



VOIP ADAPTER USER GUIDE

FTA5120

Version 1.0.0
Sep. 2021

Copyright

Copyright © Flyingvoice Network Technology CO., LTD.

Copyright © Flyingvoice Network Technology CO., LTD. All rights reserved. No parts of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, photocopying, recording, or otherwise, for any purpose, without the express written permission of Flyingvoice Network Technology CO., LTD. Under the law, reproducing includes translating into another language or format.

When this publication is made available on media, Flyingvoice Network Technology CO., LTD. gives its consent to downloading and printing copies of the content provided in this file only for private use but not for redistribution. No parts of this publication may be subject to alteration, modification or commercial use. Flyingvoice Network Technology CO., LTD. will not be liable for any damages arising from use of an illegally modified or altered publication.

Trademark

Flyingvoice®, the logo and the name and marks is 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.

Declaration of Conformity

Part 15 FCC Rules

This device complies with Part 15 of the FCC Rules. Operation is subject to the following three conditions:

- This device may not cause harmful interference.
- This device must accept any interference received, including interference that may cause undesired operation.
- The distance between user and products should be no less than 20cm.

Note: This equipment has been tested and found to comply with the limits of 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 energy, and if not installed and used in accordance with the instructions, may 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.

Note: the manufacturer is not responsible for any radio or TV interference caused by unauthorized modifications to this equipment. Such modifications could void the user's authority to operate this equipment.

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

CE

Manufacturer: Flyingvoice Network Technology Co., Ltd.

Address: Room 207~209, 2/F, Bldg B52#, Zhongchuang Industrial park, Liuxian Avenue, Taoyuan Street, Nanshan District, Shenzhen.

Hereby, Flyingvoice Network Technology Co., Ltd. declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU

A copy of the declaration of conformity can be obtained with this user manual; this product is not restricted in the EU.

The wireless operation frequency.

WiFi: 2412MHz-2472MHz, Max EIRP Power 19.36dBm.

Safety Warning and Attentions

If use adapter, adapter is required to comply 2014/30/EU Directive.

Adapter Caution: Adapter shall be installed near the equipment and shall be easily accessible.

Do not store or use your product in temperatures higher than 50°C.

RF Exposure Statement

The distance between user and products should be no less than 20cm.

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 FTA5120 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://priv3.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	6
Getting Started with Your ATA	7
Hardware Overview	7
FTA5120 Hardware	7
LED Indicator	7
Hardware Installation	8
Documents	9
Basic Features	10
ATA initialization	10
ATA Status	10
Basic Network Setting	11
Static IP	11
DHCP	12
PPPoE	13
Configuring SIP trunk	14
SIP trunk register	14
PSTN setting	15
Call Route	16
Advanced Web Configuration	16
Login	17
Status	17
System status	17
LAN Host	18
System Log	19
Network	20
WAN	20
LAN	26
VPN	29
DMZ	29
DDNS	30
QoS	30
Port Setting	31

Table of Contents

Routing	32
Advanced	32
FXO.....	33
SIP.....	33
FXO	38
Call Route	39
Dial Plan(SIP->FXO).....	40
Change Number(FXO->SIP)	41
Dial Plan Syntactic.....	42
Security	43
Filtering Setting.....	43
Content Filtering.....	45
Application.....	47
Advance NAT.....	47
UPnP	47
Administration	48
Management	48
Firmware Upgrade	52
Scheduled Tasks	53
Provision.....	53
SNMP	56
TR-069.....	57
Diagnosis.....	58
Operating Mode.....	60

About This Guide

Thank you for choosing Flyingvoice FTA5120, 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

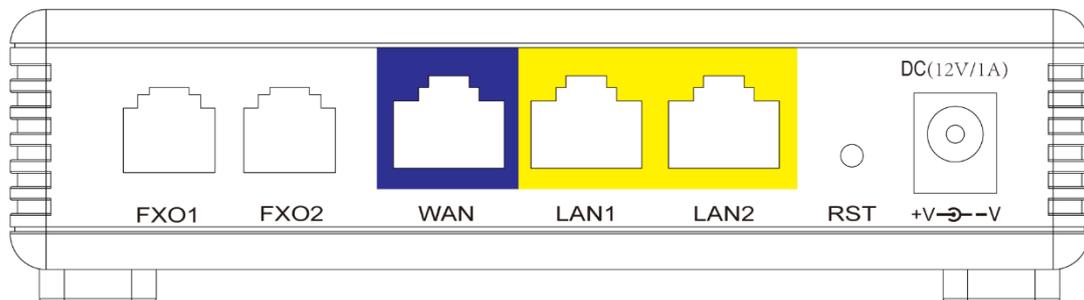
Topics

[FTA5120 Hardware](#)

