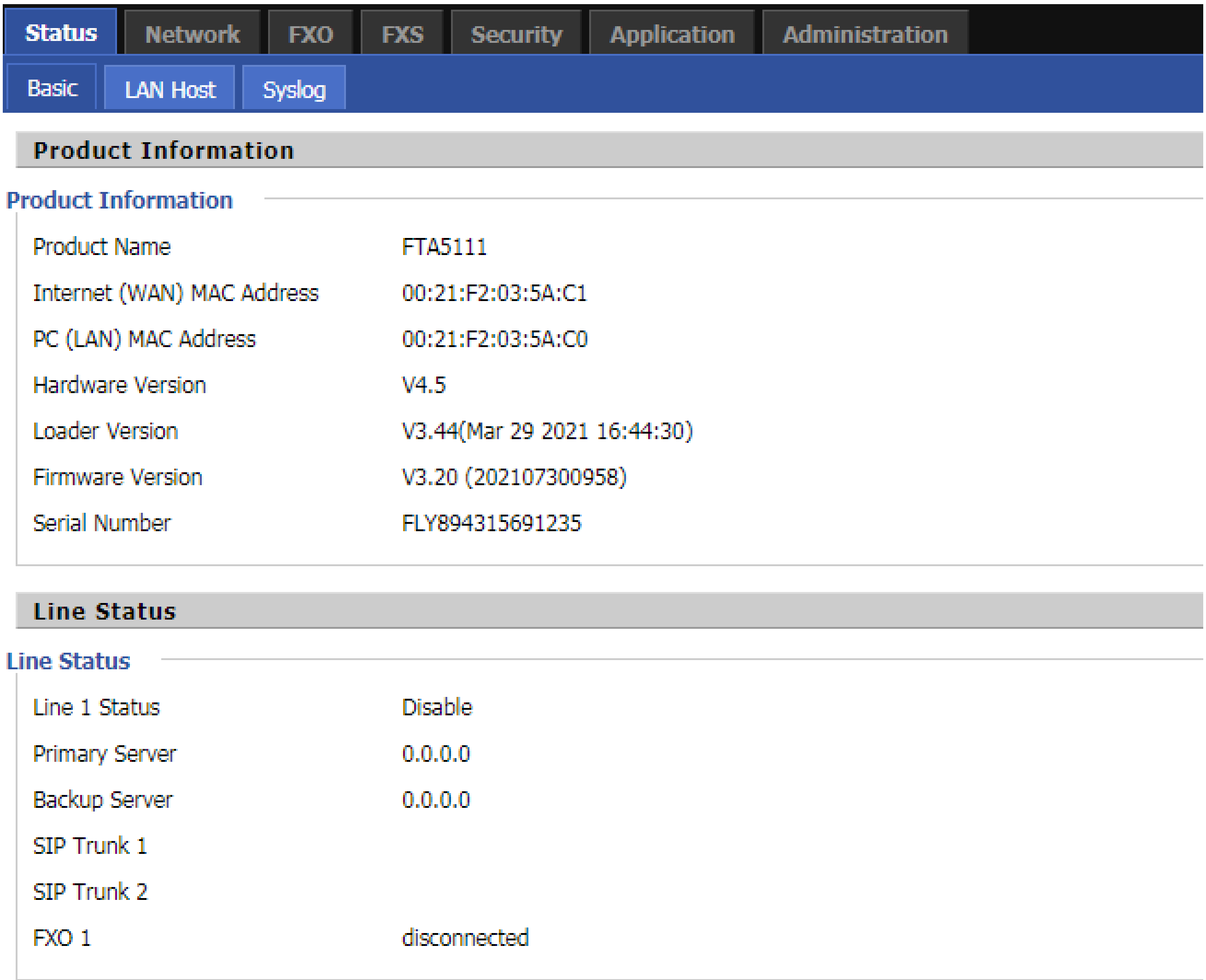


Procedure	
1.	Connect the LAN port of the ATA to your PC an Ethernet cable.
2.	Open a web browser on your PC and type http://192.168.1.1.
3.	Enter Username admin and Password admin.
4.	Click Login.

Status

This webpage shows the status information about the Product, Network, and System including Product Information, SIP Account Status, FXS Port Status, Network Status. Wireless Info and System Status.

System status


Status
Network
FXO
FXS
Security
Application
Administration
Basic
LAN Host
Syslog
Product Information
Product Information
Product Name FTA5111
Internet (WAN) MAC Address 00:21:F2:03:5A:C1
PC (LAN) MAC Address 00:21:F2:03:5A:C0
Hardware Version V4.5
Loader Version V3.44(Mar 29 2021 16:44:30)
Firmware Version V3.20 (202107300958)
Serial Number FLY894315691235
Line Status
Line Status
Line 1 Status Disable
Primary Server 0.0.0.0
Backup Server 0.0.0.0
SIP Trunk 1
SIP Trunk 2
FXO 1 disconnected

Network Status

Ethernet WAN Port Status

WAN Port Status	Link Down
Connection Type	
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	
Link-local IPv6 Address	fe80::221:f2ff:fe03:5ac1/64
IPv6 PD Prefix	
IPv6 Domain Name	
IPv6 Primary DNS	
IPv6 Secondary DNS	
WAN Down Speed	0B/s
WAN Upload Speed	0B/s

VPN Status

VPN Type	Disable
Initial Service IP	
Virtual IP Address	

LAN Port Status

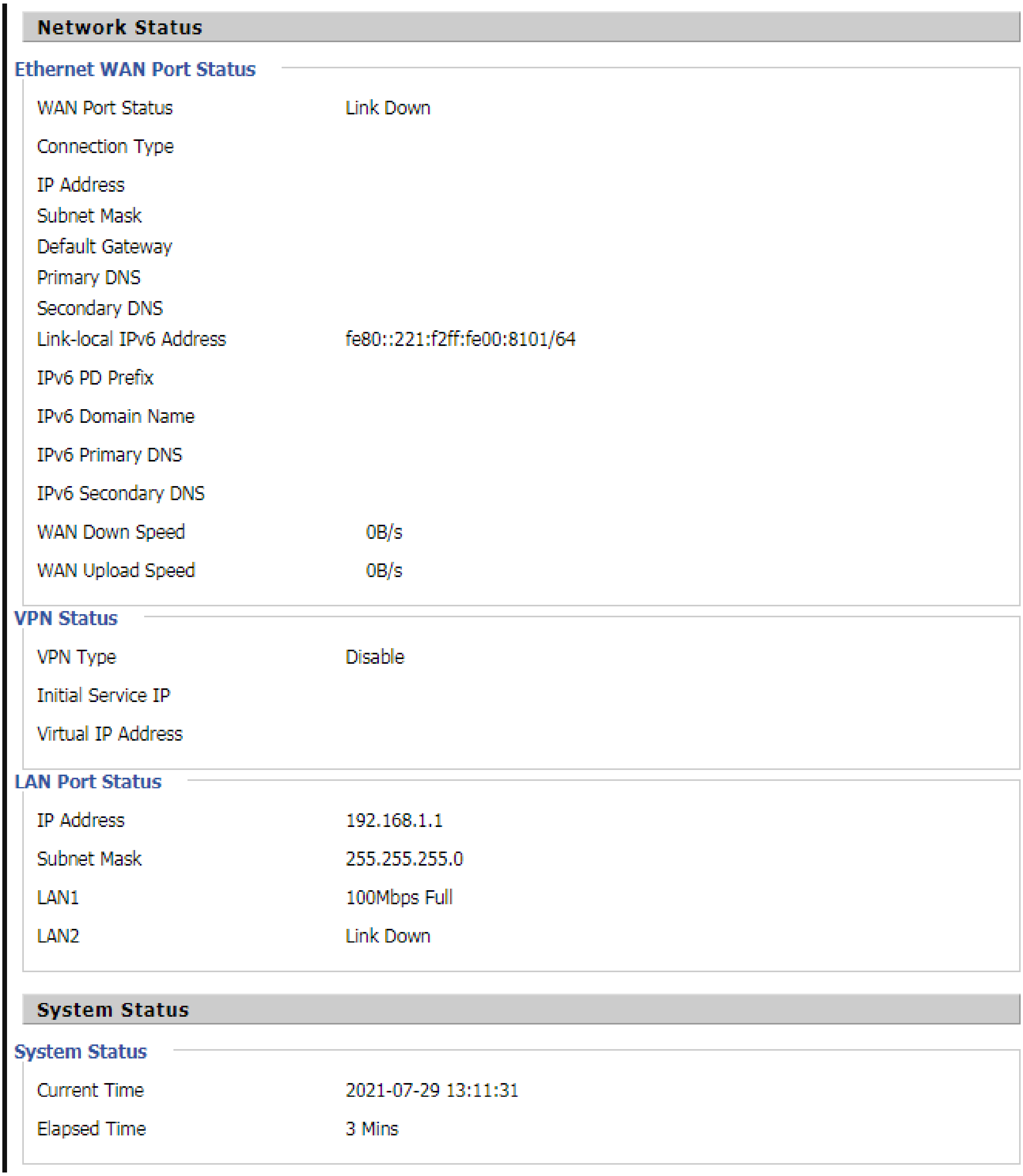
IP Address	192.168.1.1
Subnet Mask	255.255.255.0
LAN1	100Mbps Full
LAN2	Link Down

System Status

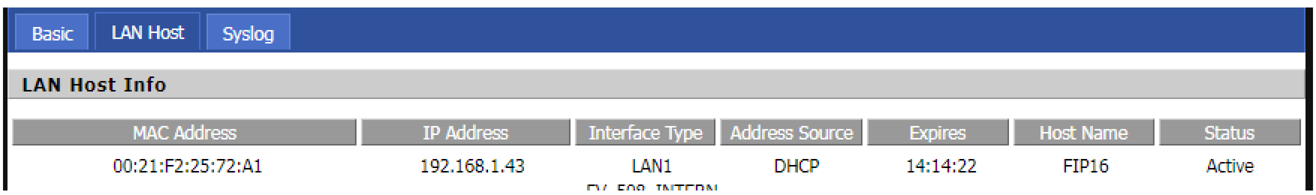
System Status

Current Time	2021-07-30 02:32:14
Elapsed Time	34 Mins

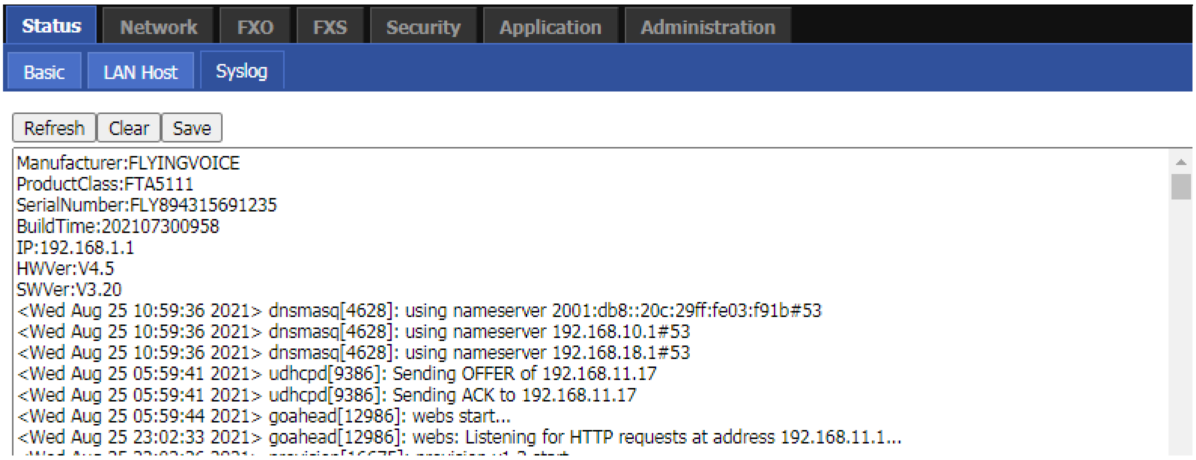
Refresh



LAN Host



System Log



Description
If you enable the system log in Status/syslog webpage, you can view the system log in this. webpage.

Network

You can configure the WAN port, LAN port, DDNS, Multi WAN, DMZ, Port Forward and other parameters in this section of the web management interface.

Topics

WAN

LAN

VPN

DMZ

DDNS

QoS

Port Setting

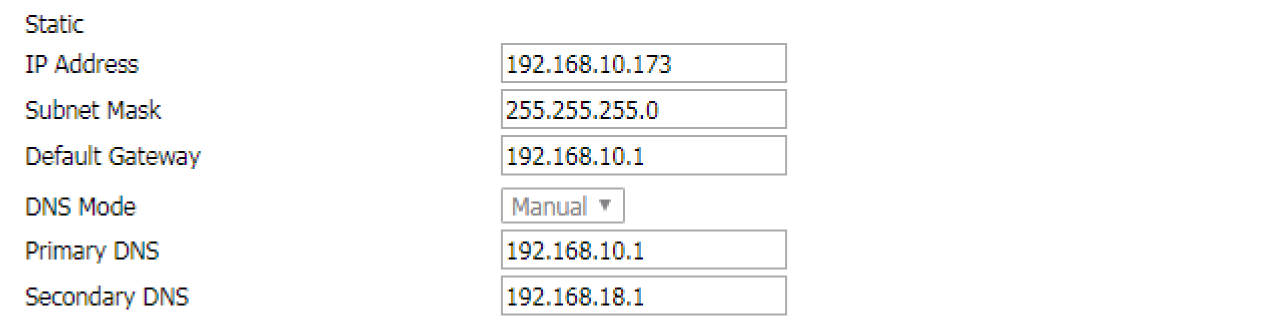
Advanced

WAN

This page allows you to set WAN configuration with different modes. Use the Connection Type drop down list to choose one WAN mode and then the corresponding page will be displayed.

Static IP

This configuration may be utilized when a user receives a fixed public IP address or a public subnet, namely multiple public IP addresses from the Internet providers. In most cases, a Cable service provider will offer a fixed public IP, while a DSL service provider will offer a public subnet. If you have a public subnet, you can assign an IP address to the WAN interface.

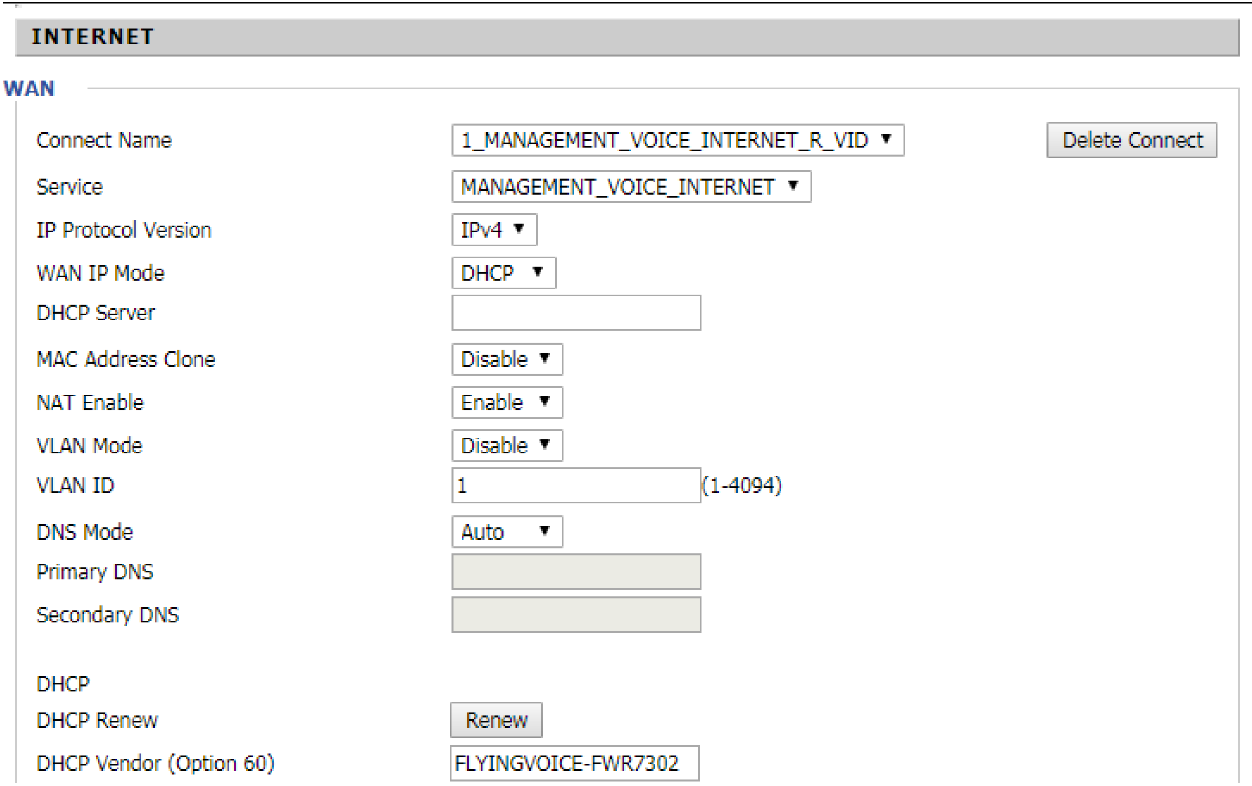


Field Name	Description
IP Address	The IP address of Internet port
Subnet Mask	The subnet mask of Internet port
Default Gateway	The default gateway of Internet port
DNS Mode	Select DNS mode, options are Auto and Manual: 3. When DNS mode is Auto, the device under LAN port will automatically obtain the preferred DNS and alternate DNS 4. When DNS mode is Manual, the user manually configures the preferred DNS and alternate DNS information
Primary DNS Address	The primary DNS of Internet port
Secondary DNS Address	The secondary DNS of Internet port

DHCP

The ATA has a built-in DHCP server that assigns private IP address to each local client.

The DHCP feature allows to the ATA to obtain an IP address automatically from a DHCP server. In this case, it is not necessary to assign an IP address to the client manually.

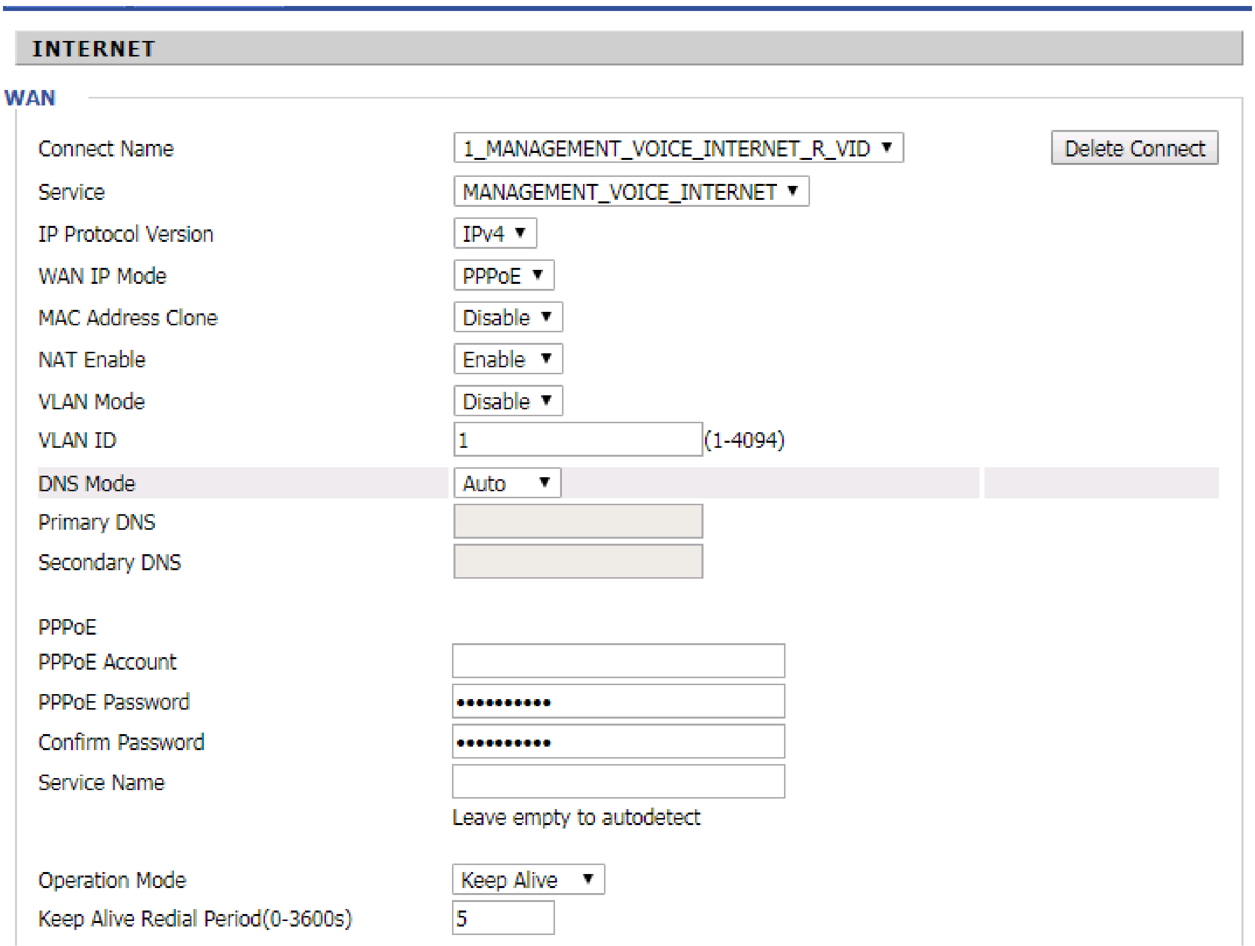


Field Name	Description
DNS Mode	Select DNS mode, options are Auto and Manual: When DNS mode is Auto, the device under LAN port will automatically obtain the preferred DNS and alternate DNS. When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS.
Primary DNS Address	Primary DNS of Internet port.
Secondary DNS Address	Secondary DNS of Internet port.
DHCP Renew	Refresh the DHCP IP address.
DHCP Vendor (Option60)	Specify the DHCP Vendor field. Display the vendor and product name.

