



V1.20210315

Contents

.....	1
About This User Guide	1
Contacting ReadyNet	2
Purpose	3
Cross references.....	3
Feedback	3
Declaration of Conformity	4
Part 15 FCC Rules	4
Warnings and Notes	5
Warnings	5
Notes	5
Chapter 1: Product Description	6
AC1100MSF.....	7
Table 1 Features at-a-glance	7
LED Indicators and Interfaces	8
Table 2 LED Indicators	8
Table 3 Interfaces	9
Voice Prompt	12
Table 4 Voice Menu Setting Options	12
Chapter 2 Configuring Basic Settings	17
Two-Level Management	18
Web Management Interface	18
Web Management Interface Details.....	20
Table 5 Web management interface	20
Setting the Time Zone	21
Table 6 Setting time zone	21
Configuring an Internet Connection.....	22
Table 7 Configuring an internet connection	22
Setting up Wireless Connections.....	24
Table 9 Wireless Security web page	26
Configuring Session Initiation Protocol (SIP)	27
Table 10 Configuring SIP the Web Management Interface	27
Table 11 Registration status	28
Making a Call	29
.....	31
Chapter 3: Web Interface	31
Login	32
Table 12 Login details	32
Status	33

Contents

Table 13 Status Page	33
Network and Security	37
WAN	37
Table 14 Internet	37
Table 15 DHCP	38
Table 16 PPPoE	39
Table 17 Bridge Mode	41
LAN	43
Table 18 LAN port	43
Table 19 DHCP server settings.....	45
Table 20 DHCP server, DNS and Client Lease Time.....	45
LTE	46
Table 21 LTE.....	46
Table 22 VPN	47
Table 22 Port Forward.....	48
Table 23 VLAN	49
Table 24 DMZ.....	50
Table 25 DDNS	50
Table 26 QoS.....	51
Table 27 Port setting	52
Table 28 Routing.....	52
Table 29 Advance.....	53
Wireless 2.4G.....	54
Table 30 Basic	54
Table 31 Wireless security	57
Table 32 Wi-Fi Security Setting.....	58
Table 33 WPA-PSK	59
Table 34 WPAPSKWPA2PSK.....	59
Table 35 Wireless Access Policy.....	60
Table 36 WMM	61
Table 37 WDS	62
Table 38 WPS.....	63
Table 39 Station info	64
Table 40 Advanced.....	65
Wireless 5G.....	67
SIP	68
Table 41 SIP settings	68
Table 42 VoIP QoS.....	69
Table 43 Parameters and settings	70
Table 44 Adding one dial plan.....	72
Table 45 Dial Plan	73
Table 46 Blacklist	74
Table 47 Call log.....	75
FXS1	77

Contents

Table 48 SIP Account - Basic.....	77
Table 49 Audio configuration.....	78
Table 50 Supplementary service.....	79
Table 51 Advanced.....	80
Table 52 Volume settings.....	82
Table 53 Regional.....	83
Table 54 Features and call forward.....	84
Table 55 Miscellaneous	86
FXS2	87
Security	88
Table 56 Filtering setting	88
Table 57 Content filtering	89
Application.....	91
Table 58 advance NAT	91
Table 59 UPnP.....	91
Table 60 IGMP	92
Storage.....	93
Table 61 Disk Management	93
.....	93
Table 62 FTP Setting	94
Table 63 Smb setting	95
Administration	96
Management.....	96
Table 64 Save Config File	96
Table 65 Administrator settings	97
Table 66 NTP settings	98
Table 67 Daylight Saving Time.....	99
Table 68 System log Setting	100
Table 69 Factory Defaults Setting.....	100
Table 70 Factory Defaults	101
Firmware Upgrade	101
Table 71 Firmware upgrade	101
LTE Upgrade	102
Table 72 LTE upgrade	102
Table 73 Scheduled Tasks	102
Provision.....	103
Table 74 Provision.....	104
Table 75 Firmware Upgrade.....	105
SNMP	106
Table 76 SNMP.....	106
TR-069	107
Table 77 TR069	107
Diagnosis	109
Table 78 Diagnosis	109