[LED Indicator](#)

[Hardware Installation](#)

FTA5120 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	FXO1-FXO2	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
LAN	ON(GREEN)	Connected (Data)
	On Blinking (GREEN)	Connected (Registered)
	OFF	Disconnected/Power off
FXO	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 FXO 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 use 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](#)

[ATA Status](#)

[Basic Network Setting](#)

[Configuring SIP trunk](#)

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 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.

Static	
IP Address	<input type="text" value="192.168.10.173"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.10.1"/>
DNS Mode	<input type="text" value="Manual"/>
Primary DNS	<input type="text" value="192.168.10.1"/>
Secondary DNS	<input type="text" value="192.168.18.1"/>

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: <ol style="list-style-type: none"> 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 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.

INTERNET	
WAN	
Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID <input type="button" value="Delete Connect"/>
Service	MANAGEMENT_VOICE_INTERNET
IP Protocol Version	IPv4
WAN IP Mode	DHCP
DHCP Server	<input type="text"/>
MAC Address Clone	Disable
NAT Enable	Enable
VLAN Mode	Disable
VLAN ID	1 (1-4094)
DNS Mode	Auto
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
DHCP	
DHCP Renew	<input type="button" value="Renew"/>
DHCP Vendor (Option 60)	FLYINGVOICE-FWR7302

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.

INTERNET	
WAN	
Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID ▼ Delete Connect
Service	MANAGEMENT_VOICE_INTERNET ▼
IP Protocol Version	IPv4 ▼
WAN IP Mode	PPPoE ▼
MAC Address Clone	Disable ▼
NAT Enable	Enable ▼
VLAN Mode	Disable ▼
VLAN ID	1 (1-4094)
DNS Mode	Auto ▼
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
PPPoE	
PPPoE Account	<input type="text"/>
PPPoE Password	••••••••
Confirm Password	••••••••
Service Name	<input type="text"/>
	Leave empty to autodetect
Operation Mode	Keep Alive ▼
Keep Alive Redial Period(0-3600s)	5

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; <div style="display: flex; justify-content: space-between;"> Operation Mode On Demand ▾ </div> <div style="display: flex; justify-content: space-between;"> On Demand Idle Time(0-60m) 5 </div> 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

FTA5120 support forward call between SIP trunk and FXO.

SIP trunk register

Status	Network	FXO	Security	Application	Administration
SIP	FXO	Call Route	Dial Plan(SIP->FXO)	Change Number(FXO->SIP)	
SIP Trunk	SIP 1 ▾	Replicating Set between accounts		<input type="checkbox"/>	
Basic					
Basic Setup					
Register	Enable ▾				
Proxy and Registration					
Proxy Server	<input type="text"/>	Proxy Port	5060		
Outbound Server	<input type="text"/>	Outbound Port	<input type="text"/>		
Subscriber Information					
Display Name	<input type="text"/>	Phone Number	<input type="text"/>		
Account	<input type="text"/>	Password	<input type="text"/>		
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

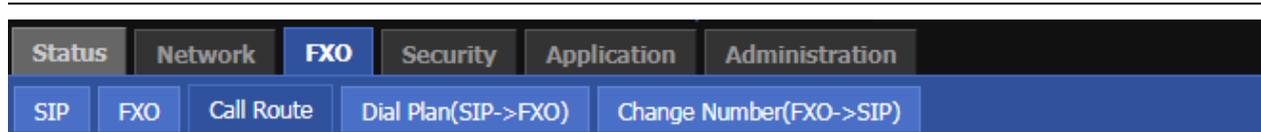
Basic

PSTN Trunk Outing

Tone Region	<input type="text" value="United States/North America"/>
Ring Back Type	<input type="text" value="Belgium (1s-3s)"/>
Impedance match FXO	<input type="text" value="600Ohms"/>
FXO Use Callerid	<input type="text" value="Yes"/>
FXO CH Cid Type	<input type="text" value="FSK"/>
FXO Minimum ring voltage	<input type="text" value="21V"/>
FXO TX Vol	<input type="text" value="GAIN_3DB"/>
FXO RX Vol	<input type="text" value="GAIN_6DB"/>
DTMF CID LEVEL	<input type="text"/>
Silence_Threshold	<input type="text"/>
FXO Backup	<input type="text" value="Disable"/>