PPPoE

PPPoE stands for Point-to-Point Protocol over Ethernet. It relies on two widely accepted standards: PPP and Ethernet. It connects users through an Ethernet to the Internet with a common broadband medium, such as a single DSL line, wireless device or cable modem. All the users over the Ethernet can share a common connection.

PPPoE is used for most of DSL modem users. All local users can share one PPPoE connection for accessing the Internet. Your service provider will provide you information about user name, password, and authentication mode.

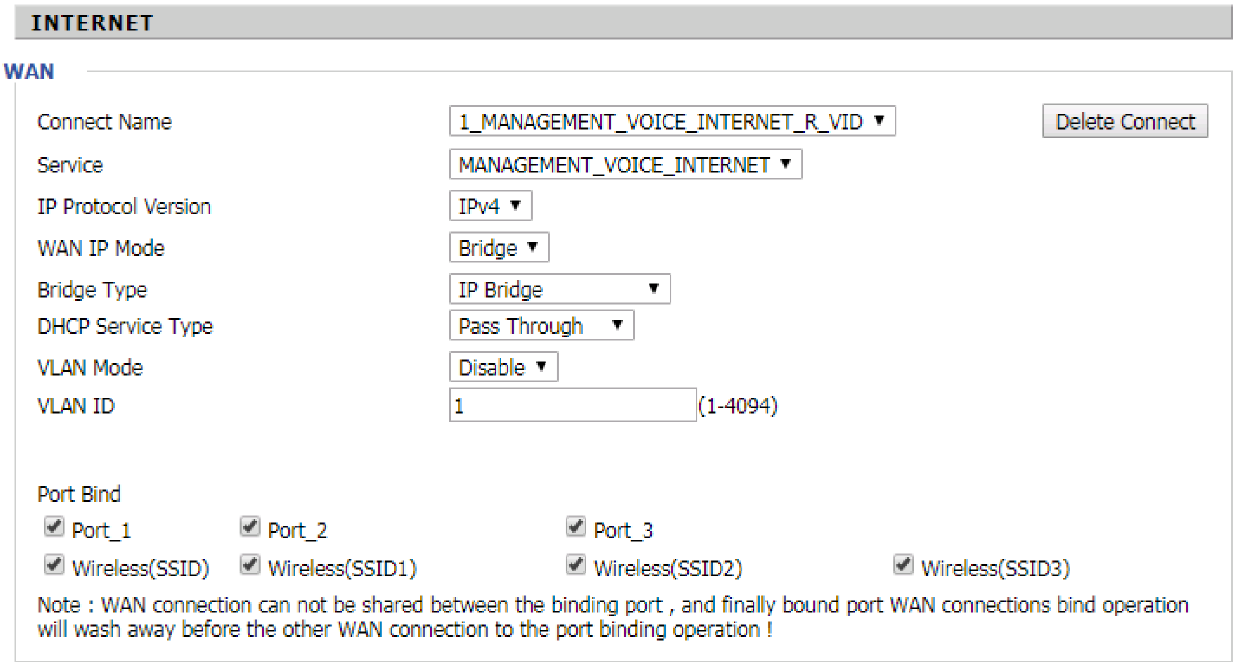


Field Name	Descriptio
PPPoE Account	Enter a valid user name provided by the ISP.
PPPoE Password	Enter a valid password provided by the ISP. The password can contain special characters and allowed special characters are $, +, *, #, @ and ! For example, the password can be entered as #net123@IT!$+*.

Confirm Password	Enter your PPPoE password again.
Service Name	Enter a service name for PPPoE authentication. If it is left empty, the service name is auto detected.
Operation Mode	Select the mode of operation, options are Keep Alive, On Demand and Manual: When the mode is Keep Alive, the user sets the 'keep alive redial period' values range from 0 to 3600s, the default setting is 5 minutes; When the mode is On Demand, the user sets the 'on demand idle time' value in the range of 0-60 minutes, the default setting is 5 minutes;  When the mode is Manual, there are no additional settings to configure.
Keep Alive Redial	Set the interval to send Keep Alive messaging.
PPPoE Account	Assign a valid user name provided by the ISP.

Bridge Mode

Bridge Mode under Multi WAN is different with traditional bridge setting. Bridge mode employs no IP addressing and the device operates as a bridge between the WAN port and the LAN port. Route Connection has to be built to give IP address to local service on device.



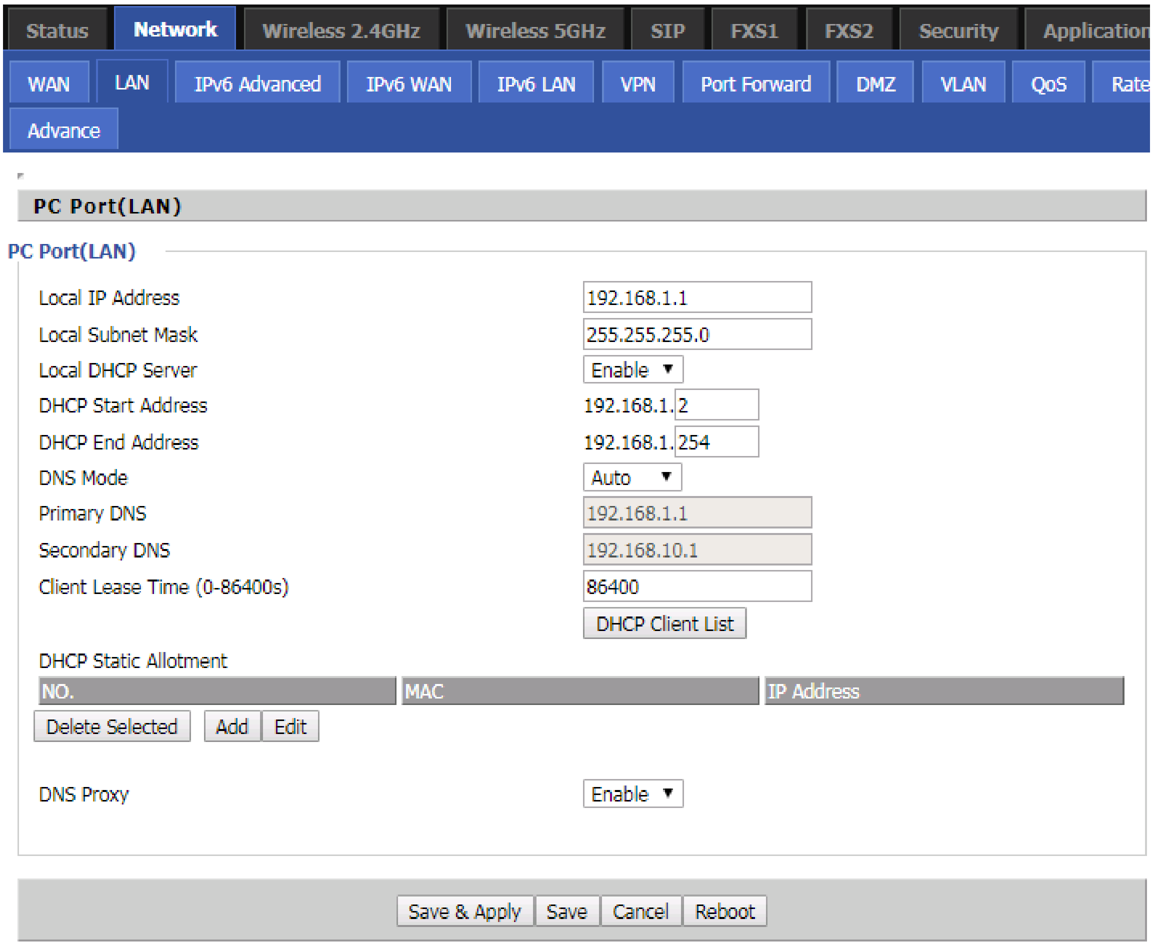
Field Name	Descriptio
Bridge Type	
IP Bridge	Allow all Ethernet packets to pass. PC can connect to upper network directly.
PPPoE Bridge	Only Allow PPPoE packets pass. PC needs PPPoE dial-up software.
Hardware IP Bridge	Packets pass through hardware switch with wired speed. Does not support wireless port binding.
DHCP Service Type	
Pass Through	DHCP packets can be forwarded between WAN and LAN, DHCP server in gateway will not allocate IP to clients of LAN port.
DHCP Snooping	When gateway forwards DHCP packets from LAN to WAN it will add option82 to DHCP packet, and it will remove option82 when forwarding.

	DHCP packet from the WAN interface to the LAN interface. Local DHCP service will not allocate IP to clients of LAN port.
Local Service	Gateway will not forward DHCP packets between LAN and WAN, it also blocks DHCP packets from the WAN port. Clients connected to the LAN port can get IP from DHCP server run in gateway.
VLAN Mode	
Disable	The WAN interface is untagged. LAN is untagged.
Enable	The WAN interface is tagged. LAN is untagged.
Trunk	Only valid in bridge mode. All ports, including WAN and LAN, belong to this VLAN Id and all ports are tagged with this VLAN id. Tagged packets can pass through WAN and LAN.
VLAN ID	Set the VLAN ID. **Note** Multiple WAN connections may be created with the same VLAN ID.
802.1p	Set the priority of VLAN, Options are 0~7.

LAN

LAN Port

NAT translates the packets from public IP address to local IP address to forward packets to the proper destination.

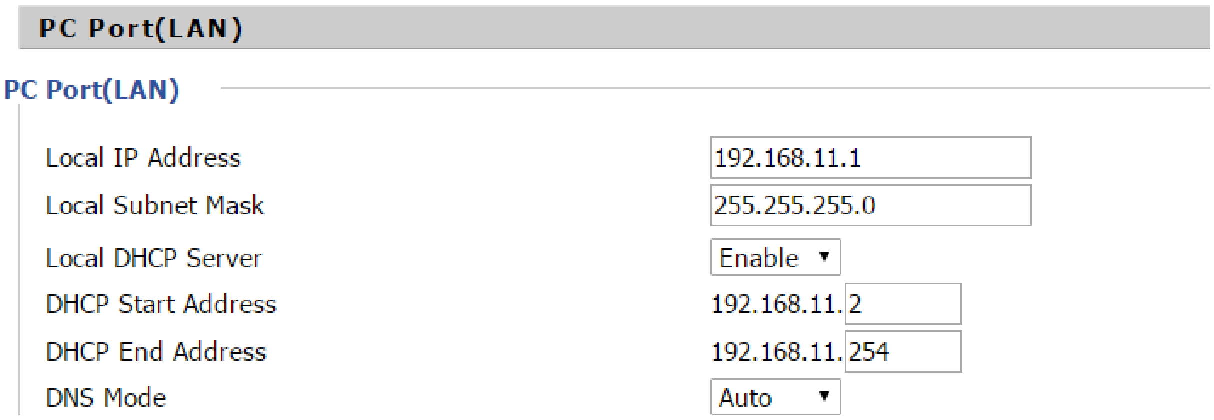


Field Name	Description
IP Address	Enter the IP address of the ATA on the local area network. All the IP addresses of the computers which are in the ATA's LAN must be in the same network segment with this address, and the default gateway of the computers must be this IP address. (The default is 192.168.11.1).
Local Subnet Mask	Enter the subnet mask to determine the size of the network (default is 255.255.255.0/24).
Local DHCP Server	Enable/Disable Local DHCP Server.

DHCP Start Address	Enter a valid IP address as a starting IP address of the DHCP server, and if the ATA's LAN IP address is 192.168.11.1, starting IP address can be 192.168.11.2 or greater, but should be less than the ending IP address.
DHCP End Address	Enter a valid IP address as an end IP address of the DHCP server.
DNS Mode	Select DNS mode, options are Auto and Manual: When DNS mode is Auto, the device under LAN port will automatically obtains the preferred DNS and alternate DNS. When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS.
Primary DNS	Enter the preferred DNS address.
Secondary DNS	Enter the secondary DNS address.
Client Lease Time	This option defines how long the address will be assigned to the computer within the network. In that period, the server does not assign the IP address to the other computer.
DNS Proxy	Enable or disable; If enabled, the device will forward the DNS request of LAN-side network to the WAN-side network.

DHCP Server

The ATA has a built-in DHCP server that assigns private IP address to each local client. DHCP stands for Dynamic Host Configuration Protocol. The ATA, by factory default acts a DHCP server for your network so it automatically dispatches related IP settings to any local user configured as a DHCP client. It is highly recommended that you leave the ATA enabled as a DHCP server if you do not have a DHCP server for your network.



Field Name	Description
Local DHCP Server	Enable/Disable DHCP server.
DHCP Start Address	Enter a value of the IP address pool for the DHCP server to start with when issuing IP addresses.
DHCP End Address	Enter a value of the IP address pool for the DHCP server to end with when issuing IP addresses.
DNS Mode	If DNS information is to be received from a network server, set this parameter to Auto. If DNS information is to be configured manually, set this parameter to Manual.

DHCP server, DNS and Client Lease Time

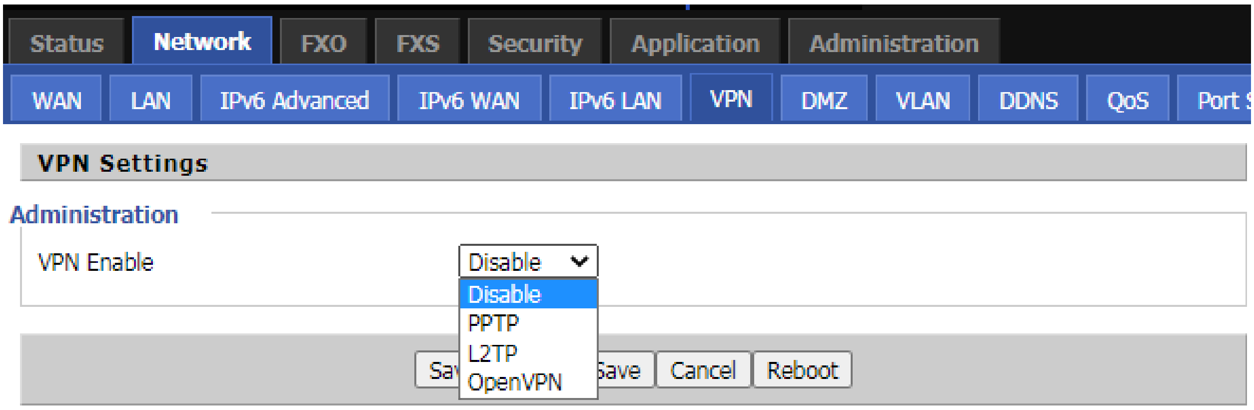
Field Name	Description
Primary DNS	Specify the Primary DNS address provided by your ISP. If your ISP does not provide it, the ATA will automatically apply default DNS Server IP address: 202.96.134.33 to this field.

Secondary DNS	Specify the Secondary DNS address provided by your ISP. If your ISP does not provide this address, the ATA will automatically apply default Secondary DNS Server IP of 202.96.128.86 to this field. If both the Primary IP and Secondary IP Address fields are left empty, the ATA will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.
Client Lease Time	It allows you to set the leased time for the specified PC.

VPN

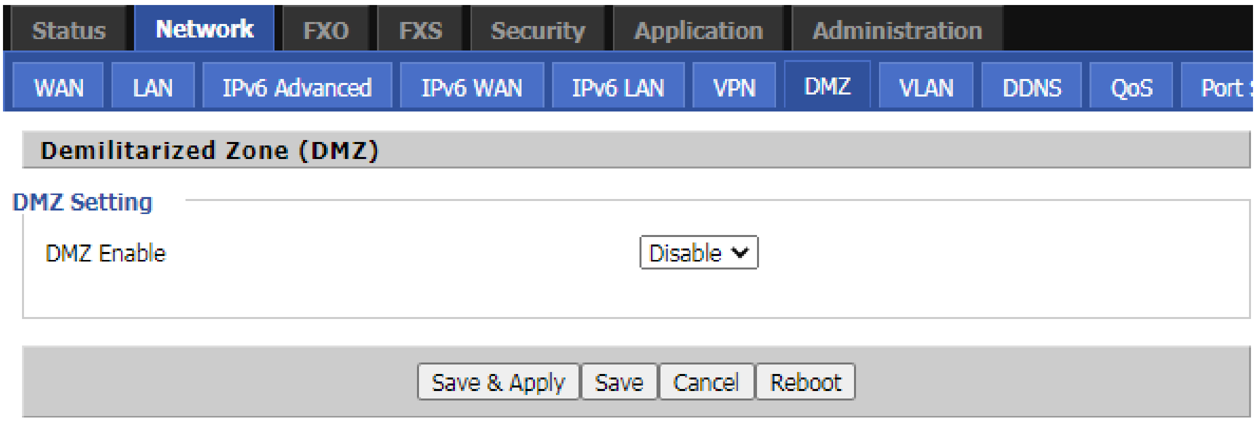
The ATA supports VPN connections with PPTP-based VPN servers.

VPN



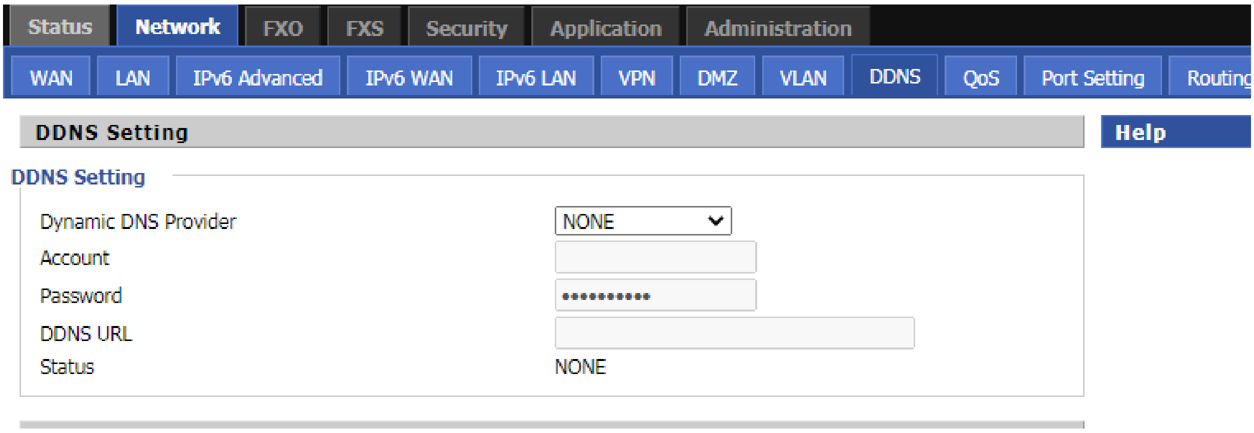
Field Name	Description
VPN Enable	Enable/Disable VPN. If the VPN is enabled, user can select PPTP and L2TP mode VPN.
Initial Service IP	Enter VPN server IP address.
User Name	Enter authentication username.
Password	Enter authentication password.

DMZ



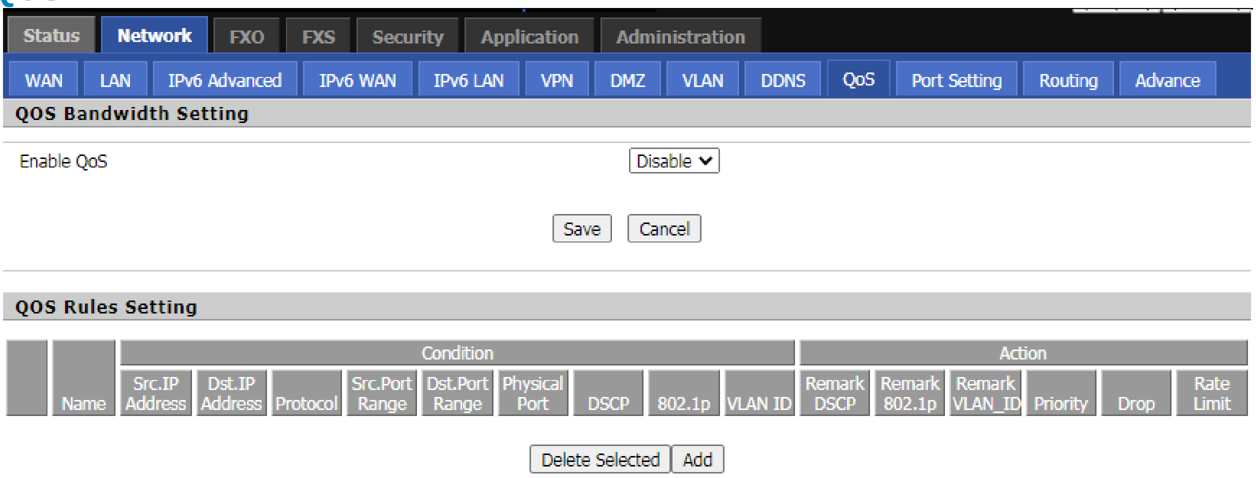
Field Name	Description
DMZ Enable	Enable/Disable DMZ.
DMZ Host IP Address	Enter the private IP address of the DMZ host.