Contents

Operating Mode	111
Table 79 Operating mode	111
System Log	112
Table 80 System log	112
Logout	112
Table 81 Logout	112
Reboot.....	112
Chapter 4 IPv6 address configuration	113
Introduction	114
Table 82 IPv6 Modes	114
IPv6 Advance	115
Table 83 Enabling IPv6.....	115
Configuring IPv6	115
Table 84 Configuring Statefull IPv6.....	116
Table 85 Configuring Stateless IPv6	117
Viewing WAN port status	118
IPv6 DHCP configuration for LAN/WLAN clients	118
LAN DHCPv6	119
Chapter 5 Troubleshooting Guide.....	120
Configuring PC to get IP Address automatically	121
Cannot connect to the Web	122
Forgotten Password	122
Chapter 6: Appendix A – Auto Provisioning Manual	123

Tables

Table 1 Features at-a-glance.....	7
Table 2 LED Indicators.....	8
Table 3 Interfaces	11
Table 4 Voice Menu Setting Options	15
Table 5 Web management interface	23
Table 6 Setting time zone	24
Table 7 Configuring an internet connection	25
Table 9 Wireless Security web page	29
Table 10 Configuring SIP the Web Management Interface.....	30
Table 11 Registration status	31
Table 12 Login details	35
Table 13 Status Page.....	36
Table 14 Internet	40
Table 15 DHCP	41
Table 16 PPPoE	42
Table 17 Bridge Mode.....	44
Table 18 LAN port	46
Table 19 DHCP server settings	48
Table 20 DHCP server, DNS and Client Lease Time.....	48
Table 21 LTE.....	49
Table 22 VPN.....	50
Table 22 Port Forward	51
Table 23 VLAN.....	52
Table 24 DMZ.....	53
Table 25 DDNS	53
Table 26 QoS.....	54
Table 27 Port setting.....	55
Table 28 Routing	55
Table 29 Advance	56
Table 30 Basic	57
Table 31 Wireless security	60
Table 32 Wi-Fi Security Setting	61
Table 33 WPA-PSK	62
Table 34 WPAPSKWPA2PSK.....	62
Table 35 Wireless Access Policy.....	63

Table 36	WMM	64
Table 37	WDS	65
Table 38	WPS	66
Table 39	Station info	67
Table 40	Advanced	68
Table 41	SIP settings	71
Table 42	VoIP QoS	72
Table 43	Parameters and settings	73
Table 44	Adding one dial plan	74
Table 45	Dial Plan	75
Table 46	Blacklist	76
Table 47	Call log	77
Table 48	SIP Account - Basic	79
Table 49	Audio configuration	80
Table 50	Supplementary service	81
Table 51	Advanced	82
Table 52	Volume settings	84
Table 53	Regional	85
Table 54	Features and call forward	86
Table 55	Miscellaneous	88
Table 56	Filtering setting	90
Table 57	Content filtering	91
Table 58	advance NAT	93
Table 59	UPnP	93
Table 60	IGMP	94
Table 61	Disk Management	95
Table 62	FTP Setting	96
Table 63	Smb setting	97
Table 64	Save Config File	98
Table 65	Administrator settings	99
Table 66	NTP settings	100
Table 67	Daylight Saving Time	101
Table 68	System log Setting	102
Table 69	Factory Defaults Setting	102
Table 70	Factory Defaults	103
Table 71	Firmware upgrade	103
Table 72	LTE upgrade	104
Table 73	Scheduled Tasks	104
Table 74	Provision	106
Table 75	Firmware Upgrade	107
Table 76	SNMP	108