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



Call Route Basic Configuration

Basic Setting

No.	Name	Origin	Destination	Dial Prefix	Strip	Priority	Changed number
1	<input type="checkbox"/>	<input type="text"/>					
2	<input type="checkbox"/>	<input type="text"/>					
3	<input type="checkbox"/>	<input type="text"/>					
4	<input type="checkbox"/>	<input type="text"/>					

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.

Advanced Web Configuration

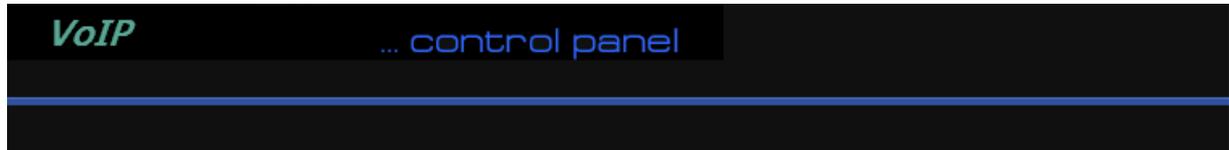
This chapter guides users to execute advanced (full) configuration through admin mode operation.

Topics:

[Login](#)

- [Status](#)
- [Network](#)
- [FXO](#)
- [Security](#)
- [Application](#)
- [Administration](#)

Login



Username	<input type="text" value="admin"/>
Password	<input type="password" value="****"/>
	<input type="button" value="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. and System Status.

System status

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:fe00:8101/64
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	2021-07-29 13:11:31
Elapsed Time	3 Mins

LAN Host

Basic LAN Host Syslog

LAN Host Info

MAC Address	IP Address	Interface Type	Address Source	Expires	Host Name	Status
00:21:F2:25:72:A1	192.168.1.43	LAN1	DHCP	14:14:22	FIP16	Active

System Log

Status	Network	FXO	FXS	Security	Application	Administration
Basic	LAN Host	Syslog				

Refresh Clear Save

```
Manufacturer:FLYINGVOICE
ProductClass:FTA5111
SerialNumber:FLY894315691235
BuildTime:202107300958
IP:192.168.1.1
HWVer:V4.5
SWVer:V3.20
<Wed Aug 25 10:59:36 2021> dnsmasq[4628]: using nameserver 2001:db8::20c:29ff:fe03:f91b#53
<Wed Aug 25 10:59:36 2021> dnsmasq[4628]: using nameserver 192.168.10.1#53
<Wed Aug 25 10:59:36 2021> dnsmasq[4628]: using nameserver 192.168.18.1#53
<Wed Aug 25 05:59:41 2021> udhcpd[9386]: Sending OFFER of 192.168.11.17
<Wed Aug 25 05:59:41 2021> udhcpd[9386]: Sending ACK to 192.168.11.17
<Wed Aug 25 05:59:44 2021> goahead[12986]: webs start...
<Wed Aug 25 23:02:33 2021> goahead[12986]: webs: Listening for HTTP requests at address 192.168.11.1...
```

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](#)

[Routing](#)

[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.

Static	
IP Address	<input type="text" value="192.168.10.173"/>
Subnet Mask	<input type="text" value="255.255.255.0"/>
Default Gateway	<input type="text" value="192.168.10.1"/>
DNS Mode	<input type="text" value="Manual"/>
Primary DNS	<input type="text" value="192.168.10.1"/>
Secondary DNS	<input type="text" value="192.168.18.1"/>

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: <ol style="list-style-type: none"> 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 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.