DDNS



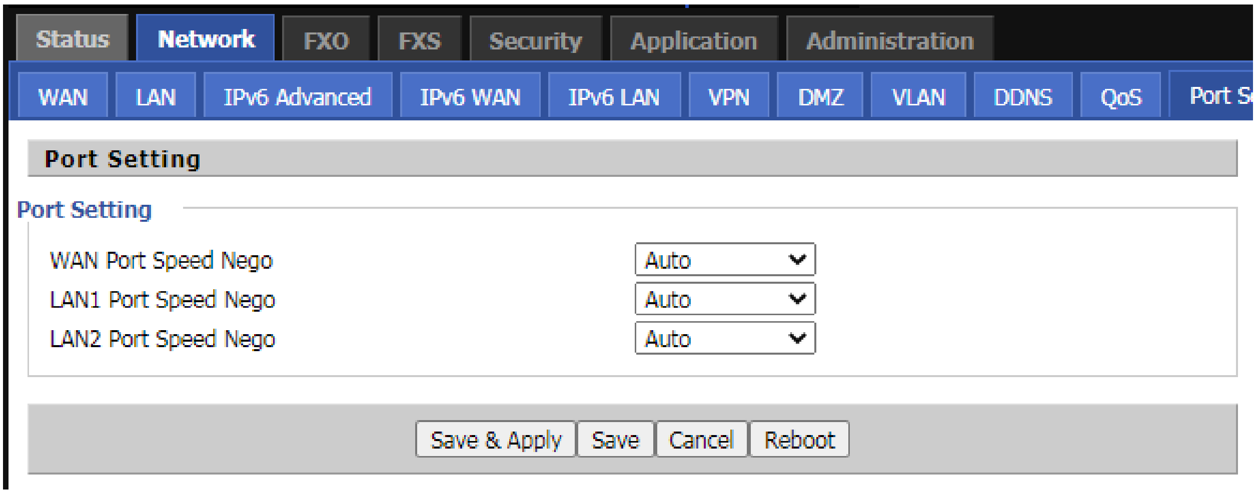
Field Name	Description
Dynamic DNS	Enable DDNS and select the DDNS service provider.
Account	Fill in the DDNS service account.
Password	Fill in the DDNS service account password.
DDNS URL	Fill in the DDNS domain name or IP address.
Status	Check if DDNS is successfully upgraded.

QoS



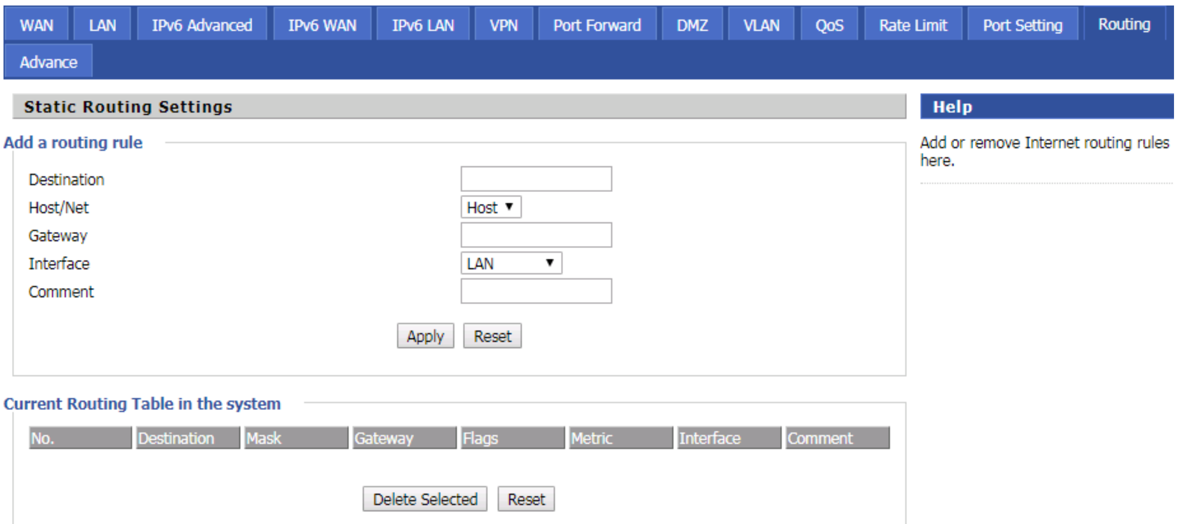
Field Name	Description
QoS Enable	Enable/Disable QoS function.
Upstream	Set the upstream bandwidth.
Downstream	Set the downstream bandwidth.
Delete Selected	In NO., Check the items you want to delete, click the Delete option.
Add	Click Add to add a new parameter.

Port Setting



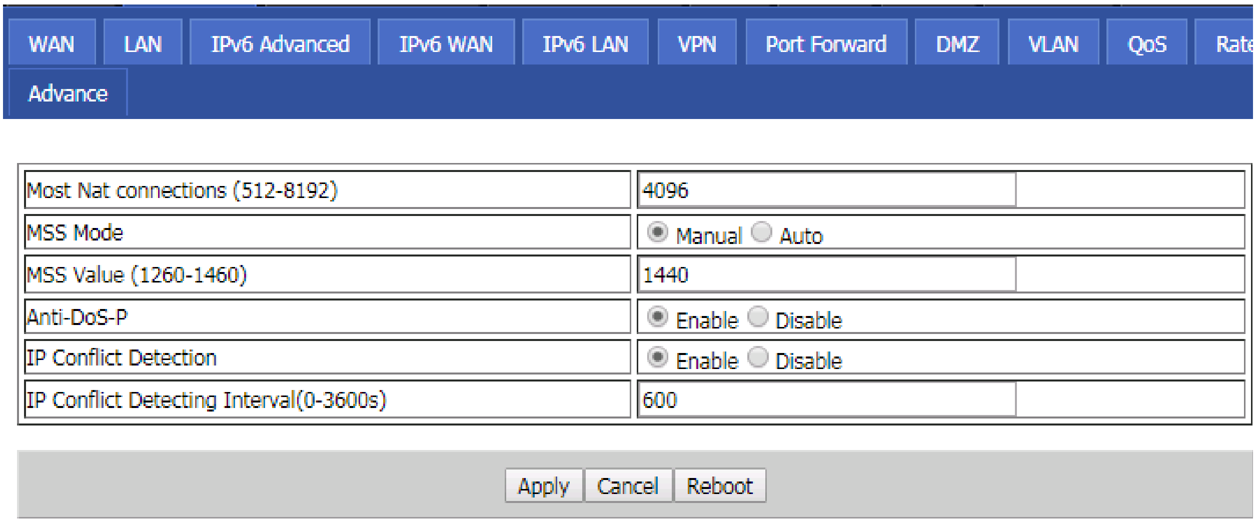
Field Name	Description
WAN Port speed Nego	Auto-negotiation, options are Auto, 100M full, 100M half-duplex, 10M half and full.
LAN1~LAN2 Port Speed Nego	Auto-negotiation, options are Auto, 100M full, 100M half, 10M half and 10M full.

Routing



Field Name	Description
Destination	Destination address
Host/Net	Both Host and Net selection
Gateway	Gateway IP address
Interface	LAN/WAN/Custom three options, and add the corresponding address
Comment	Comment

Advanced



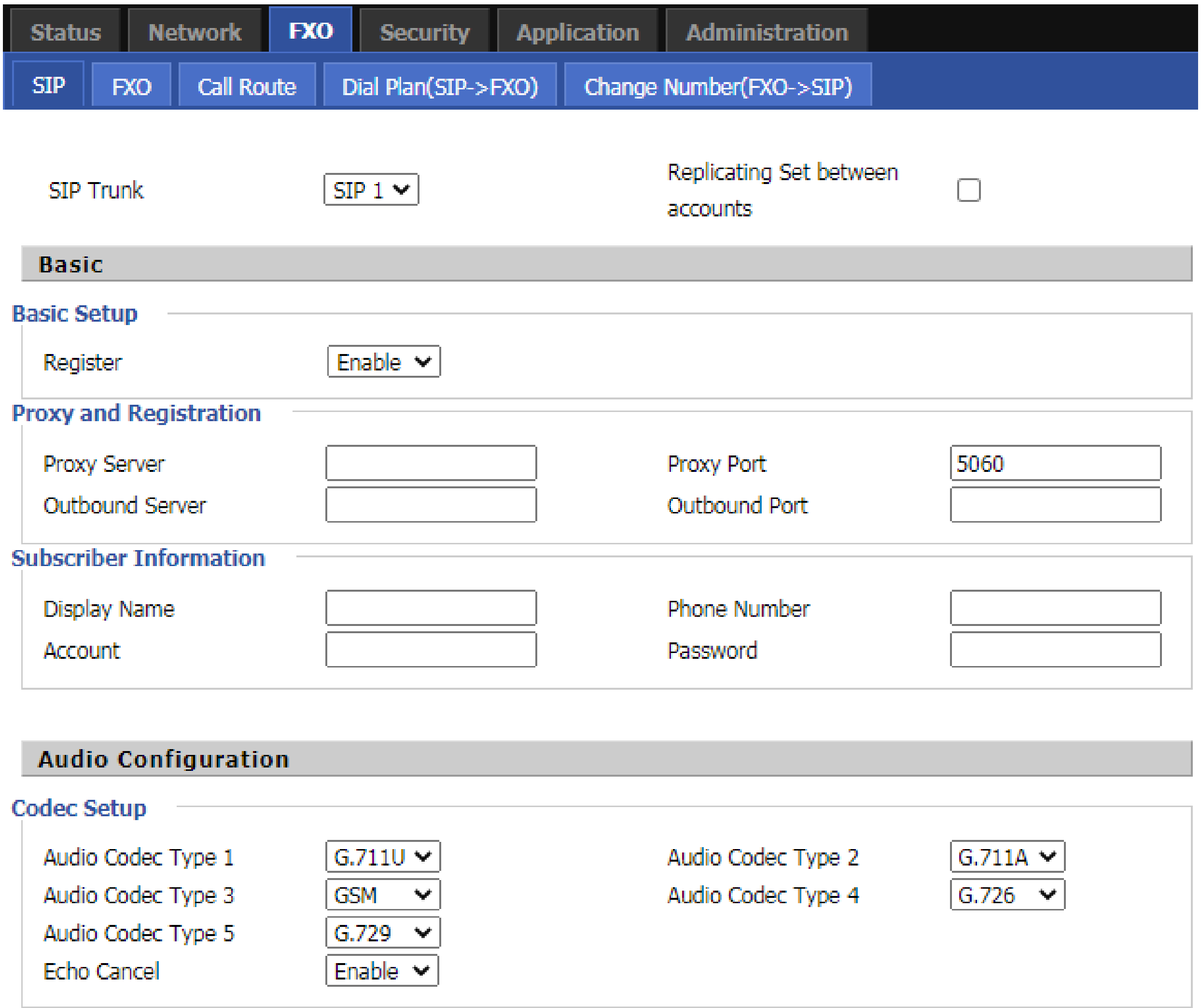
Field Name	Description
Most Nat connections	The largest value which the FWR7302 can provide
MSS Mode	Choose MSS Mode from Manual and Auto
MSS Value	Set the value of TCP
Anti-Dos-p	You can choose to enable or prohibit
IP conflict detection	Select enable if enabled, phone IP conflict will have tips or prohibit
IP conflict Detecting Interval	Detect IP address conflicts of the time interval

FXO

Topics

SIP

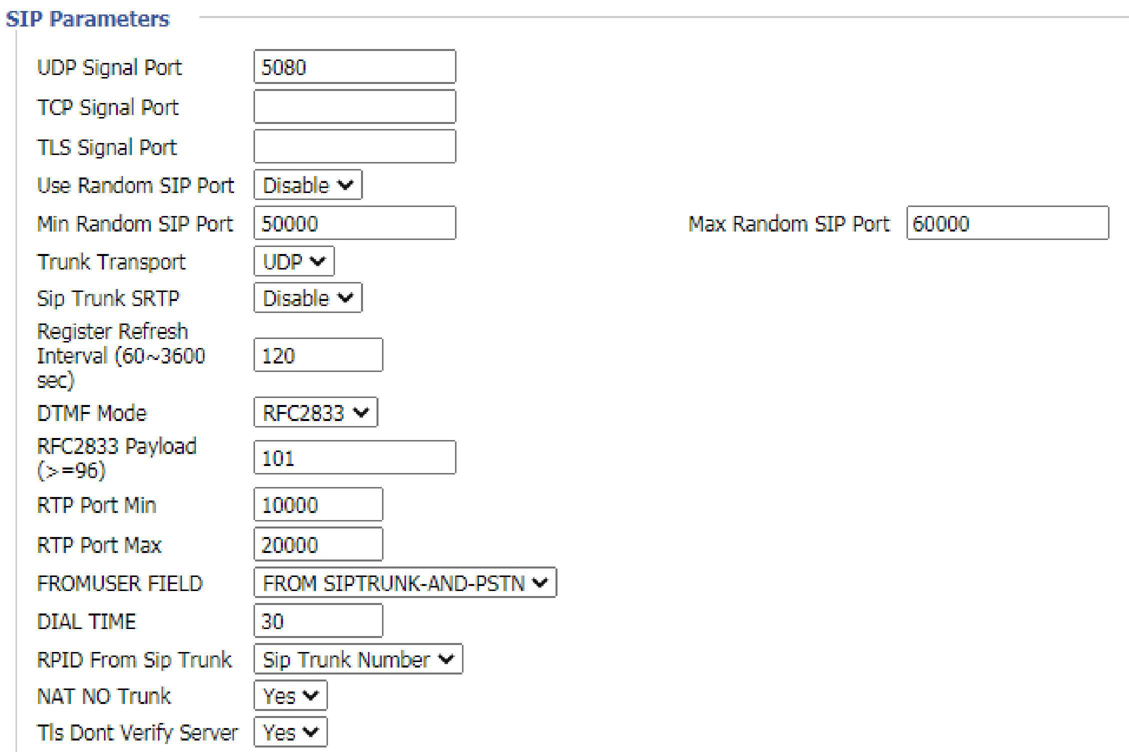
Basic



Field name	Description
SIP trunk	Choose SIP trunk
Register	Enable: as VoIP terminal, register other SIP server Disable: SIP trunk use peer to peer mode
Proxy Server	The IP address or the domain of SIP Server
Outbound Server	The IP address or the domain of Outbound Server
Backup Outbound Server	The IP address or the domain of Backup Outbound Server
Proxy port	SIP Service port, default is 5060
Outbound Port	Outbound Proxy's Service port, default is 5060
Backup Outbound Port	Backup Outbound Proxy's Service port, default is 5060
Display Name	The number will be displayed on LCD
Phone Number	Enter telephone number provided by SIP Proxy
Account	Enter SIP account provided by SIP Proxy
Password	Enter SIP password provided by SIP Proxy

Audio Codec Type1	Choose the audio codec type from G.711U, G.711A, GSM, G.729, G.726
Audio Codec Type2	Choose the audio codec type from G.711U, G.711A, GSM, G.729, G.726
Audio Codec Type3	Choose the audio codec type from G.711U, G.711A, GSM, G.729, G.726
Audio Codec Type4	Choose the audio codec type from G.711U, G.711A, GSM, G.729, G.726
Audio Codec Type5	Choose the audio codec type from G.711U, G.711A, GSM, G.729, G.726
Echo Cancel	Enable/Disable echo cancel. By default, it is enabled

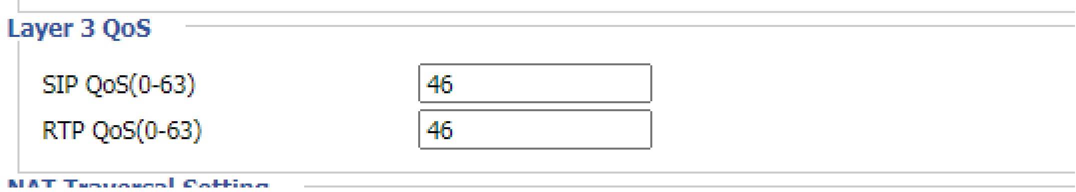
SIP Parameters



Field Name	Description
UDP Signal Port	The local port of SIP protocol, default is 5080
Use Random SIP port	The local random port of SIP protocol
Min Random SIP port	Min Random SIP port, default is 50000
Max Random SIP port	Max Random SIP port, default is 60000
Trunk Transport	SIP protocol: UDP, TCP, TLS
SIP Trunk SRTP	Enable = RTP encrypt / disable = RTP unencrypt
Register Refresh Interval (60~3600 sec)	The interval between two normal Register messages. default setting is 120
DTMF Mode	Choose the DTMF type from Inband, RFC2833 and INFO
RFC2833Payload(>=96)	User can use the default setting
RTP Port min	Min Random RTP port, default is 10000
RTP Port max	Min Random RTP port, default is 20000
FROMUSER FIELD	FROM SIPTRUNK-AND-PSTN: SIP header data from field=sip trunk number and PSTN number FROM SIPTRUNK: SIP header data from field=SIP trunk number FROM PSTN: SIP header data from field=PSTN number
DIAL TIME	Call route from FXO to SIP trunk timeout setting
RPID From Sip Trunk	SIP header data Remote-Party-ID setting.

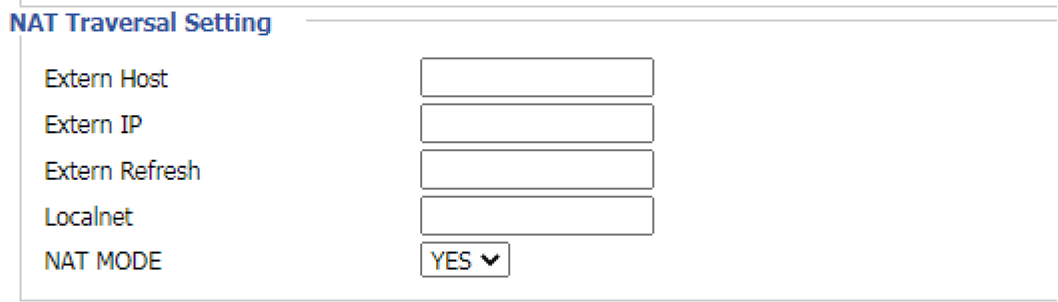
NAT NO Trunk	IP directly call with NAT
Tls Dont Verify Server	TLS peer to peer call

Layer 3 QoS



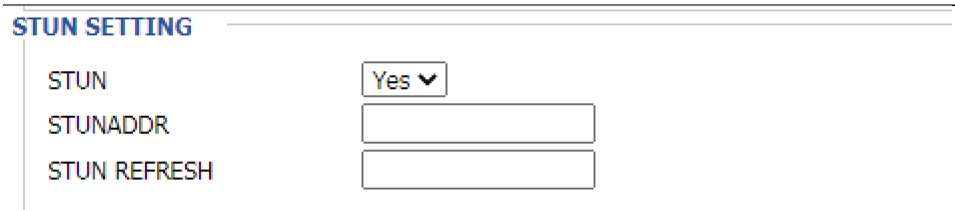
Field Name	Description
SIP QoS(0-63)	VoIP SIP data QoS setting
RTP QoS(0-63)	VoIP RTP data QoS setting

NAT Traversal Setting



Field Name	Description
Extern Host	Upper ATA's domain name which use to do NAT
Extern IP	Upper ATA's IP which use to do NAT
Extern Refresh	NAT setting refresh time
Localnet	Device's IP net
NAT MODE	Enable/disable NAT traversal

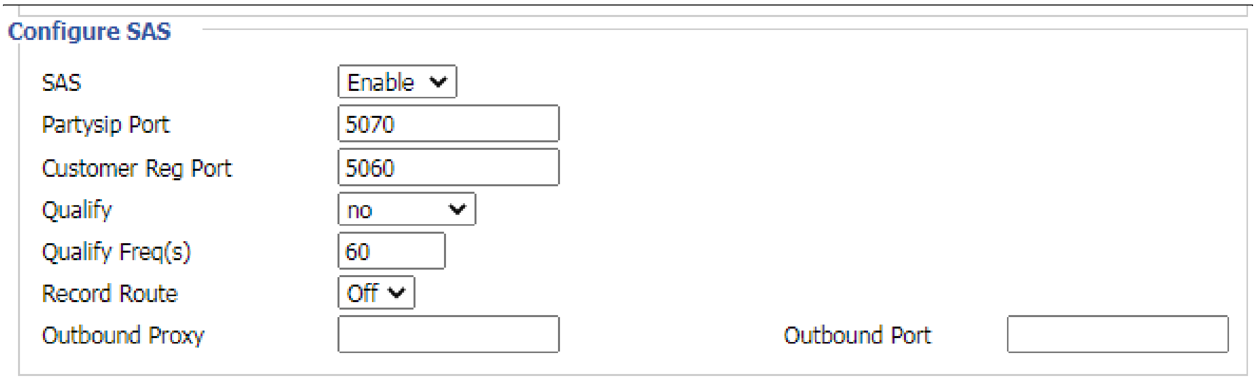
STUN SETTING



Field Name	Description
STUN	Enable/disable STUN
STUNADDR	STUN server IP
STUN REFRESH	Refresh time to refresh stun information

Configure SAS

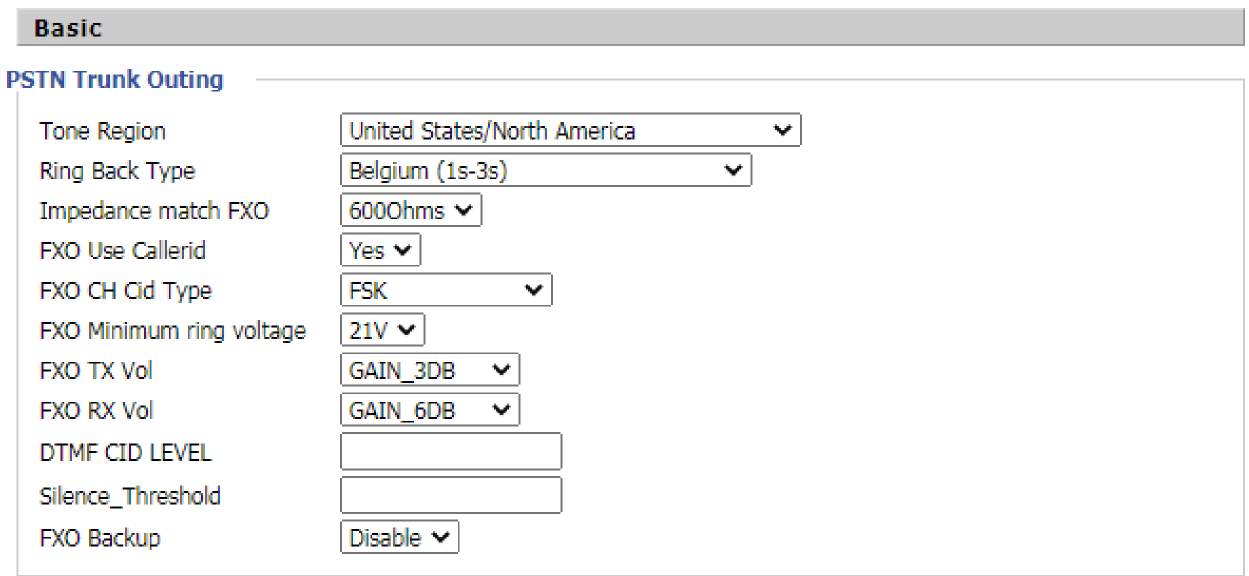
Stand-alone survivability (SAS) is a resource that allows it to assume the functions of an IP PBX in a limited manner, should the latter become unavailable. This way, it is possible to maintain the basic telephony functions until the IP PBX is made available again. It is a useful resource for environments with a cloud-based IP PBX, for example, where communications need to be kept active in case the connection with the IP PBX becomes unavailable. It is necessary to configure the extensions in a way that the ATA will be defined as a proxy SIP. The survivability module verifies the availability of the IP PBX at a configurable interval of seconds through the SIP OPTIONS command. If there is no response to the SIP OPTIONS command within the defined time interval, its mode of operation is changed from proxy to survival mode.