Table

Table 77 TR069	109
Table 78 Diagnosis	111
Table 79 Operating mode	113
Table 80 System log	114
Table 81 Logout	114
Table 82 IPv6 Modes.....	116
Table 83 Enabling IPv6.....	117
Table 84 Configuring Statefull IPv6.....	118
Table 85 Configuring Stateless IPv6.....	119

About This User Guide

Thank you for choosing the AC1100MSF wireless router with VoIP. This product will allow you to make ATA call using your broadband connection, and provides Wi-Fi router function. This manual provides basic information on how to install and connect the AC1100MSF wireless router with VoIP to the Internet. It also includes features and functions of wireless router with VoIP components, and how to use it correctly. Before you can connect the AC1100MSF to the Internet and use it, you must have a high-speed broadband connection installed. A high-speed connection includes environments such as DSL, cable modem, and a leased line. The AC1100MSF wireless router with VoIP is a stand-alone device, which requires no PC to make Internet calls. This product guarantees clear and reliable voice quality on the Internet, which is fully compatible with SIP industry standards and able to interoperate with many other SIP devices and software on the market.



This guide contains the following chapters:

- [Chapter 1: Product description](#)
- [Chapter 2: Configuring Basic Settings](#)
- [Chapter 3: Web Interface Management](#)
- [Chapter 4: Managing device](#)
- [Chapter 5: Troubleshooting Guide](#)

Contacting ReadyNet

Main Phone Line: +1 (801) 566-0100

Sales Department: +1 (801) 984-5133, +1 (801) 984-5130

Customer Service: +1 (801) 566-0100, Option 1

Service Provider Support: +1 (855) 671-7932

Sales: sales@readynetsolutions.com

Customer Support: customerservice@readynetsolutions.com

Service Provider Technical Support: engineering@readynetsolutions.com

ReadyNet Address

6952 S. High Tech Drive, Suite B

Midvale, UT 84047

Purpose

This document is intended to instruct and assist personnel in the operation, installation and maintenance of the ReadyNet equipment and ancillary devices. It is recommended that all personnel engaged in such activities be properly trained. ReadyNet disclaims all liability whatsoever, implied or expressed, for any risk of damage, loss or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf, to abide by the instructions, system parameters, or recommendations made in this document.

Cross references

References to external publications are shown in italics. Other cross references, emphasized in blue text in electronic versions, are active links to the references.

This document is divided into numbered chapters that are divided into sections. Sections are not numbered, but are individually named at the top of each page, and are listed in the table of contents.

Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents.

Send feedback to customerservice@readynetsolutions.com

Declaration of Conformity

Part 15 FCC Rules

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

- This device may not cause harmful interference, and
- This device must accept any interference received, including interference that may cause undesired operation.

Class B Digital Device or Peripheral

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 can generate, use and radiate radio frequency energy. If not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. However, there is no guarantee that interference does not occur in a particular installation.



Note

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

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 interferences 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.

Warnings and Notes

The following describes how warnings and notes are used in this document and in all documents of the ReadyNet document set.

Warnings

Warnings precede instructions that contain potentially hazardous situations. Warnings are used to alert the reader to possible hazards that could cause loss of life or physical injury. A warning has the following format:



Warning

Warning text and consequence for not following the instructions in the warning.

Notes

A note means that there is a possibility of an undesirable situation or provides additional information to help the reader understand a topic or concept. A note has the following format:



Notes

Notes text and consequence for not following the instructions in the Notes.

GNU GPL Information

ReadyNet firmware contains third-party software under the GNU General Public License (GPL). Please refer to the GPL for the exact terms and conditions of the license. See links below for important regulatory information.