INTERNET	
WAN	
Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID ▼ Delete Connect
Service	MANAGEMENT_VOICE_INTERNET ▼
IP Protocol Version	IPv4 ▼
WAN IP Mode	DHCP ▼
DHCP Server	<input type="text"/>
MAC Address Clone	Disable ▼
NAT Enable	Enable ▼
VLAN Mode	Disable ▼
VLAN ID	1 (1-4094)
DNS Mode	Auto ▼
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
DHCP	
DHCP Renew	Renew
DHCP Vendor (Option 60)	FLYINGVOICE-FWR7302

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.

INTERNET	
WAN	
Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID ▼ Delete Connect
Service	MANAGEMENT_VOICE_INTERNET ▼
IP Protocol Version	IPv4 ▼
WAN IP Mode	PPPoE ▼
MAC Address Clone	Disable ▼
NAT Enable	Enable ▼
VLAN Mode	Disable ▼
VLAN ID	1 (1-4094)
DNS Mode	Auto ▼
Primary DNS	<input type="text"/>
Secondary DNS	<input type="text"/>
PPPoE	
PPPoE Account	<input type="text"/>
PPPoE Password	••••••••
Confirm Password	••••••••
Service Name	<input type="text"/>
	Leave empty to autodetect
Operation Mode	Keep Alive ▼
Keep Alive Redial Period(0-3600s)	5

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!\$+*

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.

INTERNET

WAN

Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID ▾	Delete Connect
Service	MANAGEMENT_VOICE_INTERNET ▾	
IP Protocol Version	IPv4 ▾	
WAN IP Mode	Bridge ▾	
Bridge Type	IP Bridge ▾	
DHCP Service Type	Pass Through ▾	
VLAN Mode	Disable ▾	
VLAN ID	1 (1-4094)	

Port Bind

Port_1
 Port_2
 Port_3
 Wireless(SSID)
 Wireless(SSID1)
 Wireless(SSID2)
 Wireless(SSID3)

Note : WAN connection can not be shared between the binding port , and finally bound port WAN connections bind operation will wash away before the other WAN connection to the port binding operation !

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 form 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.

Status	Network	FXO	Security	Application	Administration					
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	DMZ	VLAN	DDNS	QoS	Port

PC Port(LAN)

PC Port(LAN)

Local IP Address:

Local Subnet Mask:

Local DHCP Server:

DHCP Start Address:

DHCP End Address:

DNS Mode:

Primary DNS:

Secondary DNS:

Client Lease Time (0-86400s):

DHCP Static Allotment

NO.	MAC	IP Address
<input type="button" value="Delete Selected"/> <input type="button" value="Add"/> <input type="button" value="Edit"/>		

DNS Proxy:

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.

PC Port(LAN)

PC Port(LAN)

Local IP Address	<input type="text" value="192.168.11.1"/>
Local Subnet Mask	<input type="text" value="255.255.255.0"/>
Local DHCP Server	<input type="text" value="Enable"/>
DHCP Start Address	<input type="text" value="192.168.11.2"/>
DHCP End Address	<input type="text" value="192.168.11.254"/>
DNS Mode	<input type="text" value="Auto"/>

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

Primary DNS	<input type="text" value="192.168.11.1"/>
Secondary DNS	<input type="text" value="8.8.8.8"/>
Client Lease Time(0-86400s)	<input type="text" value="86400"/>
	<input type="button" value="DHCP Client List"/>

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

The screenshot shows the 'VPN Settings' section of the configuration interface. The 'VPN Enable' dropdown menu is open, displaying the following options: Disable (selected), PPTP, L2TP, and OpenVPN. Below the dropdown, there are buttons for 'Save', 'Save & Apply', 'Cancel', and 'Reboot'.

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

The screenshot shows the 'Demilitarized Zone (DMZ)' section of the configuration interface. The 'DMZ Enable' dropdown menu is open, displaying the option: Disable. Below the dropdown, there are buttons for 'Save & Apply', 'Save', 'Cancel', and 'Reboot'.