Field Name	Description
SAS	Enable/disable SAS
Partysip Port	Cloud PBX's SIP listen port
Customer Reg Port	Client register port
Qualify	Enable/disable to monitor PBX
Qualify Freq(s)	Device monitoring PBX interval
Record Route	NAT setting refresh time
Outbound Proxy	Device's IP net
Outbound Port	Enable/disable NAT traversal

FXO

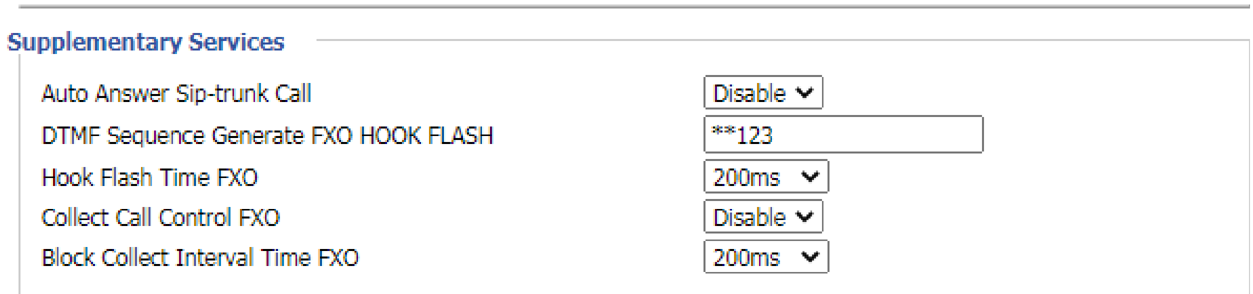
PSTN Trunk Outing



Field Name	Description

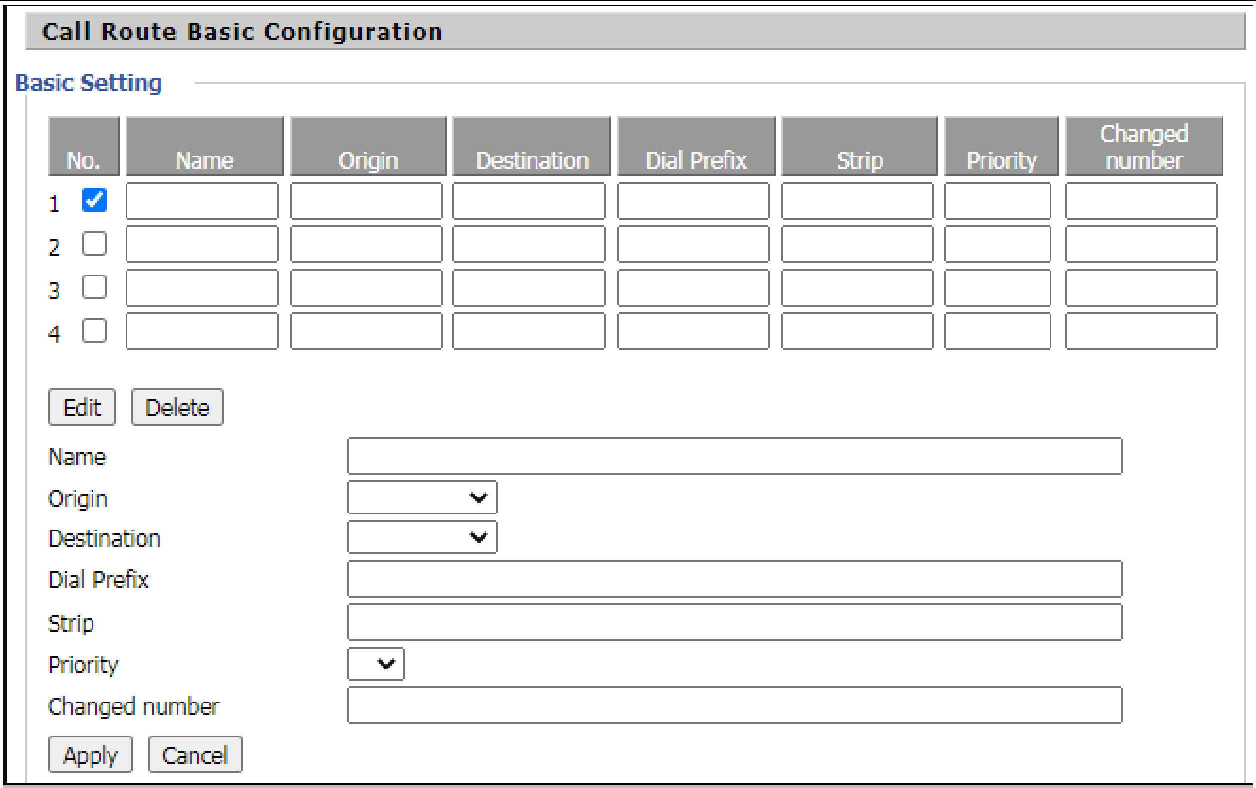
Tone Region	Used to match gateway's tone region setting for DTMF CID detect
Ring Back Type	Used to match gateway's ring back type for DTMF CID detect
Impedance match FXO	FXO impedance setting
FXO Use Callerid	FXO CID enable/disable
FXO CH Cid Type	FXO CID type setting: FSK or DTMF
FXO Minimum ring	FXO ring voltage setting
FXO TX Vol	FXO volume gain setting
FXO RX Vol	FXO volume gain setting
DTMF CID LEVEL	DTMF energy setting, when DTMF CID LEVEL > Silence_Threshold, device will detect DTMF CID number
Silence_Threshold	Device default energy setting
FXO Backup	FXO backup setting, enable, FXO1 and FXO2 are backup for each other

Supplementary Services



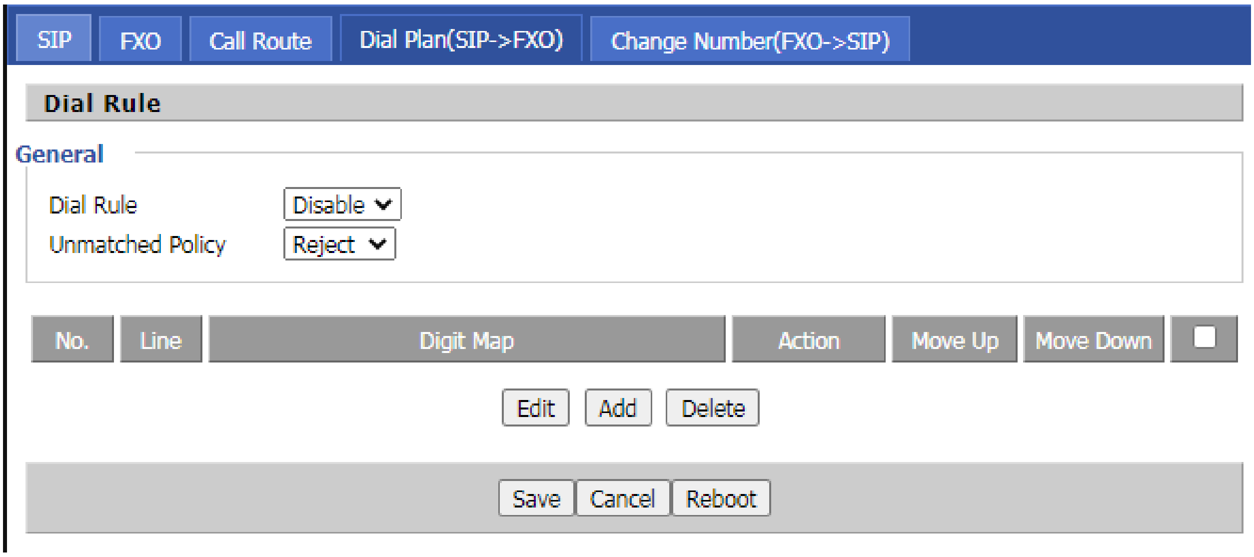
Field Name	Description
Auto Answer Sip-trunk Call	Enable: support two-stage dialing users could call sip trunk number, then dial out going number again. Disable: doesn't support two-stage dialing.
DTMF Sequence Generate FXO HOOK FLASH	DTMF number which used to do HOOK FLASH.
Hook Flash Time FXO	Within this time, if users press DTMF number, then device will hold the call.
Collect Call Control FXO	Block collect call, Collect call is a call that the user receiving this call from PSTN line will pay for.
Block Collect Interval Time FXO	Block collect call interval setting.

Call Route



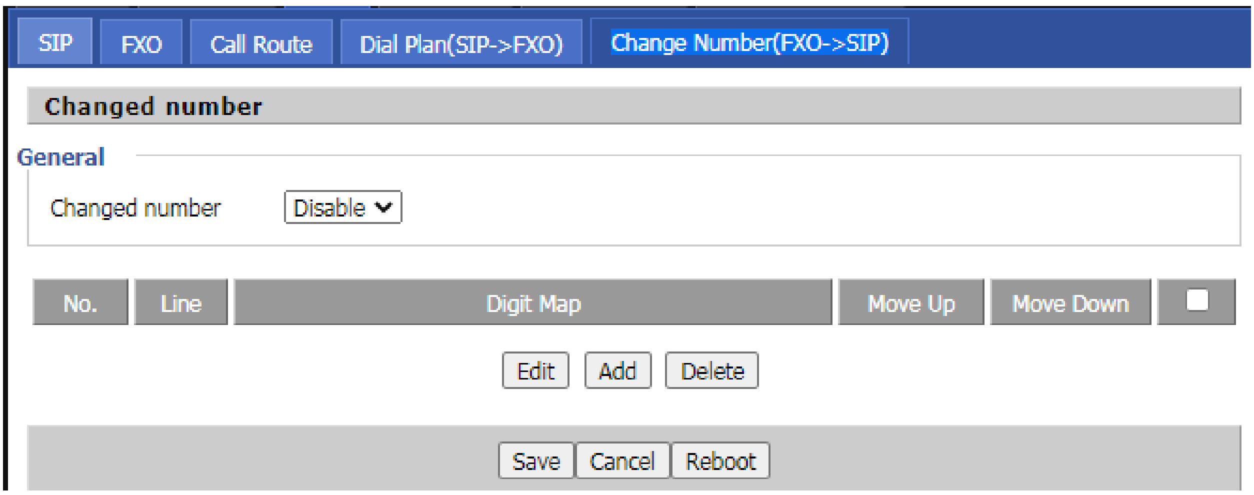
Field Name	Description
Name	Call route name
Origin	Call route source interface, where the call from
Destination	Call route destination interface, where the call will to
Dial Prefix	Call dial prefix setting
Strip	Dial prefix number setting, strip =2, there should be 2 dial prefix number
Priority	Call route priority setting
Changed number	The destination number setting When the call from FXO to SIP trunk, changed number is mandatory When the call from sip trunk to FXO, changed number is not mandatory

Dial Plan (SIP->FXO)



Field Name	Description
Controls how calls will be dialed using this line. It can add a Prefix to Matched Numbers and remove Digits by setting Dial Cuts	
Dial Plan	Enable/Disable dial plan
Line	Set the line
Digit Map	Enter the sequence used to match input number
Action	Choose the dial plan mode from Deny and Dial Out
Move Up	Move the dial plan up the list
Move Down	Move the dial plan down the list

Change Number(FXO->SIP)



Field Name	Description
Handles the source number of the KAP dial-in call to the server by changing in the “from” field in the KAP INVITE	
Dial Plan	Enable/Disable dial plan
Line	Set the line
Digit Map	Enter the sequence used to match input number
Move Up	Move the dial plan up the list
Move Down	Move the dial plan down the list

Dial Plan Syntactic

No.	String	Description
1	0 1 2 3 4 5 6 7 8 9 * #	Allowed characters
2	x	Lowercase letter “x” stands for one legal character
3	[sequence]	To match one character from sequence. For example: [0-9]: match one digit from 0 to 9 [2-5*]: match one character from 2 or 3 or 4 or 5 or *
4	x.	Match to x, xx, xxx, xxxx and so on For example: “01” can be match to “0”,”01”,”011”…”011111…” and so on
5	<dialed: substituted>	Replace dialed with substituted For example: <8:1650>123456:input is “85551212”, output is “16505551212”
6	x,y	Make outside dial tone after dialing “x”, stop until dialing character “y” For example: “9,1xxxxxxxxxx”: the device reports dial tone after inputting “9”, stops tone until inputting “1” “9,8,010x”: make outside dial tone after inputting “9”, stop tone until inputting “0”
7	T	Set the delayed time. For example: “<9:111>T2”: The device will dial out the matched number “111” after 2 seconds

FXS

Topics

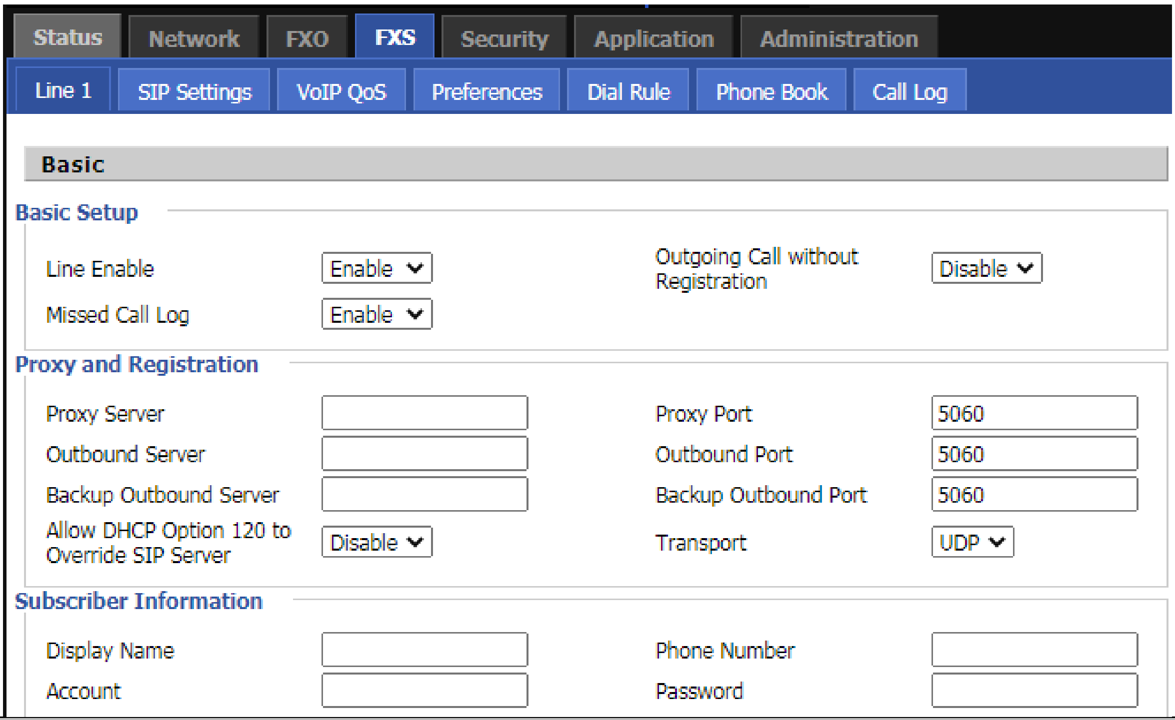
[Line1]()
[SIP Settings]()

[VoIP QoS]
[Preferences]
[Dial Rule]
[Phone Book]
[Call Log]

Line1

Basic

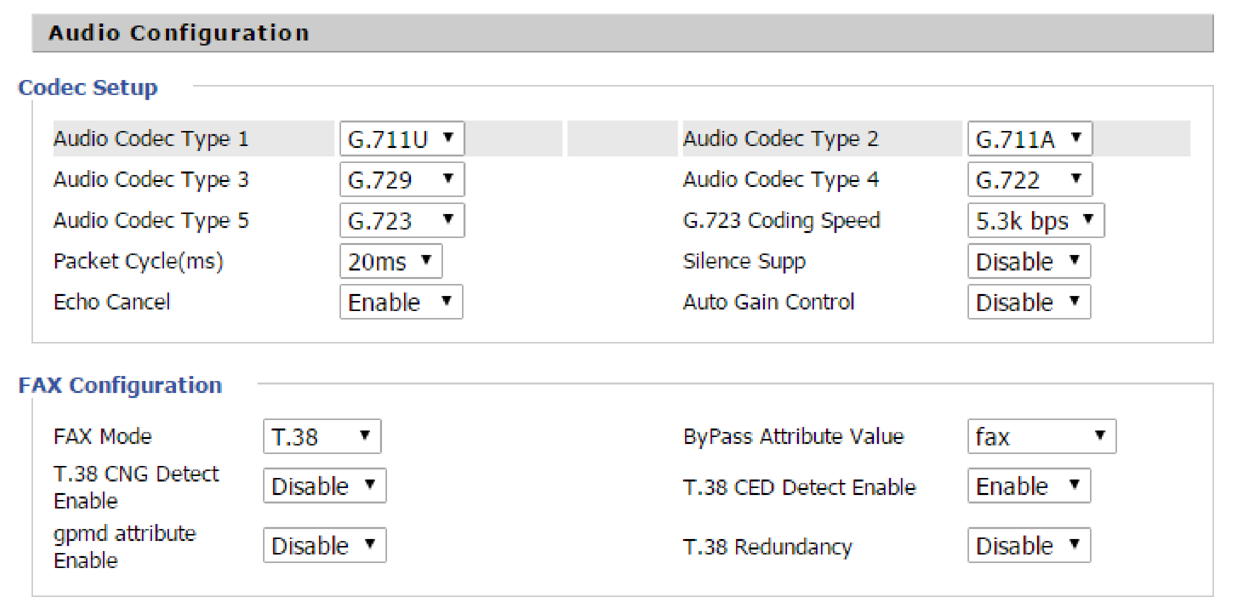
Set the basic information provided by your VOIP Service Provider, such as Phone Number, Account, password, SIP Proxy and others.