GNU General Public License (GPL): <https://www.readynetsolutions.com/gnu-general-public-license>
GPL Support: <https://www.readynetsolutions.com/gpl-support>


Chapter 1: Product Description

This chapter covers:

- [AC1100MSF](#)
- [LED Indicators and Interfaces](#)
- [Hardware Installation](#)
- [Voice Prompt](#)

AC1100MSF

Table 1 Features at-a-glance

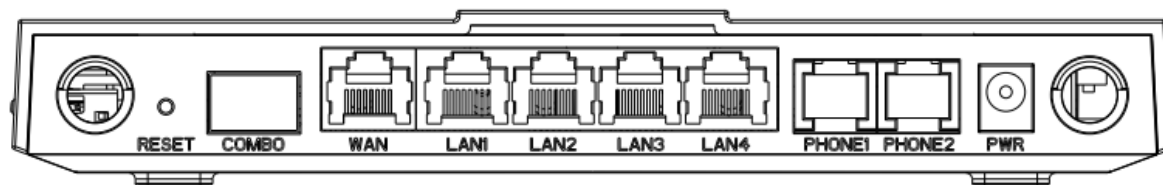
Port/Model		AC1100MSF	
Picture			
WAN		1	
LAN		4	
FXS		2	
USB		1	
LTE		No	
SPF		1	
Speed limit NAT		Yes	
Ethernet interface		5* RJ45 10/100M/1000M	
Fax		T.30, T.38 Fax	
Wi-Fi	2.4G 2T2R (300Mbps)	2.4G 2T2R(300Mbps)	2.4G 2T2R (300Mbps)
	5G 2T2R (867Mbps)		5G 2T2R (867Mbps)
Voice Code	G.711 (A-law, U-law), G.729A/B, G.723, G.722 (Wide band)		
Management	Voice menu, Web Management, Provision: TFTP/HTTP/HTTPS, TR069, SNMP		
VLAN	Support		

LED Indicators and Interfaces

Table 2 LED Indicators



AC1100MSF		
LED	Status	Explanation
Power	on Green	System is powered on
	off	System is powered off
System	on Green	System runs normally
	Blinking Green	System trouble
	off	System is powered off
SFP	on Green	SFP module is connected
	off	SFP module has no connection.
WAN	on Green	Network is connected (physical connection established), no data transmission
	Blinking Green	There is data being transmitted
	off	System is powered off or the network port is not connected to the network device.
LAN	on Green	Network is connected (physical connection established), no data transmission
	Blinking Green	There is data being transmitted
	off	System is powered off or the network port is not connected to the network device.
2.4G	on Green	Wireless access point is ready.
	Blinking Green	2.4g is connected, and there is data transmitted
	off	2.4g Wi-Fi off or system is powered off
5G	on Green	Wireless access point is ready.
	Blinking Green	5g is connected, and there is data transmitted
	off	5g Wi-Fi off or system is powered off
FXS(1-2)	on Green	Registered successfully, but no data transfer
	Blinking Green	There is data being transmitted or FXS port is registering
	off	Power is off or registered failed

Table 3 Interfaces**AC1100MSF**

Interface	Description
POWER	Connector for a power adapter
Phone1/2	ATA Analog phone connector
WAN	Connector for accessing the Internet
LAN 1/2/3/4	Connectors for local networked devices
COMBO	Connect the optical module
RESET	Restore the factory settings button, press and hold the device after 5s to restore the factory settings

Hardware Installation

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

Procedure 1 Configuring the Router

1. Connect analog phone to ATA Port with an RJ11 cable.
2. Connect the WAN port to the Internet your network's modem/switch/router/ADSL
3. equipment using an Ethernet cable.
4. Connect one end of the power cord to the power port of the device. Connect the other end to the wall outlet.
5. Check the Power, WAN, and LAN 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 AC1100MSF 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.
-

Voice Prompt

The devices may be configured by navigating the unit's voice menu. By using your phone and dialing a sequence of commands, the device may be configured for operation. Each device configuration section may be accessed by entering a certain operation code, as shown below.