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

DDNS

DDNS Setting

Dynamic DNS Provider: NONE

Account:

Password:

DDNS URL:

Status: NONE

Save & Apply Save Cancel Reboot

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

Status **Network** FXO Security Application Administration
WAN LAN IPv6 Advanced IPv6 WAN IPv6 LAN VPN DMZ VLAN DDNS QoS Port Setting

QoS Bandwidth Setting

Enable QoS Disable ▾

Save Cancel

QoS Rules Setting

Name	Condition										Remark DSCP	Remark 802.1p	Remark VLAN
	Src.IP Address	Dst.IP Address	Protocol	Src.Port Range	Dst.Port Range	Physical Port	DSCP	802.1p	VLAN ID				

Delete Selected Add

Reboot

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

Status **Network** FXO Security Application Administration
WAN LAN IPv6 Advanced IPv6 WAN IPv6 LAN VPN DMZ VLAN DDNS QoS Port Setting Routing Ad

Port Setting Help

Port Setting

WAN Port Speed Nego Auto ▾

LAN1 Port Speed Nego Auto ▾

LAN2 Port Speed Nego Auto ▾

Save & Apply Save Cancel Reboot

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 Auto-negotiation, options are Auto, 100M full, 100M half, 10M half and 10M full.

Routing

Status	Network	FXO	Security	Application	Administration						
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	DMZ	VLAN	DDNS	QoS	Port Setting	Routing

Static Routing Settings Help

Add a routing rule

Destination

Host/Net

Gateway

Interface

Comment

Current Routing Table in the system

No.	Destination	Mask	Gateway	Flags	Metric	Interface	Comment
<input type="button" value="Delete Selected"/> <input type="button" value="Reset"/>							

StaticRoute (Option 121)

StaticRoute (Option 121)

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

Status	Network	FXO	Security	Application	Administration							
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	DMZ	VLAN	DDNS	QoS	Port Setting	Routing	Advance

[Help](#)

Most Nat connections (512-8192)	4096
MSS Mode	<input checked="" type="radio"/> Manual <input type="radio"/> Auto
MSS Value (1260-1460)	1440
Anti-DoS-P	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Conflict Detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Conflict Detection Interval(0-3600s)	0

Field Name	Description
Most Nat connections	The largest value
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](#)

[FXO](#)

[Call Route](#)

[Dial Plan \(SIP->FXO\)](#)

[Change Number \(FXO->SIP\)](#)

[Dial Plan Syntactic](#)

SIP

Basic

Status	Network	FXO	Security	Application	Administration
SIP	FXO	Call Route	Dial Plan(SIP->FXO)	Change Number(FXO->SIP)	
SIP Trunk		SIP 1 ▼		Replicating Set between accounts <input type="checkbox"/>	
Basic					
Basic Setup					
Register		Enable ▼			
Proxy and Registration					
Proxy Server		<input type="text"/>	Proxy Port		5060
Outbound Server		<input type="text"/>	Outbound Port		<input type="text"/>
Subscriber Information					
Display Name		<input type="text"/>	Phone Number		<input type="text"/>
Account		<input type="text"/>	Password		<input type="text"/>
Audio Configuration					
Codec Setup					
Audio Codec Type 1		G.711U ▼	Audio Codec Type 2		G.711A ▼
Audio Codec Type 3		GSM ▼	Audio Codec Type 4		G.726 ▼
Audio Codec Type 5		G.729 ▼			
Echo Cancel		Enable ▼			

Field name	Description
SIP trunk	Choose SIP trunk
Register	Enable: as VoIP terminal, register another 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

SIP Parameters

UDP Signal Port	<input type="text" value="5080"/>	
TCP Signal Port	<input type="text"/>	
TLS Signal Port	<input type="text"/>	
Use Random SIP Port	<input type="button" value="Disable"/>	
Min Random SIP Port	<input type="text" value="50000"/>	Max Random SIP Port <input type="text" value="60000"/>
Trunk Transport	<input type="button" value="UDP"/>	
Sip Trunk SRTP	<input type="button" value="Disable"/>	
Register Refresh Interval (60~3600 sec)	<input type="text" value="120"/>	
DTMF Mode	<input type="button" value="RFC2833"/>	
RFC2833 Payload (>=96)	<input type="text" value="101"/>	
RTP Port Min	<input type="text" value="10000"/>	
RTP Port Max	<input type="text" value="20000"/>	
FROMUSER FIELD	<input type="button" value="FROM SIPTRUNK-AND-PSTN"/>	
DIAL TIME	<input type="text" value="30"/>	
RPID From Sip Trunk	<input type="button" value="Sip Trunk Number"/>	
NAT NO Trunk	<input type="button" value="Yes"/>	
Tls Dont Verify Server	<input type="button" value="Yes"/>	

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

Layer 3 QoS

SIP QoS(0-63)

RTP QoS(0-63)

NAT Traversal Setting

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

NAT Traversal Setting

NAT Traversal Setting

Extern Host

Extern IP

Extern Refresh

Localnet

NAT MODE

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

STUN SETTING

STUN

STUNADDR

STUN REFRESH

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.