Field Name	Description
Line Enable	Enable/Disable the line
Peer To Peer	Enable/Disable PEER to PEER If enabled, SIP-1 will not send register request to SIP server; but in Status/ SIP Account Status webpage, Status is Registered; lines 1 can dial out, but the external line number cannot dialed line1
Proxy Server	The IP address or the domain of SIP Server
Outbound Server	The IP address or the domain of Outbound Server
Backup Outbound	The IP address or the domain of Backup Outbound Server
Proxy port	SIP Service port, default is 5060
Outbound Port	Outbound Proxy’s Service port, default is 5060
Backup Outbound Port	Backup Outbound Proxy’s Service port, default is 5060
Display Name	The number will be displayed on LCD
Phone Number	Enter telephone number provided by SIP Proxy
Account	Enter SIP account provided by SIP Proxy

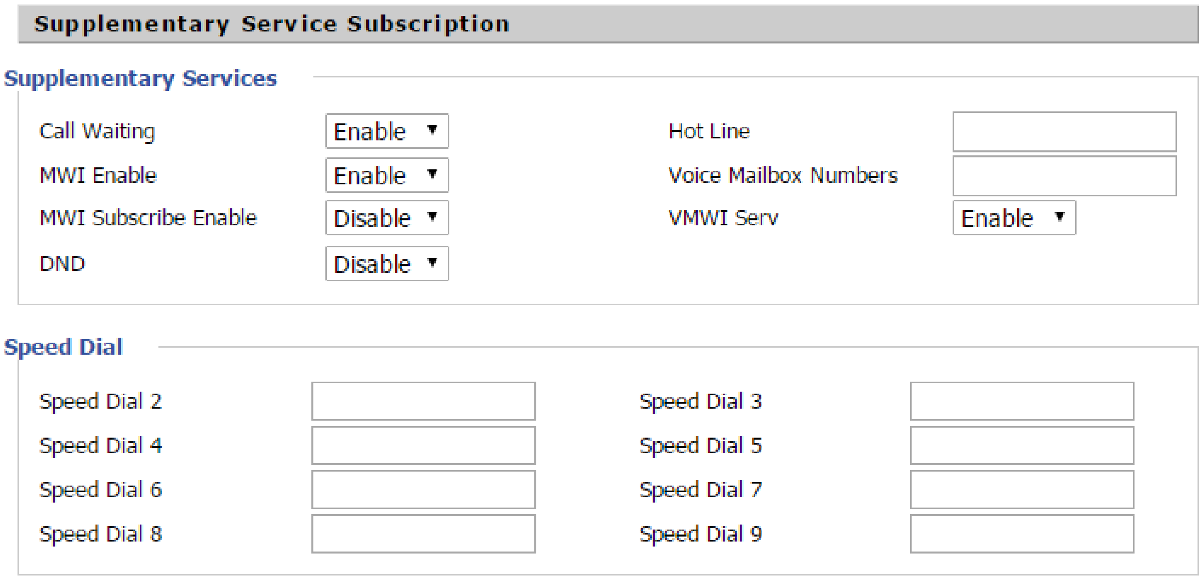
Password	Enter SIP password provided by SIP Proxy

Audio Configuration



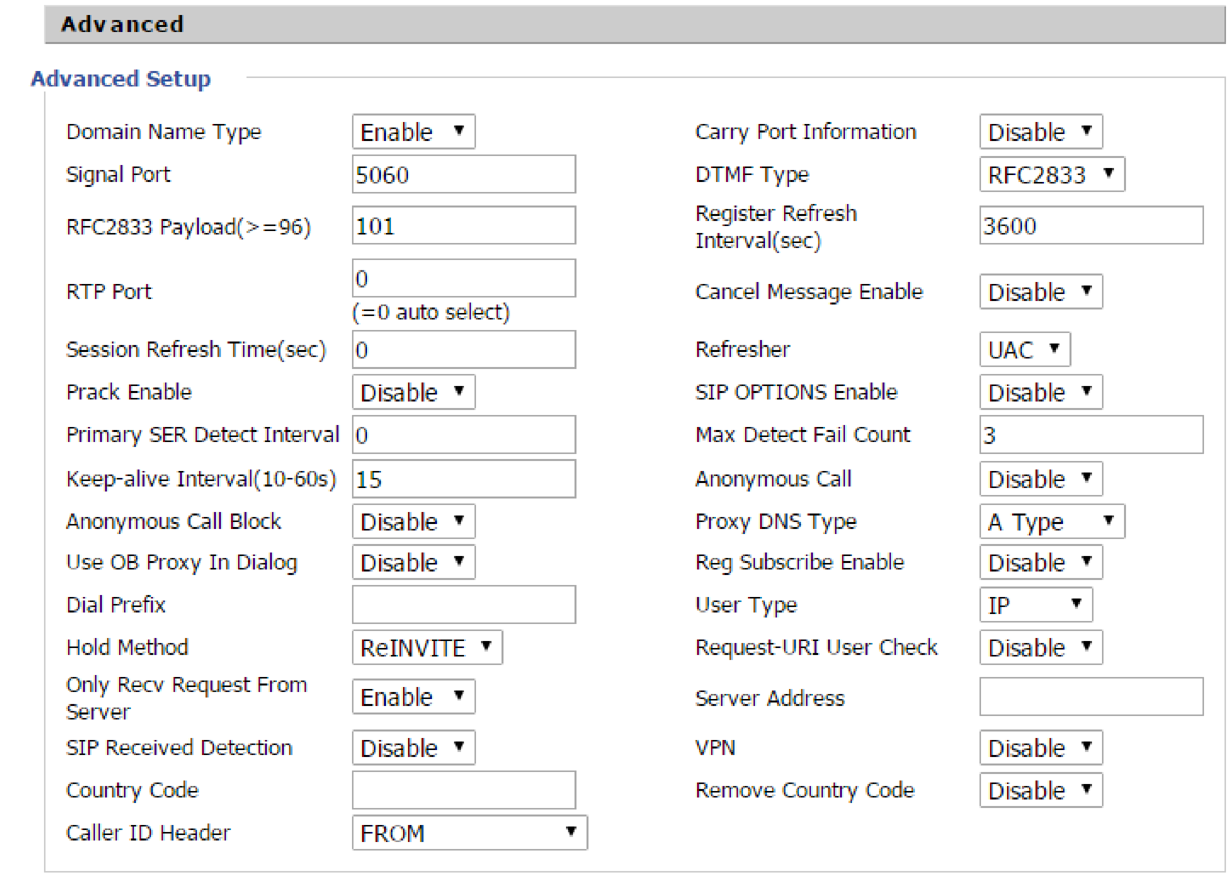
Audio Codec Type1	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type2	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type3	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type4	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type5	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
G.723 Coding Speed	Choose the speed of G.723 from 5.3kbps and 6.3kbps
Packet Cycle	The RTP packet cycle time, default is 20ms
Silence Supp	Enable/Disable silence support
Echo Cancel	Enable/Disable echo cancel. By default, it is enabled
Auto Gain Control	Enable/Disable auto gain
T.38 Enable	Enable/Disable T.38
T.38 Redundancy	Enable/Disable T.38 Redundancy
T.38 CNG Detect Enable	Enable/Disable T.38 CNG Detect
gpmd attribute Enable	Enable/Disable gpmd attribute

Supplementary Service Subscription



Field Name	Description
Call Waiting	Enable/Disable Call Waiting
Hot Line	Fill in the hotline number, Pickup handset or press hands-free or headset button, the device will dial out the hotline number automatically
MWI Enable	Enable/Disable MWI (message waiting indicate). If the user needs to use voice mail, please enable this feature
MWI Subscribe Enable	Enable/Disable MWI Subscribe
Voice Mailbox Numbers	Fill in the voice mailbox phone number, Asterisk platform, for example, its default voice mail is *97
VMWI Serv	Enable/Disable VMWI service
DND	Enable/Disable DND (do not disturb)
Speed Dial	Enter the speed dial phone numbers. Dial *74 to active speed dial function. Then press the speed dial numbers, for example, press 2, phone dials 075526099365 directly

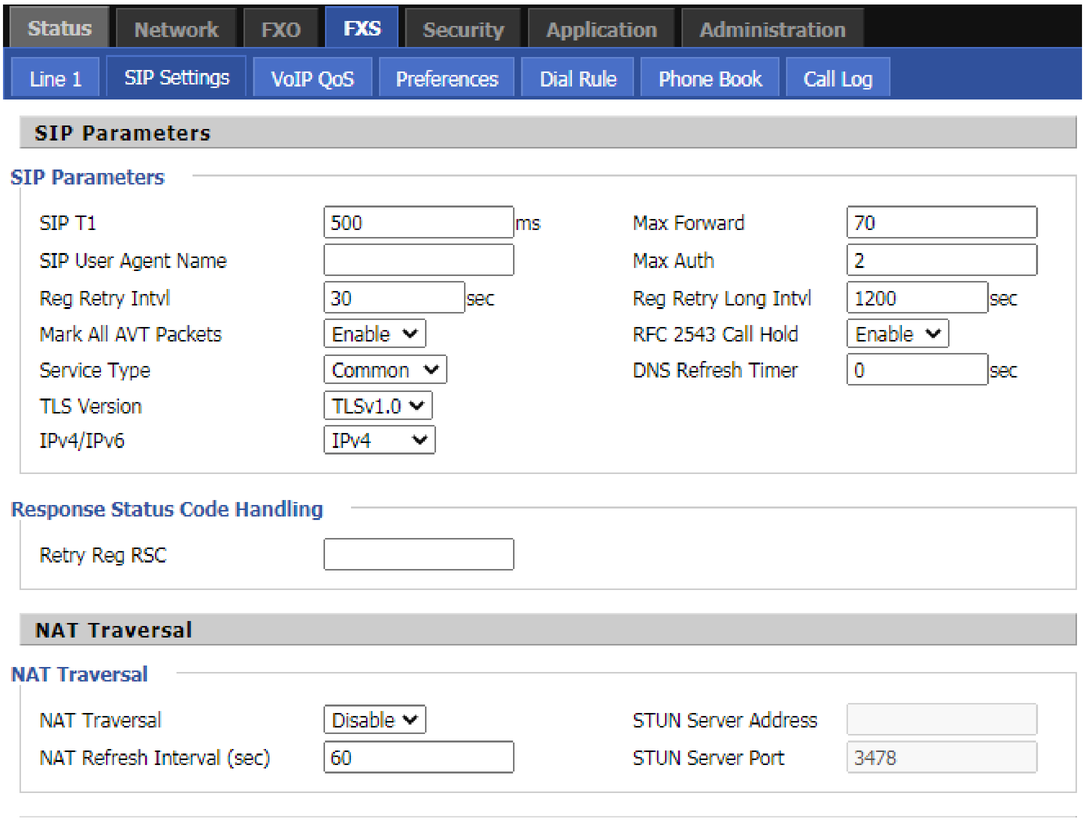
Advanced



Field Name	Description
Domain Name Type	If or not use domain name in the SIP URI.
Carry Port Information	If or not carry port information in the SIP URI.
Signal Port	The local port of SIP protocol, default is 5060.
DTMF Type	Choose the DTMF type from Inbound, RFC2833 and SIP INFO.
RFC2833Payload (>=96)	User can use the default setting.
Register Refresh Interval	The interval between two normal Register messages. You can use the default setting.
RTP Port	Set the port to send RTP. The device will select one idle port for RTP if you set “0”; otherwise use the value which user sets.
Cancel Message Enable	When you set enable, an unregistered message will be sent before registration, while you set disable, unregistered message will not be sent before registration. You should set the option for different Proxy.
Session Refresh	Time interval between two sessions, you can use the default settings.
Refresher	Choose refresher from UAC and UAS.
Prack Enable	Enable/Disable prack.

SIP OPTIONS Enable	When you set enable, the device will send SIP-OPTION to the server, instead of sending periodic Hello message. The sending interval is Keep-alive interval.
Primary SER Detect Interval	Test interval of the primary server, the default value is 0, it represents disable.
Max Detect Fail Count	Interval of detection of the primary server fail; the default value is 3, it means that if detect 3 times fail; the device will no longer detect the primary server.
Keep-alive Interval(10-	The interval that the device will send an empty packet to proxy.
Anonymous Call	Enable/Disable anonymous call.
Anonymous Call Block	Enable/Disable anonymous call block.
Proxy DNS Type	Set the DNS server type, choose from A type and DNS SRV.
Use OB Proxy In Dialog	If or not use OB Proxy In Dialog.
Reg Subscribe Enable	If enable, subscribing will be sent after registration message, if not , do not send subscription.
Dial Prefix	The number will be added before your telephone number when making calls.
User Type	Choose the User Type from IP and Phone.
Hold Method	Choose the Hold Method from ReINVITE and INFO.
Request-URI User Check	Enable/Disable the user request URI check.
Only Recv request from server	Enable/Disable the only receive request from server.
Server Address	The IP address of SIP server.
SIP Received Detection	Enable/Disable SIP Received Detection, if enable, use it to confirm the public network address of the device.

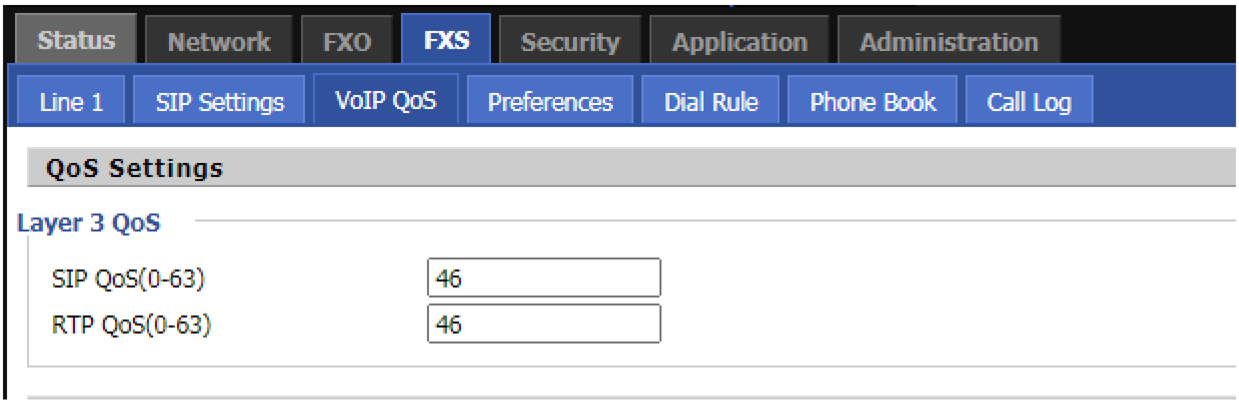
SIP Settings



Field Name	Description
SIP T1	The minimum scale of retransmission time
Max Forward	SIP contains Max Forward message header fields used to limit the requests for forwards
SIP Reg User Agent Name	The agent's name of SIP registered user
Max Auth	The maximum number of retransmissions

Mark All AVT Packets	Voice packet marking to enable this item will see the mark on the voice message when the call environment changed (such as press a key during the call)
RFC 2543 Call Hold	Enable the Connection Information field displays the address is 0.0.0.0 in the invite message of Hold. Disable the Connection Information field displays the device IP address in the invite message of Hold
SRTP	Whether to enable the call packet encryption function
SRTP Prefer Encryption	The preferred encryption type of calling packet (the Message body of INVITE Message)
Service Type	Choose the server type
NAT Traversal	Enable/Disable NAT Traversal FWR9502 supports STUN Traversal; if user wants to traverse NAT/Firewall, select the STUN
STUN Server Address	Add the correct STUN service provider IP address
NAT Refresh Interval	Set NAT Refresh Interval, default is 60s
STUN Server Port	Set STUN Server Port, default is 5060

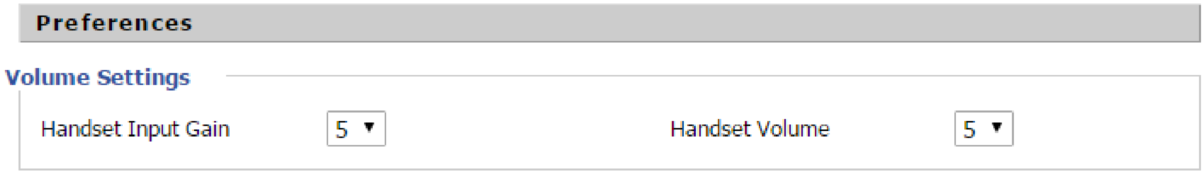
VoIP QoS



Field Name	Description
SIP /RTP QoS	The default value is 0, you can set a range of values is 0~63

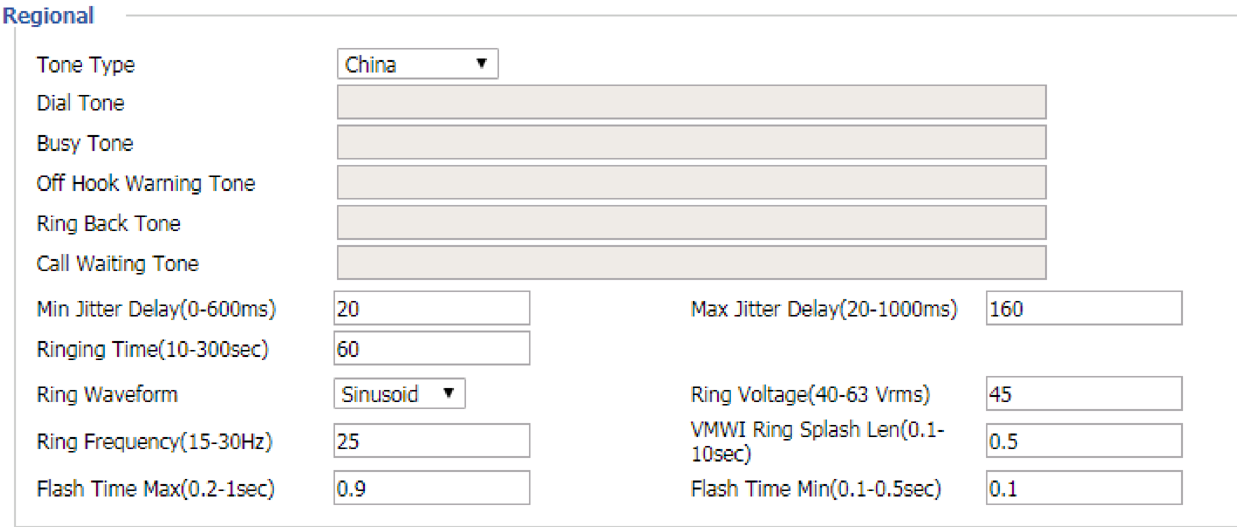
Preferences

Volume Settings



Field Name	Description
Handset Input	Adjust the handset input gain from 0 to 7
Handset Volume	Adjust the output gain from 0 to 7

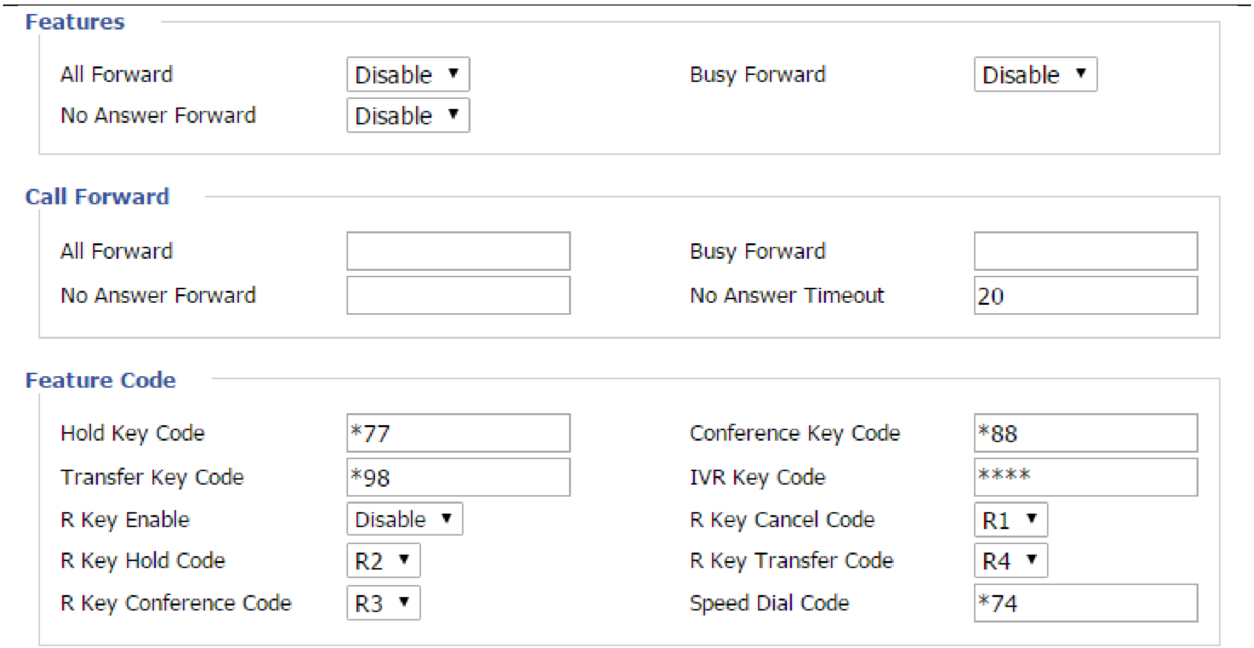
Regional



Field Name	Description
Tone Type	Choose tone type from China, US, Hong Kong and so on
Dial Tone	Dial Tone
Busy Tone	Busy Tone
Off Hook Warning	Off Hook warning tone
Ring Back Tone	Ring back tone
Call Waiting Tone	Call waiting tone
Min Jitter Delay	The Min value of home gateway's jitter delay, home gateway is an adaptive jitter mechanism
Max Jitter Delay	The Max value of home gateway's jitter delay, home gateway is an adaptive jitter mechanism
Ringing Time	How long the device will ring when there is an incoming call
Ring Waveform	Select regional ring waveform, options are Sinusoid and Trapezoid, the default Sinusoid
Ring Voltage	Set ringing voltage, the default value is 70
Ring Frequency	Set ring frequency, the default value is 25

VMWI Ring Splash Len(sec)	Set the VMWI ring splash length, default is 0.5s
Flash Time Max(sec)	Set the Max value of the device's flash time, the default value is 0.9
Flash Time Min(sec)	Set the Min value of the device's flash time, the default value is 0.1