Table 4 Voice Menu Setting Options

Operation code	Menu Navigation
1(1) WAN Port Connection Type	<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “1” , and The router reports the current WAN port connection type 3. Prompt "Please enter password" , user needs to input password and press “#” key, if user wants to configuration WAN port connection type. The password in IVR is same as web management interface login, the user may use phone keypad to enter password directly For example: WEB login password is “admin” , so the password in IVR is “admin” . The user may “23646” to access and then configure the WAN connection port. The unit reports “Operation Successful” if the password is correct. 4. Prompt "Please enter password" , user needs to input password and press “#” key if user wants to configuration WAN port connection type. 5. Choose the new WAN port connection type (1) DHCP or (2) Static The unit reports “Operation Successful” if the changes are successful. The router returns to the prompt “please enter your option ...” 6. To quit, enter “*”

<p>(2)</p> <p>WAN Port IP Address</p>	<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “2”, and The router reports current WAN Port IP Address 3. Input the new WAN port IP address and press “#” key: 4. Use “*” to replace “.”, for example user can input 192*168*20*168 to set the new IP address 192.168.20.168 5. Press # key to indicate that you have finished 6. Report “operation successful” if user operation is ok. 7. To quit, enter “**” .
<p>(3)</p> <p>WAN Port Subnet Mask</p>	<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “3”, and router reports current WAN port subnet mask 3. Input a new WAN port subnet mask and press # key: 4. Use “*” to replace “.”, user can input 255*255*255*0 to set the new WAN port subnet mask 255.255.255.0 5. Press “#” key to indicate that you have finished 6. Report “operation successful” if user operation is ok. 7. To quit, enter “**” .
<p>(4)</p> <p>Gateway</p>	<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “4”, and the router reports current gateway 3. Input the new gateway and press “#” key: 4. Use “*” to replace “.”, user can input 192*168*20*1 to set the new gateway 192.168.20.1. 5. Press “#” key to indicate that you have finished. 6. Report “operation successful” if user operation is ok. 7. To quit, press “**” .

<p>(5) DNS</p>	<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “5”, and the router reports current DNS 3. Input the new DNS and press # key: 4. Use “*” to replace “.”, user can input 192*168*20*1 to set the new gateway 192.168.20.1. 5. Press “#” key to indicate that you have finished.
<p>2 phone port configuration</p>	<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Select "2", then the device will continue to broadcast prompts the user to select current phone number; 2. registration server address; 3. registration port; 4. call forwarding configuration, 5. DNS configuration ; 3. Continue pressing "1" and the unit will continue to broadcast the phone number of the current phone port. The device will then broadcast "1. Phone number ..." again.
<p>3 Factory Reset</p>	<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “3”, and the router reports “Factory Reset” 3. Prompt "Please enter password", the method of inputting password is the same as operation 1. 4. If you want to quit, press “*” . 5. Prompt “operation successful” if password is right and then the router will be
<p>4 Reboot</p>	<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “4”, and the router reports “Reboot” 3. Prompt "Please enter password", the method of inputting password is same as operation 1. 4. the router reboots if password is right and operation

<p>5</p> <p>WAN Port Login</p>	<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “5”, and the router reports “WAN Port Login” 3. Prompt "Please enter password", the method of inputting password is same as operation 1. 4. If user wants to quit, press “*”.
<p>6</p> <p>WEB Access Port</p>	<ol style="list-style-type: none"> 5. Pick up phone and press “****” to start IVR 6. Choose “6”, and the router reports “ WEB Access Port” 7. Prompt “Please enter password”, the method of inputting password is same as operation 1. 8. Report “operation successful” if user operation is ok. 9. Report the current WEB Access Port
<p>7</p> <p>Firmware Version</p>	<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “7” and the router reports the current Firmware version