Configure SAS

SAS	Enable ▾	
Partysip Port	5070	
Customer Reg Port	5060	
Qualify	no ▾	
Qualify Freq(s)	60	
Record Route	Off ▾	
Outbound Proxy		Outbound Port <input type="text"/>

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

Basic

PSTN Trunk Outing

Tone Region	United States/North America ▾
Ring Back Type	Belgium (1s-3s) ▾
Impedance match FXO	600Ohms ▾
FXO Use Callerid	Yes ▾
FXO CH Cid Type	FSK ▾
FXO Minimum ring voltage	21V ▾
FXO TX Vol	GAIN_3DB ▾
FXO RX Vol	GAIN_6DB ▾
DTMF CID LEVEL	<input type="text"/>
Silence_Threshold	<input type="text"/>
FXO Backup	Disable ▾

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

Supplementary Services

Auto Answer Sip-trunk Call	Disable ▾
DTMF Sequence Generate FXO HOOK FLASH	**123
Hook Flash Time FXO	200ms ▾
Collect Call Control FXO	Disable ▾
Block Collect Interval Time FXO	200ms ▾

Field Name	Description
Auto Answer Sip-trunk Call	Enable: support two-stage dialing users could call sip trunk number, then dial outgoing 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

Call Route Basic Configuration

Basic Setting

No.	Name	Origin	Destination	Dial Prefix	Strip	Priority	Changed number
1	<input checked="" type="checkbox"/>	<input type="text"/>					
2	<input type="checkbox"/>	<input type="text"/>					
3	<input type="checkbox"/>	<input type="text"/>					
4	<input type="checkbox"/>	<input type="text"/>					

Name

Origin

Destination

Dial Prefix

Strip

Priority

Changed number

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)

SIP FXO Call Route **Dial Plan(SIP->FXO)** Change Number(FXO->SIP)

Dial Rule

General

Dial Rule

Unmatched Policy

No.	Line	Digit Map	Action	Move Up	Move Down	<input type="checkbox"/>
<input type="button" value="Edit"/> <input type="button" value="Add"/> <input type="button" value="Delete"/>						
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Reboot"/>						

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)

SIP FXO Call Route Dial Plan(SIP->FXO) **Change Number(FXO->SIP)**

Changed number

General

Changed number

No.	Line	Digit Map	Move Up	Move Down	<input type="checkbox"/>
<input type="button" value="Edit"/> <input type="button" value="Add"/> <input type="button" value="Delete"/>					
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Reboot"/>					

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 [23-5*]: 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	<p>Make outside dial tone after dialing “x”, stop until dialing character “y”</p> <p>For example:</p> <p>“9,1xxxxxxxx”: the device reports dial tone after inputting “9”, stops tone until inputting “1”</p> <p>“9,8,010x”: make outside dial tone after inputting “9”, stop tone until inputting “0”</p>
7	T	<p>Set the delayed time. For example:</p> <p>“<9:111>T2”: The device will dial out the matched number “111” after 2 seconds</p>

Security

Topics

[Filtering Setting](#)

[Content Filtering](#)

Filtering Setting

Basic Settings

Basic Settings

Filtering Disable ▾

Default Policy Drop ▾

The packet that don't match with any rules would be Drop

IP/Port Filter Settings

Interface LAN ▾

Mac address

Dest IP Address

Source IP Address

Protocol NONE ▾

Dest. Port Range -

Src Port Range -

Action Accept ▾

Comment

(The maximum rule count is 32)