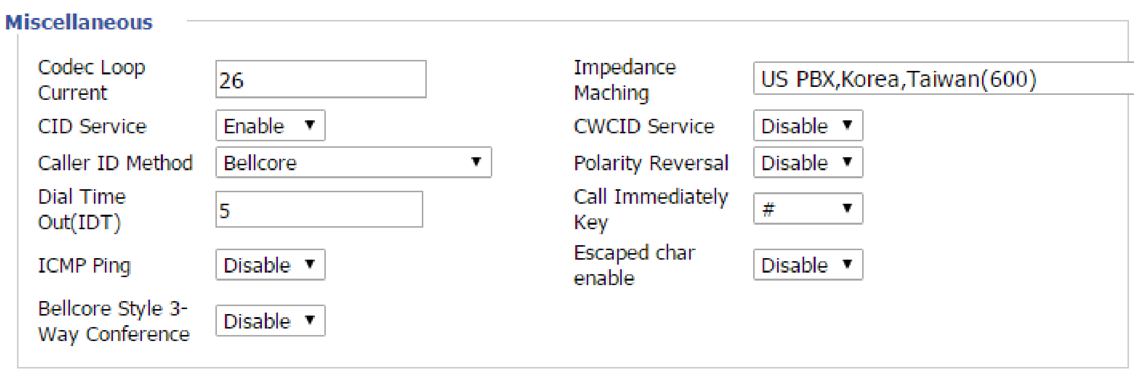
Features and Call Forward



Field Name		Description
Features	All Forward	Enable/Disable forward all calls
	Busy Forward	Enable/Disable busy forward
	No Answer Forward	Enable/Disable no answer forward
Call Forward	All Forward	Set the target phone number for all forward The device will forward all calls to the phone number immediately when there is an incoming call
	Busy Forward	The phone number which the calls will be forwarded to when line is busy
	No Answer Forward	The phone number which the call will be forwarded to when there's no answer
	No Answer Timeout	The seconds to delay forwarding calls, if there is no answer at your phone
Feature Code	Hold key code	Call hold signatures, default is *77
	Conference key	Signature of the tripartite session, default is *88

Miscellaneous

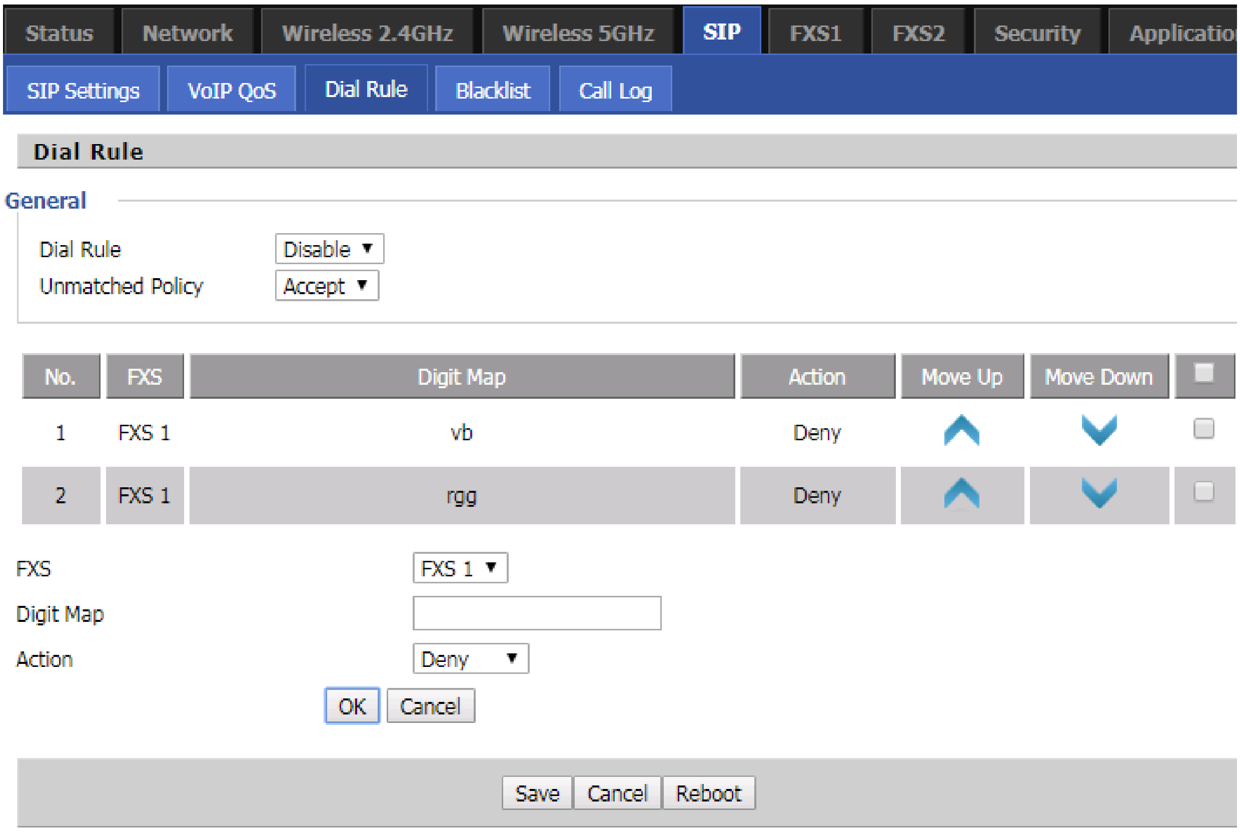
Transfer key code	Call forwarding signatures, default is *98
IVR key code	Signatures of the voice menu, default is ****
R key enable	Enable/Disable R key way call features.
R key cancel code	Set the R key cancel code, options are ranged from R1 to R9, default value is R1
R key hold code	Set the R key hold code, options are ranged from R1 to R9, default value is R2
R key transfer code	Set the R key transfer code, options are ranged from R1 to R9, default value is R4
R key conference code	Set the R key conference code, options are ranged from R1 to R9, default value is R3
Speed Dial Code	Speed dial code, default is *74



Field Name	Description
Codec Loop Current	Set off-hook loop current, default is 26.
Impedance Maching	Set impedance matching, default is US PBX, Korea, Taiwan (600).
CID service	Enable/Disable displaying caller ID; If enable, caller ID is displayed when there is an incoming call or it won't be displayed. Default is enabled.
CWCID Service	Enable/Disable CWCID. If enable, the device will display the waiting call's caller ID, or it won't display. Default is disable.
Dial Time Out	How long device will sound dial out tone when device dials a number.
Call Immediately Key	Choose call immediately key from * or # or disable.
ICMP Ping	Enable/Disable ICMP Ping. If enable this option, home gateway will ping the SIP Server every interval time, otherwise, it will send "hello" empty packet to the SIP Server.
Escaped char enable	Open special character translation function; if enable, when you press the # key, it will be translated to 23%, when disable, it is just #.

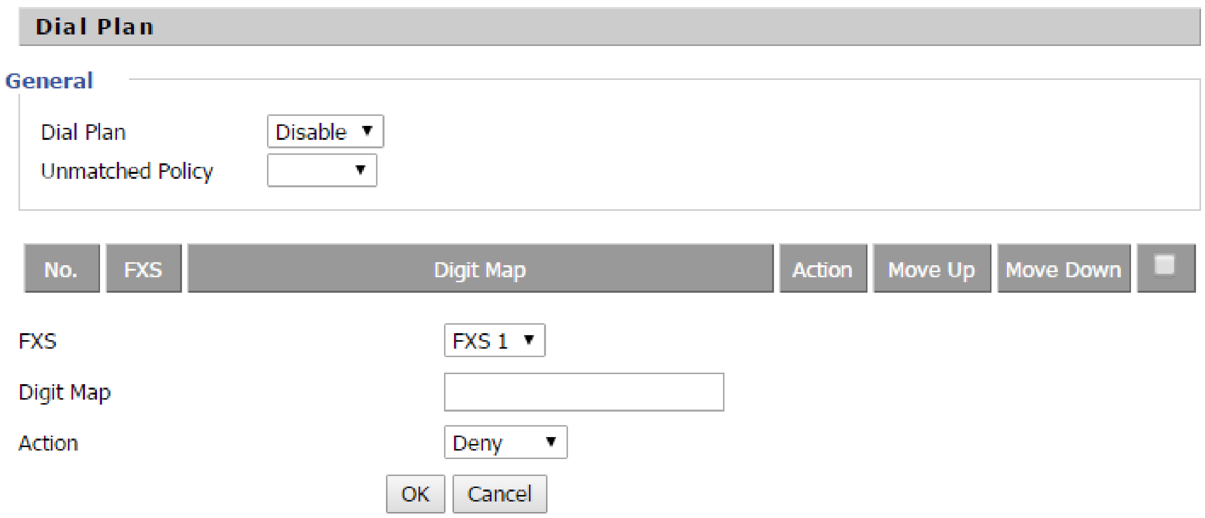
Dial Rule

Parameters and Settings



Field Name	Description
Dial Plan	Enable/Disable dial plan
Line	Set the line
Digit Map	Enter the sequence used to match input number The syntactic, please refer to the following Dial Plan Syntactic
Action	Choose the dial plan mode from Deny and Dial Out Deny means ATA will reject the matched number, while Dial Out means ATA will dial out the matched number
Move Up	Move the dial plan up the list
Move Down	Move the dial plan down the list

Adding one Dial Plan



Description
Step 1. Enable Dial Plan
Step 2. Click Add button, and the configuration table
Step 3. Fill in the value of parameters
Step 4. Press OK button to end configuration

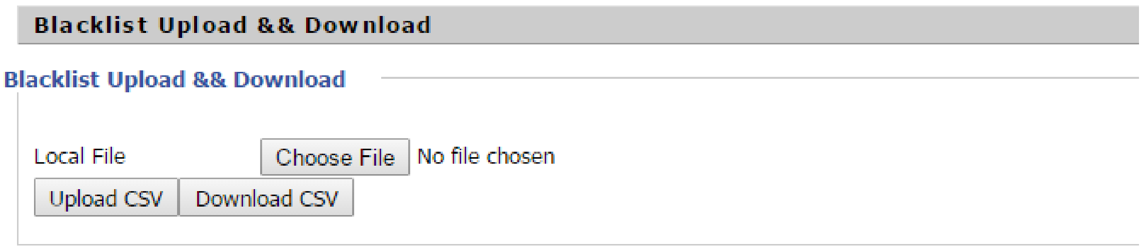
Dial Plan Syntactic

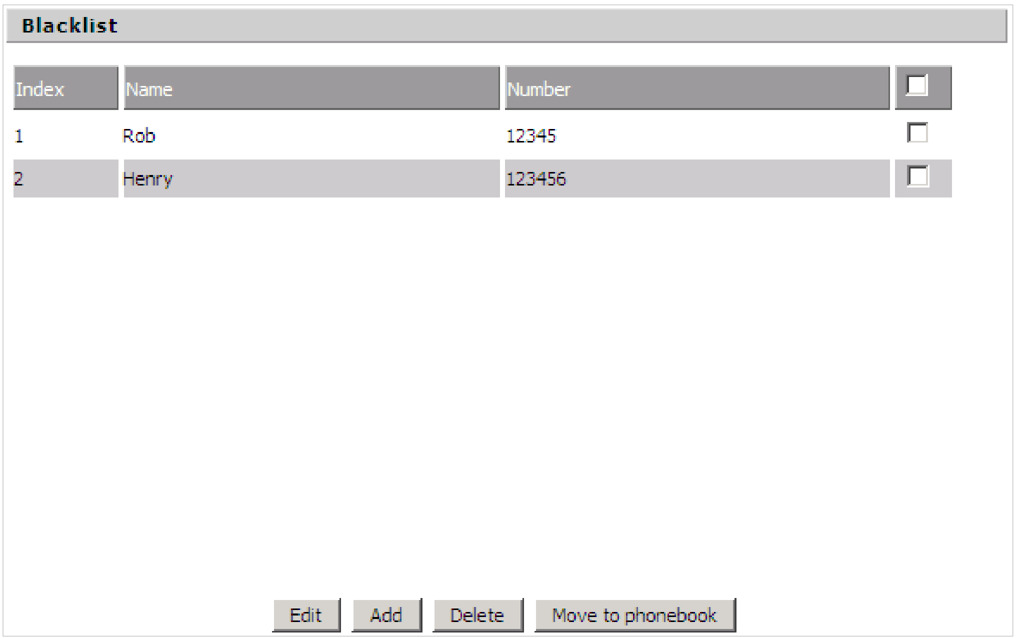
No.	String	Description
1	0 1 2 3 4 5 6 7 8 9 * #	Allowed characters
2	x	Lowercase letter “x” stands for one legal character
3	[sequence]	To match one character from sequence. For example: [0-9]: match one digit from 0 to 9 [2-5*]: match one character from 2 or 3 or 4 or 5 or *
4	x.	Match to x, xx, xxx, xxxx and so on For example: “01” can be match to “0”,”01”,”011”...”011111...” and so on
5	<dialed: substituted>	Replace dialed with substituted For example: <8:1650>123456:input is”85551212”, output is”16505551212”

6	x,y	Make outside dial tone after dialing "x", stop until dialing character "y" For example: "9,1xxxxxxxxxx": the device reports dial tone after inputting "9", stops tone until inputting "1" "9,8,010x": make outside dial tone after inputting "9", stop tone until inputting "0"
7	T	Set the delayed time. For example: "<9:111>T2": The device will dial out the matched number "111" after 2 seconds

Phone Book

In this page, user can upload or download blacklist file, and can add or delete or edit blacklist one by one.





Description

Click 选择文件 to select the blacklist file and upload CSV to upload it to device; Click download CSV to save the blacklist file to your local computer.

Select one contact and click edit to change the information, click delete to delete the contact, click Move to phonebook to move the contact to phonebook.

Click Add to add one blacklist, enter the name and phone number, click OK to confirm and click cancel to cancel.

Call Log

To view the call log information such as redial list, answered call and missed call.

Redial List

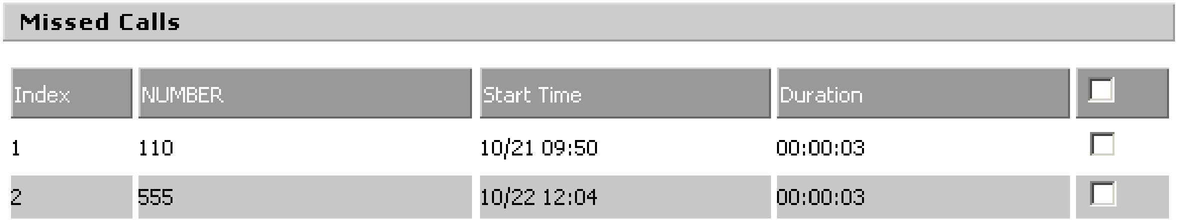
Index	NUMBER	Start Time	Duration	☐
1	123	10/28 10:30	00:00:07	☐
2	010123	10/28 12:02	00:00:01	☐
3	010123	10/28 16:16	00:00:00	☐
4	010123	10/28 16:16	00:00:00	☐
5	123	10/28 16:20	00:00:13	☐
6	123	10/28 16:21	00:00:34	☐
7	123	10/29 10:50	00:00:10	☐
8	123	10/29 14:36	00:00:01	☐
9	123	10/29 15:05	00:00:23	☐
10	123	10/29 15:06	00:00:05	☐

Redial List

Answered Calls

Index	NUMBER	Start Time	Duration	☐
1	22222	10/21 09:56	00:00:40	☐
2	110	10/21 18:14	00:00:03	☐
3	110	10/21 18:15	00:00:07	☐
4	sipp	10/23 13:40	00:00:06	☐
5	sipp	10/24 18:05	00:00:05	☐
6	sipp	10/24 18:05	00:00:05	☐
7	sipp	10/25 15:38	00:00:03	☐
8	sipp	10/25 15:42	00:00:06	☐
9	sipp	10/25 15:55	00:00:10	☐
10	sipp	10/25 16:03	00:00:02	☐

Answered Calls



Missed Calls

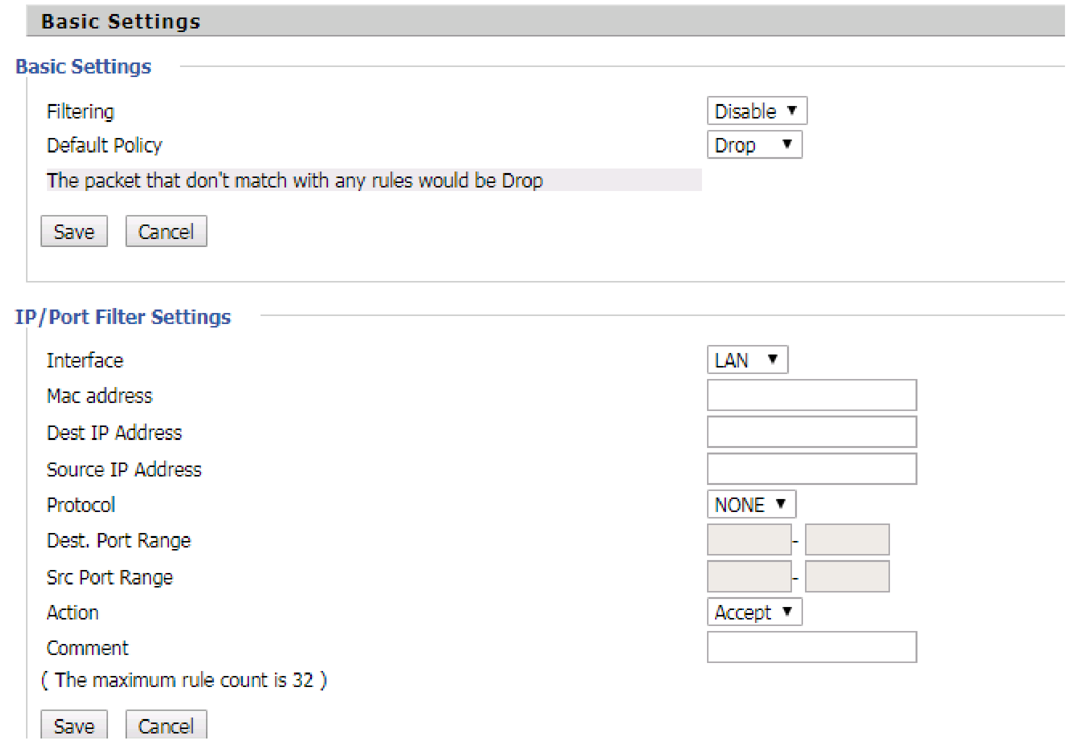
Security

Topics

[Filtering Setting]

[Content Filtering]

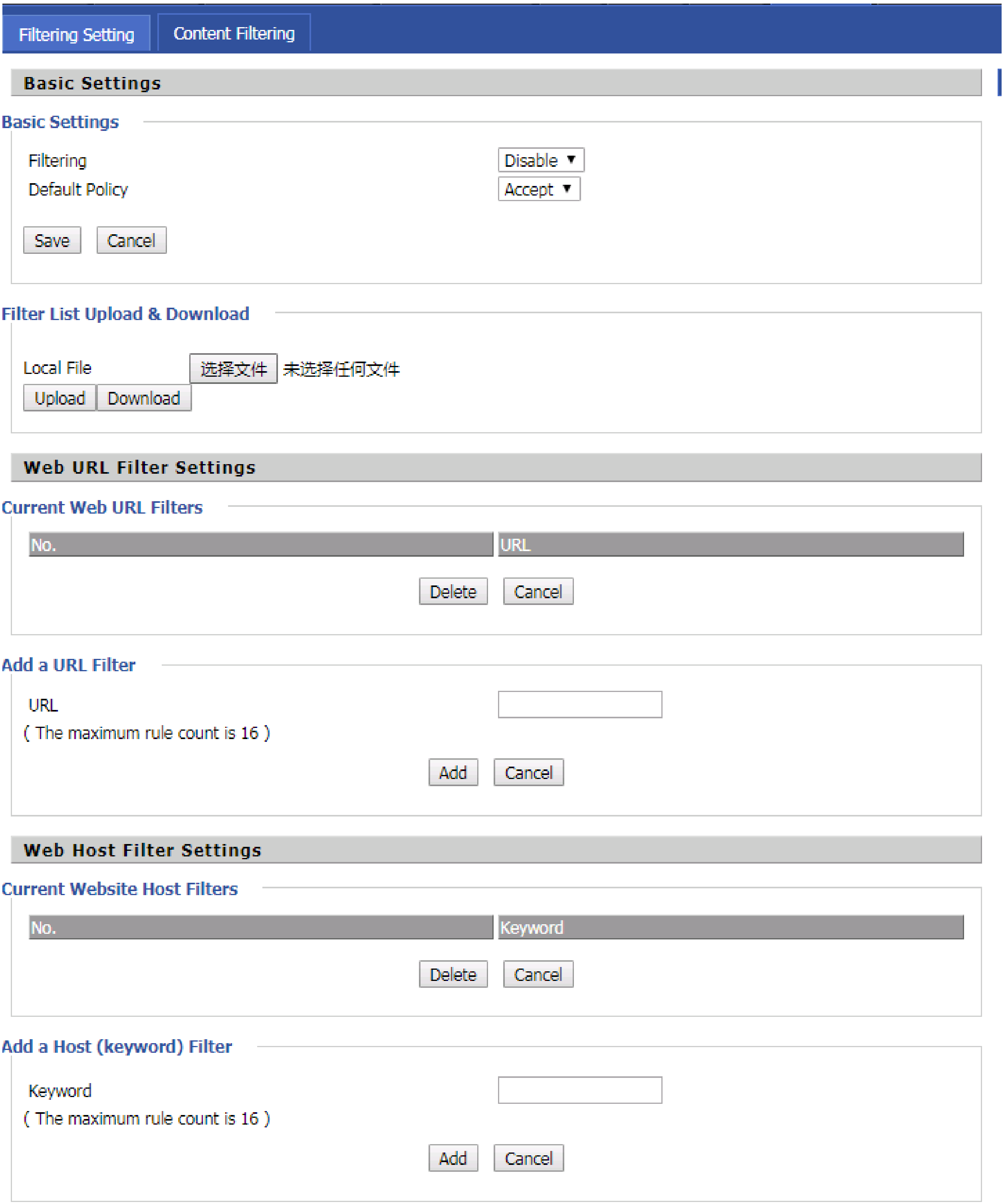
Filtering Setting



Field Name	Description
Filtering	Enable/Disable filter function
Default Policy	Choose to drop or accept filtered MAC addresses
Mac address	Add the Mac address filtering
Dest IP address	Destination IP address
Source IP address	Source IP address
Protocol	Select a protocol name, support for TCP, UDP and TCP/UDP
Dest. Port Range	Destination port ranges
Src Port Range	Source port range