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

Filtering Setting Content Filtering

Basic Settings

Basic Settings
Filtering Disable ▾
Default Policy Accept ▾
Save Cancel

Filter List Upload & Download
Local File 选择文件 未选择任何文件
Upload Download

Web URL Filter Settings

Current Web URL Filters

No.	URL
-----	-----

Delete Cancel

Add a URL Filter
URL
(The maximum rule count is 16)
Add Cancel

Web Host Filter Settings

Current Website Host Filters

No.	Keyword
-----	---------

Delete Cancel

Add a Host (keyword) Filter
Keyword
(The maximum rule count is 16)
Add Cancel

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

Status
Network
FXO
FXS
Security
Application
Administration

Advanced NAT
UPnP

ALG

ALG Setting

FTP	Enable ▼
SIP	Disable ▼
H323	Disable ▼
PPTP	Disable ▼
L2TP	Disable ▼
IPSec	Disable ▼

Description

Enable/Disable these function(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.

UPnP

UPnP Setting

Enable UPnP	<div style="border: 1px solid #ccc; padding: 2px; display: inline-block;"> Enable ▼ Disable Enable </div>
-------------	---

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

Save Config File

Config File Upload && Download

Local File 未选择任何文件

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

Administrator Settings	
Password Reset	
User Type	Admin User ▼
New User Name	admin
New Password	<input type="text"/> (The maximum length is 25)
Confirm Password	<input type="text"/>
Language	
Language	English ▼
VPN Access	
Management Using VPN	Disable ▼
Web Access	
Remote Web Login	Enable ▼
Local Web Port	80
Web Port	80
Web Idle Timeout (0 - 60min)	5
Allowed Remote IP (IP1;IP2;...)	0.0.0.0
Telnet Access	
Remote Telnet	Disable ▼
Telnet Port	23
Allowed Remote IP (IP1;IP2;...)	0.0.0.0
HostName	FWR7302

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 user name, 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,IP2,...)	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

Time/Date Setting

NTP Settings

NTP Enable Enable ▼

Option 42 Disable ▼

Current Time 2016 - 01 - 19 . 05 : 55 : 06

Sync with host Sync with host

NTP Settings (GMT-06:00) Central Time ▼

Primary NTP Server pool.ntp.org

Secondary NTP Server

NTP synchronization(1 - 1440min) 60

Daylight Saving Time

Daylight Saving Time Disable ▼

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

System Log Setting

Syslog Setting

Syslog Enable	Enable ▼
Syslog Level	INFO ▼
Login Syslog Enable	Enable ▼
Call Syslog Enable	Enable ▼
Net Syslog Enable	Enable ▼
Device Management Syslog Enable	Enable ▼
Device Alarm Syslog Enable	Enable ▼
Kernel Syslog Enable	Enable ▼
Remote Syslog Enable	Disable ▼
Remote Syslog Server	<input style="width: 100%;" type="text"/>

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

Factory Defaults Setting

Factory Defaults Setting

Factory Defaults Lock	Disable ▼
-----------------------	-----------

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

Factory Defaults

Factory Defaults

Reset to Factory Defaults	<input type="button" value="Factory Default"/>
---------------------------	--

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

Firmware Upgrade

Status	Network	FXO	FXS	Security	Application	Administration		
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diag	

Firmware Management

Firmware Upgrade

Local Upgrade 未选择任何文件

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

Status	Network	FXO	FXS	Security	Application	Administration
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069

Scheduled Tasks

Scheduled Reboot

Scheduled Reboot	Disable ▾
Uptime Days	0
Time	00 ▾ : 00 ▾

Scheduled PPPoE

Scheduled PPPoE	Disable ▾
Scheduled Mode	Every Day ▾
Time	00 ▾ : 00 ▾

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.

Status	Network	FXO	FXS	Security	Application	Administration
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069
Provision						
Configuration Profile						
Provision Enable						Enable ▼
Resync on Reset						Enable ▼
Resync Random Delay (sec)						40
Resync Periodic (sec)						3600
Resync Error Retry Delay (sec)						3600
Forced Resync Delay (sec)						14400
Resync after Upgrade						Enable ▼
Resync from SIP						Disable ▼
Option 66						Enable ▼
Option 67						Enable ▼
Config File Name						\$(MA)
User Agent						
Profile Rule						http://prv1.flyingvoice.net:69/config/\$(MA)?mac=\$(MA)&

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	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.

Firmware Upgrade

Upgrade Enable

Enable ▾

Upgrade Error Retry Delay(sec)

3600

Upgrade Rule

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

Status	Network	FXO	FXS	Security	Application	Administration
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069

SNMP Configuration

SNMP Configuration

SNMP Service	Disable ▾
Trap Server Address	<input type="text"/>
Read Community Name	public
Write Community Name	private
Trap Community	trap
Trap Period Interval (sec)	300

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.

Status	Network	FXO	FXS	Security	Application	Administration
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069

TR-069 Configuration

ACS

TR-069 Enable	Enable ▾
CWMP	Enable ▾
TLS version	TLSv1 ▾
ACS URL	<input type="text" value="https://acs.setngo.svc.khomp.com/"/>
User Name	<input type="text" value="tr069"/>
Password	<input type="password" value="....."/>
Enable Periodic Inform	Enable ▾
Periodic Inform Interval	<input type="text" value="86400"/>

Connection Request

User Name	<input type="text" value="FTA5111"/>
Password	<input type="password" value="....."/>

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

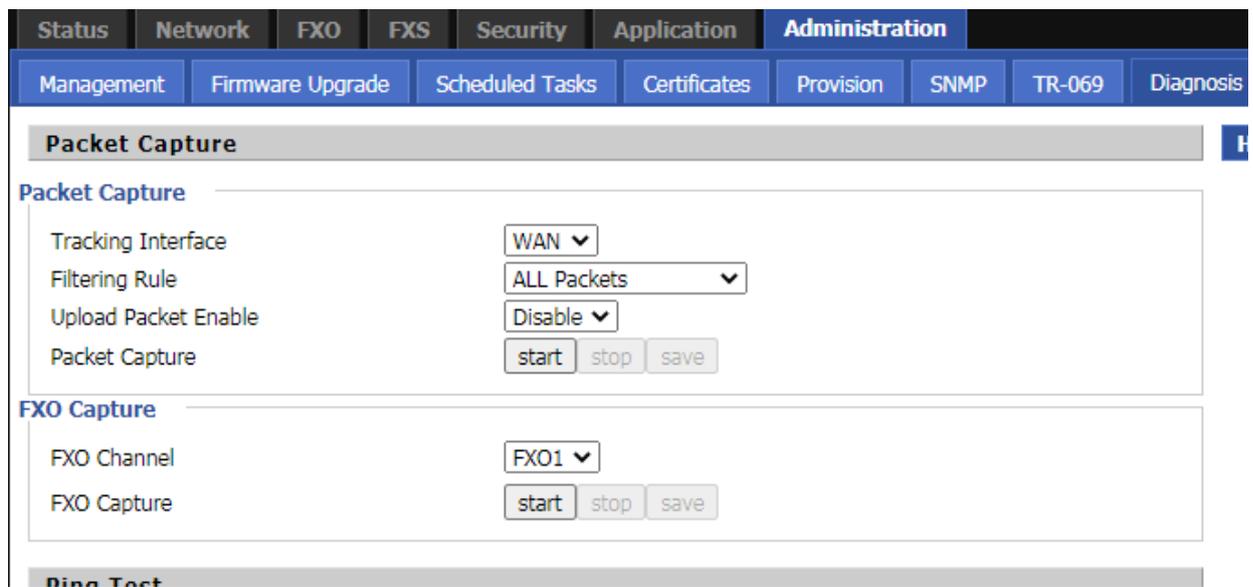
Periodic Inform Enable	Enable the function of periodic inform or not. By default it is Enabled
Periodic Inform Interval	Periodic notification interval with the unit in seconds. The default value is 3600s

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.

Ping Test

Ping Test

Dest IP/Host Name

WAN Interface

3. Traceroute Test

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

Traceroute Test

Traceroute Test

Dest IP/Host Name

WAN Interface

Operating Mode

Status	Network	FXO	FXS	Security	Application	Administration			
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diagnosis	Operating Mode	
Operating Mode Settings									Help
Operating Mode Settings									
Operating Mode <input type="text" value="Basic Mode"/>									

Description

Choose the Operation Mode as Basic Mode or Advanced Mode.