Action	You can choose to receive or give up; this should be consistent with the default policy
Comment	Add callout
Delete	Delete selected item

Content Filtering



Field Name	Description
Filtering	Enable/Disable content Filtering
Default Policy	The default policy is to accept or to prohibit filtering rules
Current Webs URL	List the URL filtering rules that already existed (blacklist)
Delete/Cancel	You can choose to delete or cancel the existing filter rules
Add a URL Filter	Add URL filtering rules
Add/Cancel	Click adds to add one rule or click cancel
Current Website Host Filters	List the keywords that already exist (blacklist)
Delete/Cancel	You can choose to delete or cancel the existing filter rules the existing
Add a Host Filter	Add keywords
Add/Cancel	Click the Add or cancel

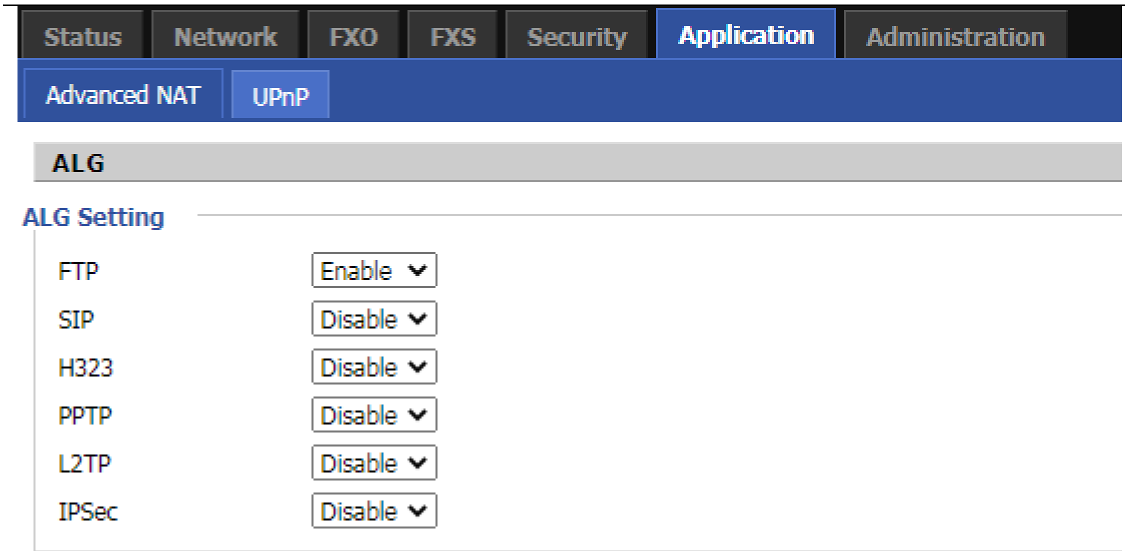
Application

Topics

Advance NAT

UPnP

Advance NAT

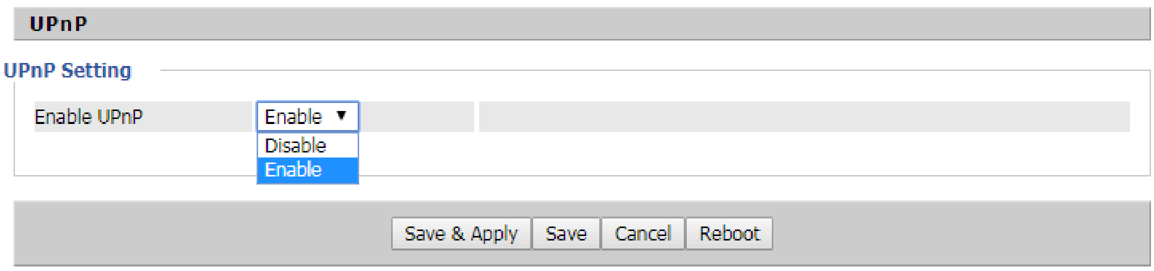


Description
Enable/Disable these functions (FTP/SIP/H323/PPTP/L2TP/IPSec)

UPnP

UPnP (Universal Plug and Play) supports zero-configuration networking, and can automatically discover a variety of networked devices. When UPnP is enabled, the connected device is allowed to access the network, obtain an IP address, and convey performance information. If the network has a DHCP and DNS server, the connected device can automatically obtain DHCP and DNS services.

UPnP devices can be automatically added to the network without affecting previously-connected devices.



Field Name	Description
UPnP enable	Enable/Disable UPnP function.

Administration

The user can manage the device in these webpages; you can configure the Time/Date, password, web access, system log and associated configuration TR069.

Topics

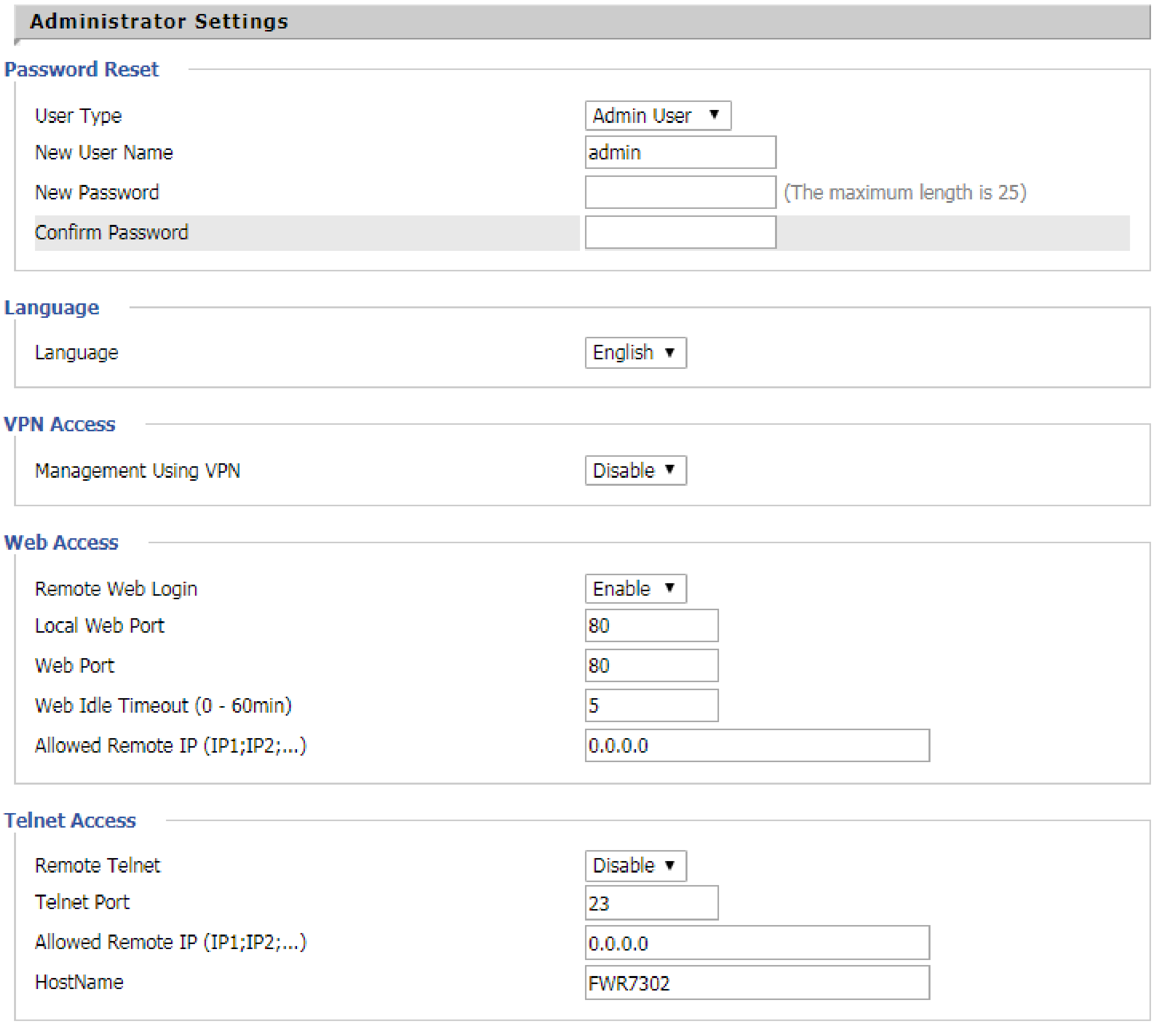
Management
Firmware Upgrade
Schedule Tasks
Provision
SNMP
TR-069
Diagnosis
Operating Mode

Management

Save config file

Field Name	Description
Config file upload and download	Upload: click on browse, select file in the local, press the upload button to begin uploading files
	Download: click to download, and then select contains the path to download the configuration file

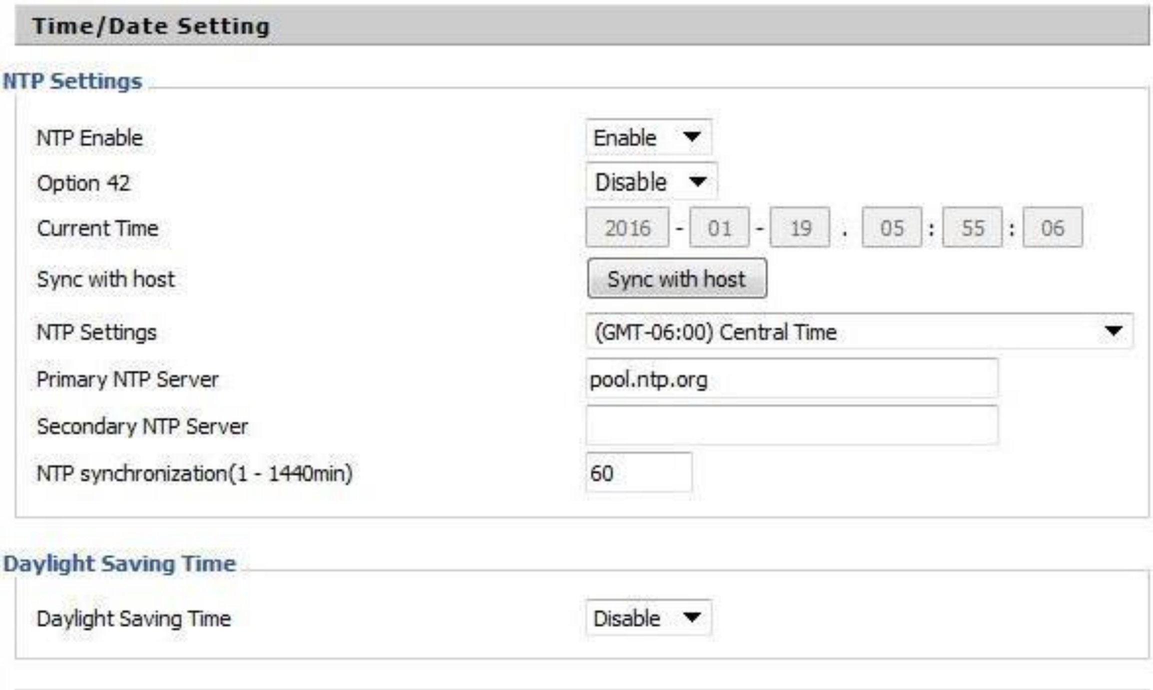
Administrator settings



Field Name	Description
User type	Choose the user type from admin user and normal user and basic user
New User Name	You can modify the username, set up a new user name
New Password	Input the new password
Confirm Password	Input the new password again
Language	Select the language for the web, the device support Chinese, English, and Spanish and so on
Remote Web Login	Enable/Disable remote Web login
Web Port	Set the port value which is used to login from Internet port and PC port, default is 80

Web Idle timeout	Set the Web Idle timeout time. The webpage can be logged out after Web Idle Timeout without any operation
Allowed Remote IP (IP1,	Set the IP from which a user can login the device remotely
Telnet Port	Set the port value which is used to telnet to the device

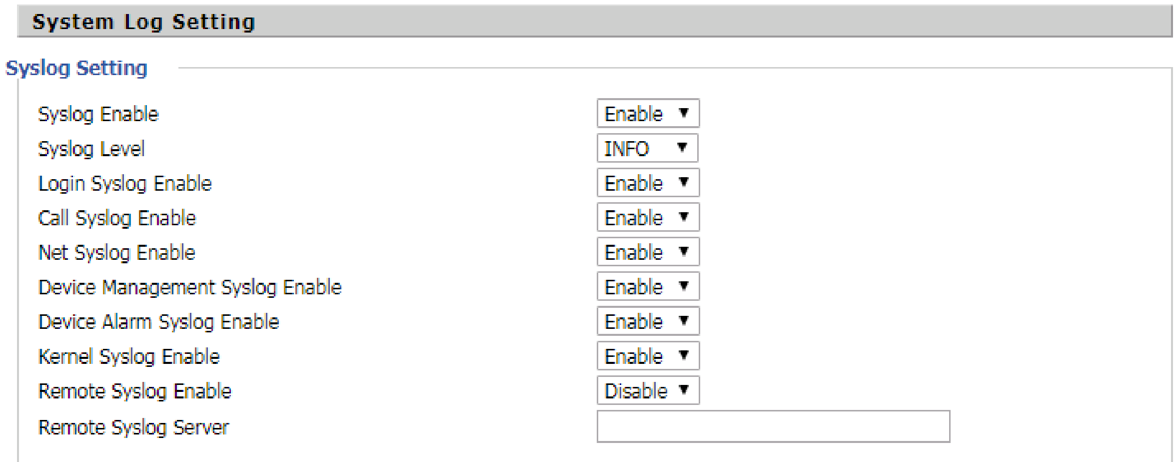
NTP settings



Field Name	Description
NTP Enable	Enable/Disable NTP
Option 42	Enable/Disable DHCP option 42. This option specifies a list of the NTP servers available to the client by IP address
Current Time	Display current time
NTP Settings	Setting the Time Zone
Primary NTP Server	Primary NTP server's IP address or domain name

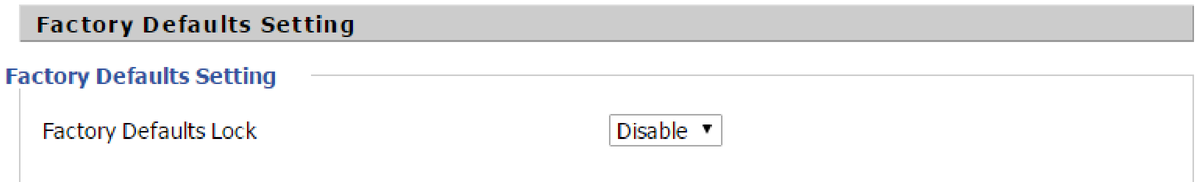
Secondary NTP Server	Options for NTP server's IP address or domain name
NTP synchronization	NTP synchronization cycle, cycle time can be 1 to 1440 minutes in any one, the default setting is 60 minutes

System Log Setting



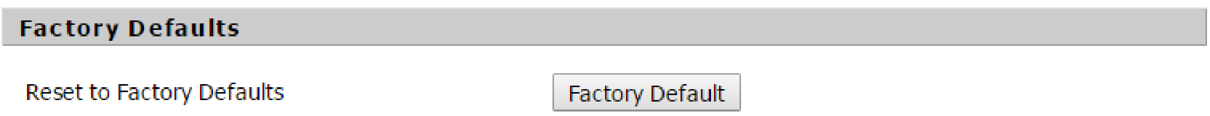
Field Name	Description
Syslog Enable	Enable/Disable syslog function
Syslog Level	Select the system log, there is INFO and Debug two grades, the Debug INFO can provide more information
Remote Syslog	Enable/Disable remote syslog function
Remote Syslog	Add a remote server IP address
Syslog Enable	Enable/Disable syslog function

Factory Defaults Setting



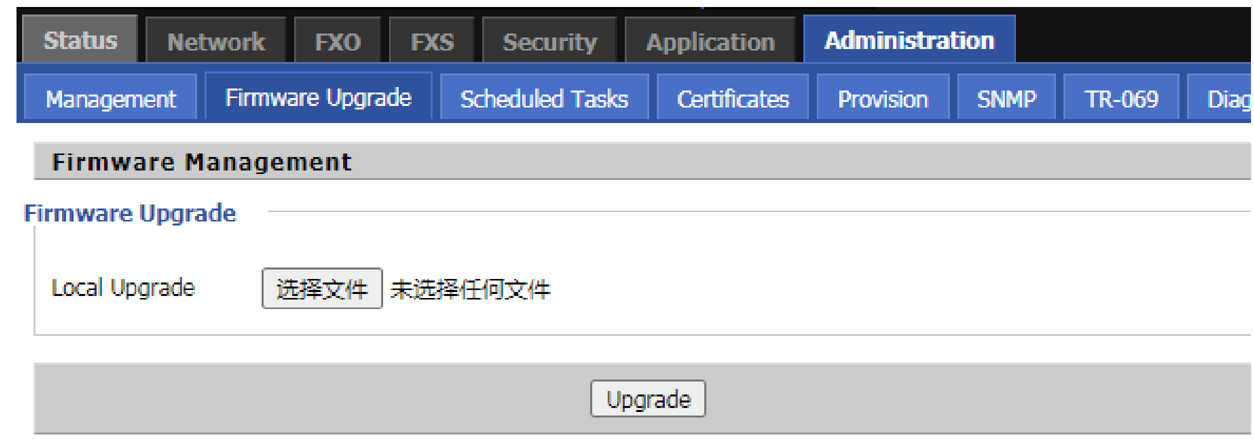
Description
When enabled, the device may not be reset to factory defaults until this parameter is reset to

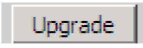
Factory Defaults



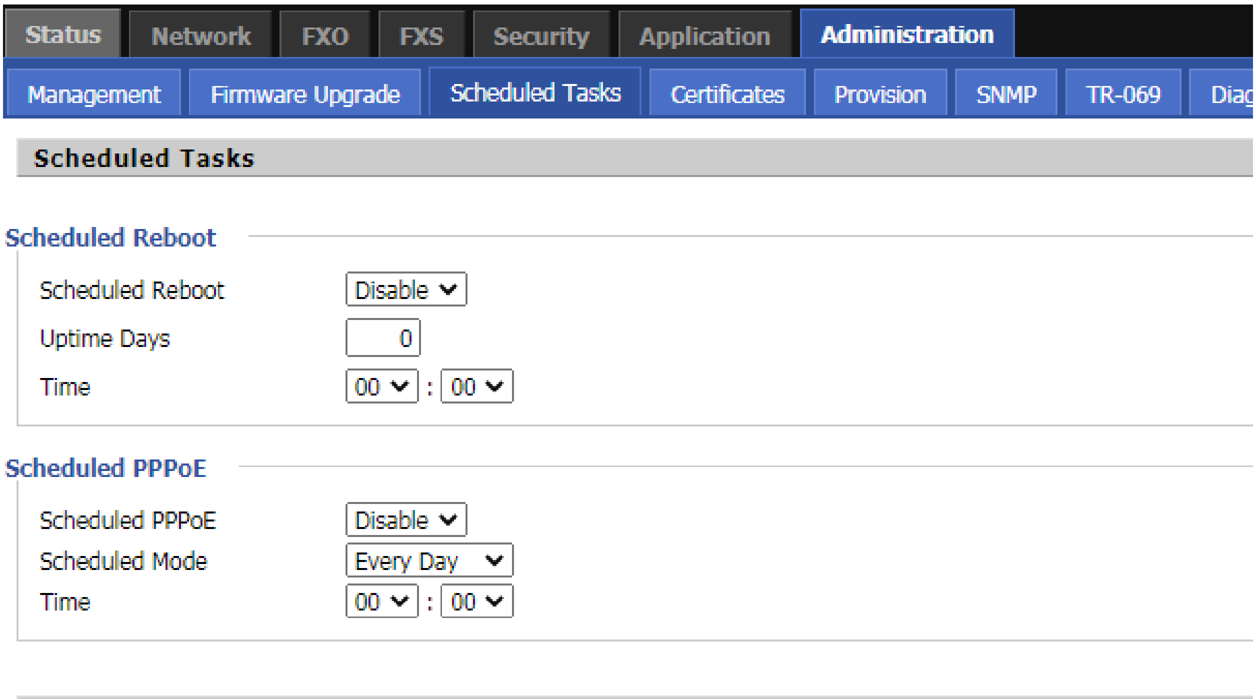
Description
Click Factory Default to restore the residential gateway to factory settings.

Firmware Upgrade



Description	
1.	Choose upgrade file type from Image File and Dial Rule
2.	Press “Browse..” button to browser file
3.	Press  to start upgrading

Scheduled Tasks

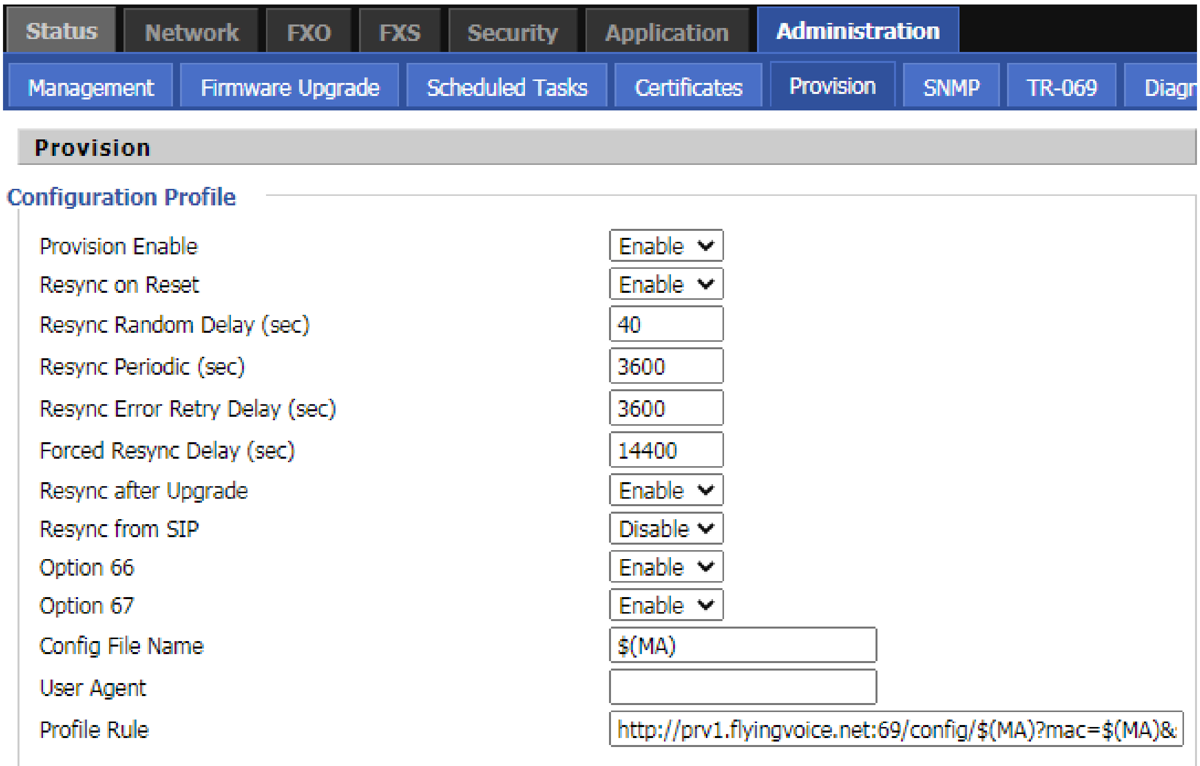


Field Name	Description
Scheduled Reboot	
Scheduled Reboot	Enable / disable scheduled reboot
Scheduled Mode	Choose work mode every day / week
Time	Set the time for scheduled reboot
Scheduled PPPoE	
Scheduled PPPoE	Enable / disable restart PPPoE
Scheduled Mode	Choose work mode every day / week
Time	Set the time for scheduled PPPoE

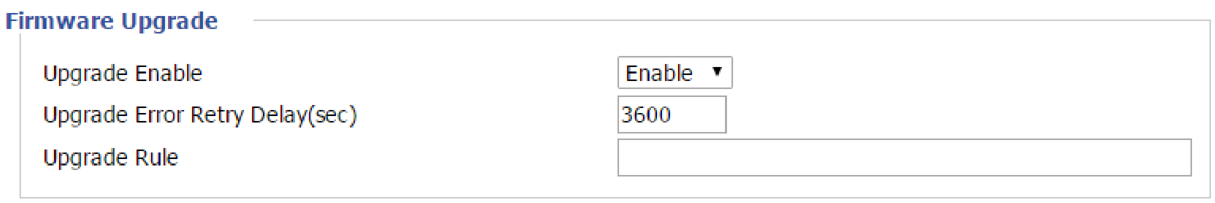
Provision

Provisioning allows the ATA to auto-upgrade and auto-configure devices which support TFTP, HTTP and HTTPs.

- Before testing or using TFTP, user should have TFTP server and upgrading file and configuring file.
- Before testing or using HTTP, user should have HTTP server and upgrading file and configuring file.
- Before testing or using HTTPS, user should have HTTPS server and upgrading file and configuring file and CA Certificate file (should same as https server's) and Client Certificate file and Private key file.
- User can upload a CA Certificate file and Client Certificate file and Private Key file in the Security page.

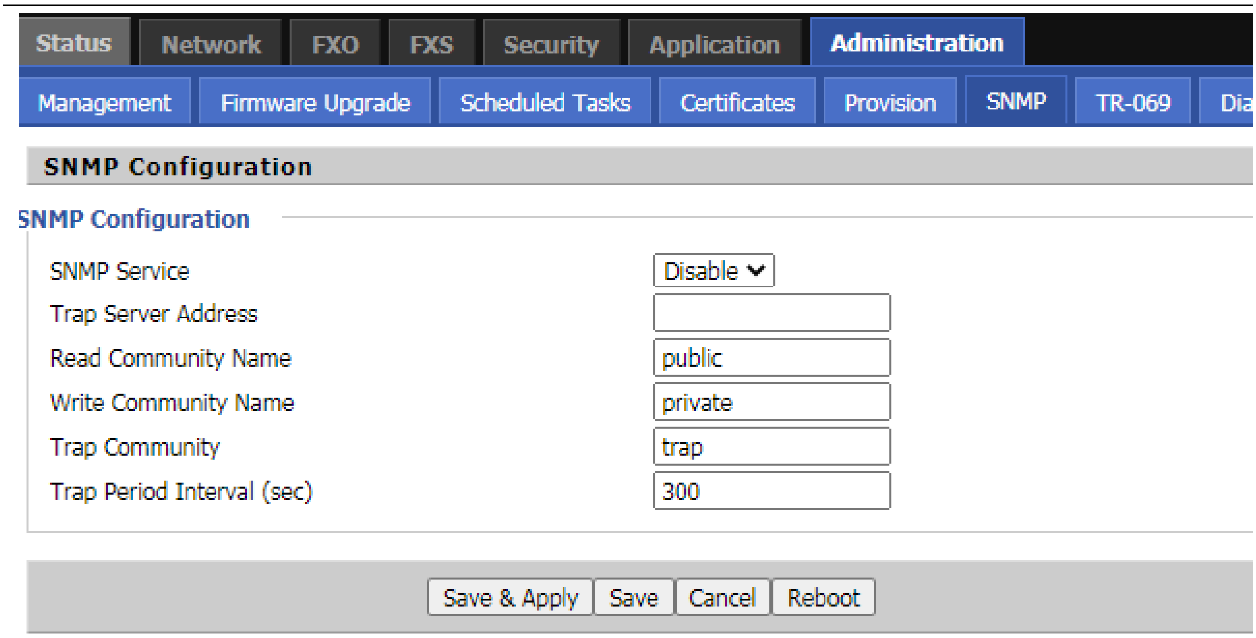


Field Name	Description
Provision Enable	Enable provision or not.
Resync on Reset	Enable resync after restart or not.
Resync Random Delay(sec)	Set the maximum delay for the request of synchronization file. The default is 40.
Resync Periodic(sec)	If the last resync was failure, The ATA will retry resync after the “Resync Error Retry Delay” time, default is 3600s.
Resync Error Retry	Set the periodic time for resync, default is 3600s.
Forced Resync Delay(sec)	If it’s time to resync, but the device is busy now, in this case, the ATA will wait for a period time, the longest is “Forced Resync Delay”, default is 14400s, when the time over, the ATA will forced to resync.
Resync After Upgrade	Enable firmware upgrade after resync or not. The default is Enabled.
Resync From SIP	Enable/Disable resync from SIP.
Option 66	It is used for In-house provision mode only. When use TFTP with option 66 to realize provisioning, user must input right configuration file name in the webpage. When disable Option 66, this parameter has no effect.
Config File Name	It is used for In-house provision mode only. When use TFTP with option 66 to realize provisioning, user must input right configuration file name in the webpage. When disable Option 66, this parameter has no effect.
Profile Rule	URL of profile provision file. Note that the specified file path is relative to the TFTP server’s virtual root directory.



Field Name	Description
Upgrade Enable	Enable firmware upgrade via provision or not
Upgrade Error Retry Delay(sec)	If the last upgrade fails, the ATA will try upgrading again after "Upgrade Error Retry Delay" period, default is 3600s
Upgrade Rule	URL of upgrade file

SNMP



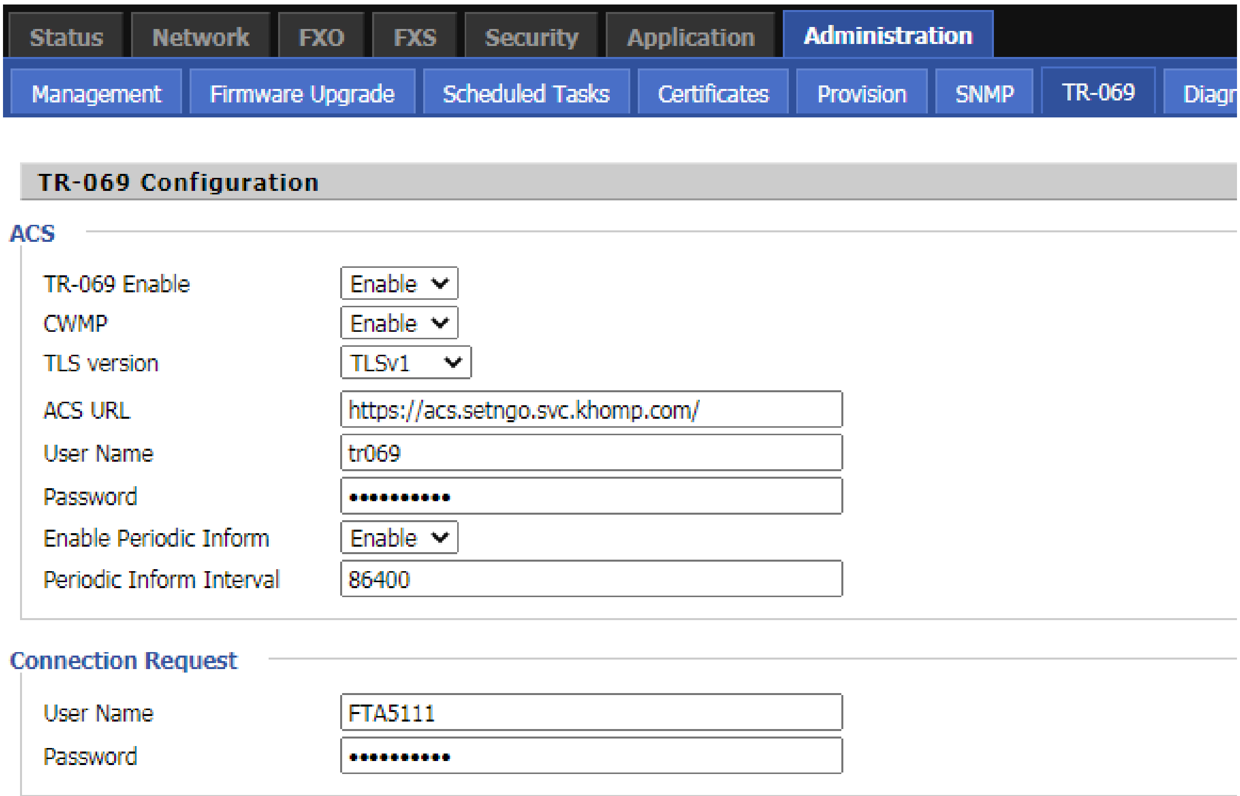
Field Name	Description
SNMP Service	Enable or Disable the SNMP service
Trap Server Address	Enter the trap server address for sending SNMP traps
Read Community Name	String value that is used as a password to request information via SNMP from the device
Write Community Name	String value that is used as a password to write configuration values to the device via SNMP
Trap Community	String value used as a password for retrieving traps from the device
Trap period interval(sec)	The interval for which traps are sent from the device

TR-069

TR-069 provides the possibility of auto configuration of internet access devices and reduces the cost of management. TR-069 (short for Technical Report 069) is a DSL Forum technical specification entitled CPE WAN Management Protocol (CWMP). It defines an application layer protocol for remote management of end-user devices. Using TR-069, the terminals establish connection with the Auto Configuration Servers (ACS) and get configured automatically.

Device Configuration using TR-069

The TR-069 configuration page is available under Administration menu.

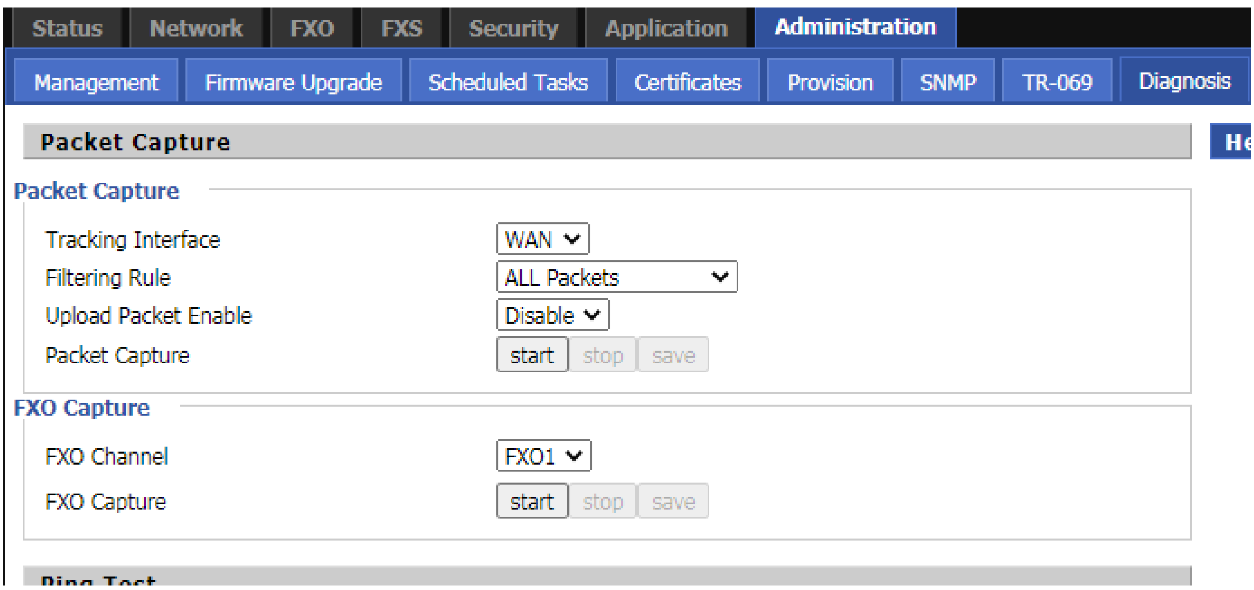


Field Name	Description
ACS parameters	
TR069 Enable	Enable or Disable TR069
CWMP	Enable or Disable CWMP
ACS URL	ACS URL address
User Name	ACS username
Password	ACS password

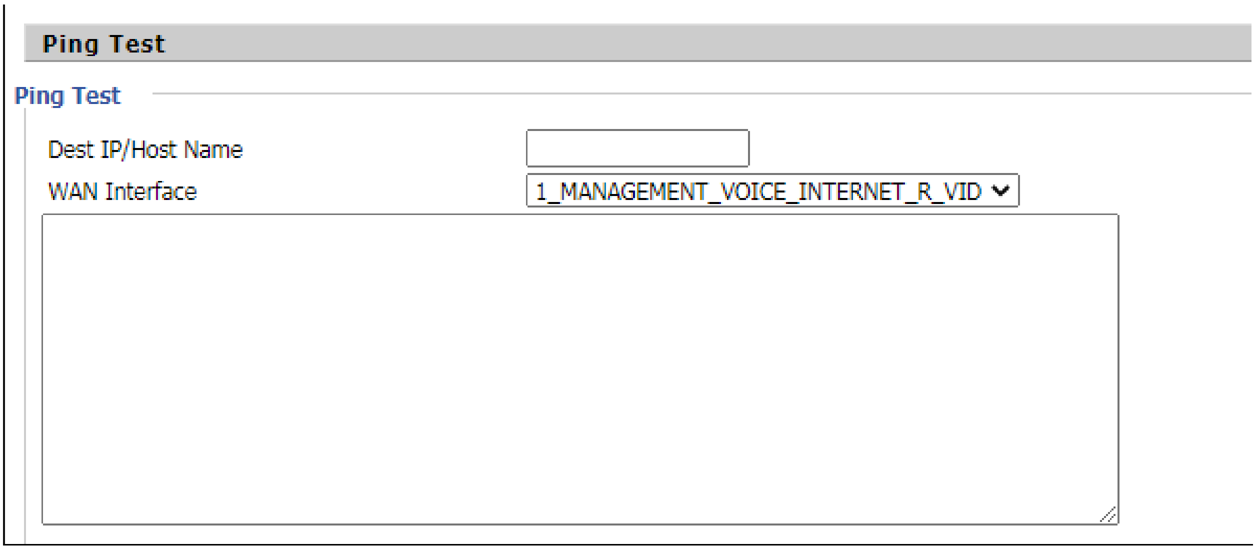
Periodic Inform Enable	Enable the function of periodic inform or not. By default, it is Enabled
Periodic Inform Interval	Periodic notification interval with the unit in seconds. The default value is 3600s
Connect Request parameters	
User Name	The username used to connect the TR069 server to the DUT
Password	The password used to connect the TR069 server to the DUT

Diagnosis

In this page, user can do packet trace, ping test and traceroute test to diagnose the device's connection status.

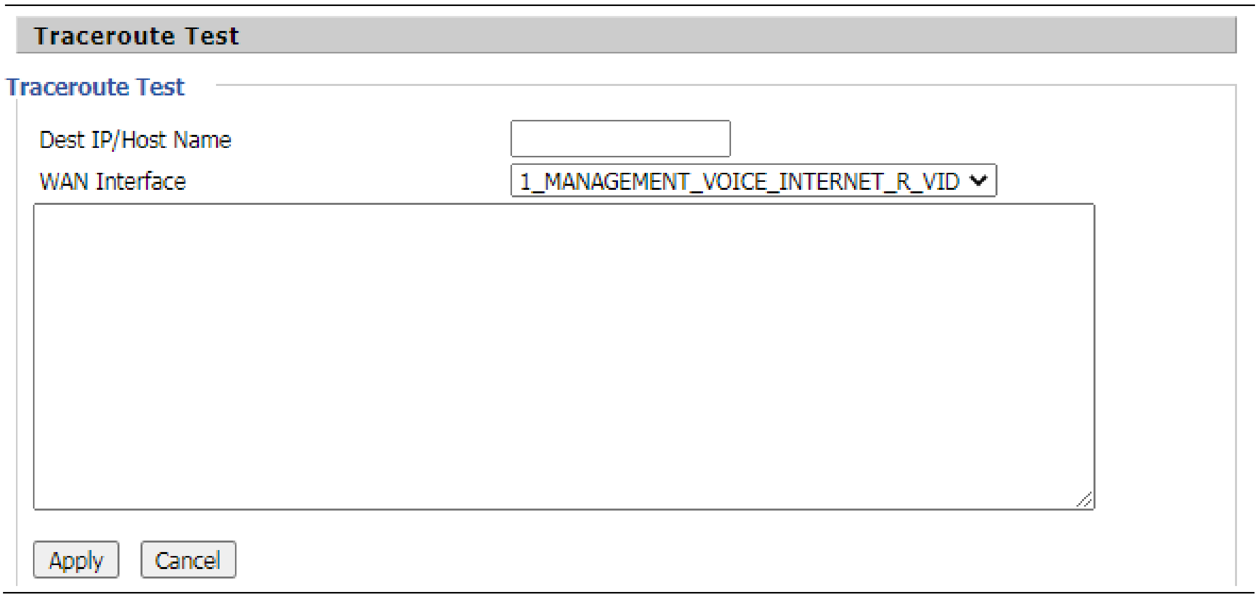


Description
1. Packet Trace Users can use the packet trace feature to intercept packets which traverse the device. Click the Start button to start home gateway tracking and keep refreshing the page until the message trace shows to stop, click the Save button to save captured packets.
2. Ping Test Enter the destination IP or host name, and then click Apply, device will perform ping test.

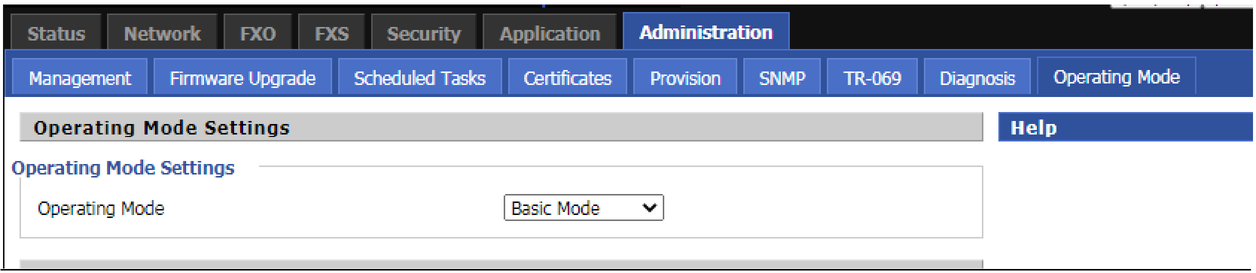


3. Traceroute Test

Enter the destination IP or host name, and then click Apply, device will perform traceroute test.



Operating Mode



Description
Choose the Operation Mode as Basic Mode or Advanced Mode.