Note

1. While using Voice menu, press * (star) to return to main menu.
2. If any changes made in the IP assignment mode, the router must be rebooted in order for the settings to take effect.
3. While entering an IP address or subnet mask, use "*" (star) to enter "." (Dot) and use "#" (hash) key to finish entering IP address or subnet mask:
4. For example, to enter the IP address 192.168.20.159 by keypad, press these keys:
192*168*20*159, use the #(hash) key to indicate that you have finished entering the IP address.
5. Use the # (hash) key to indicate that you have finish entering the IP address or subnet mask
6. While assigning an IP address in Static IP mode, setting the IP address, subnet mask and default gateway is required to complete the configuration. If in DHCP mode, please make sure that a DHCP server is available in your existing broadband connection to which WAN port of AC1100MSF is connected.
7. The default LAN port IP address of router is 192.168.11.1 and this address should not be assigned to the WAN port IP address of router in the same network segment of LAN port.
8. The password can be entered using phone keypad, the mapping table between number and letters as follows:

To input: D, E, F, d, e, f -- press '3'

To input: G, H, I, g, h, i -- press '4'

To input: J, K, L, j, k, l -- press '5'

To input: M, N, O, m, n, o -- press '6'

To input: P, Q, R, S, p, q, r, s -- press '7'

To input: T, U, V, t, u, v -- press '8'

To input: W, X, Y, Z, w, x, y, z -- press '9'

To input all other characters in the administrator password-----press '0',

Chapter 2 Configuring Basic Settings

This chapter covers:

- [Two-Level Management](#)
- [Web Management Interface](#)
- [Configuring](#)
- [Making a Call](#)

Two-Level Management

This section explains how to setup a password for an administrator or user and how to adjust basic and advanced settings.

The AC1100MSF supports two-level management:

- (1) administrator and user. For administrator mode operation, please type “admin/admin” on Username/Password and click Login button to begin configuration.
- (2) user mode operation, please type “user/user” on Username/Password and click Login button to begin configuration.

Web Management Interface

The devices feature a web browser-based interface that may be used to configure and manage the device. See below for information

Logging in from the LAN port

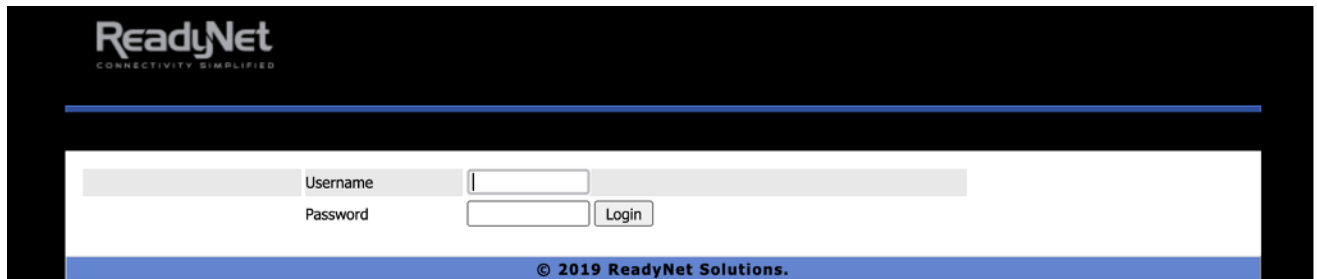
Ensure your PC is connected to the router’s LAN port correctly.



Note

You may either set up your PC to get an IP dynamically from the router or set up the IP address of the PC to be the same subnet as the default IP address of router is 192.168.11.1. For detailed information, see Chapter 5: Troubleshooting Guide.

Open a web browser on your PC and type “http://192.168.11.1” . The following window appears that prompts for Username and Password.



For administrator mode operation, please type admin/admin on Username/Password and click Login to begin configuration. For user mode operation, please type user/user on Username/Password and click Login to begin configuration.



Note

If you are unable to access the web configuration, please see Chapter 5: Troubleshooting Guide for more information.

The web management interface automatically logs out the user after 5 minutes of inactivity.

Logging in from the WAN port

Ensure your PC is connected to the router's WAN port correctly.

Obtain the IP addresses of WAN port using Voice prompt or by logging into the device web management interface via a LAN port and navigating to Network > WAN.

Open a web browser on your PC and type `http://<IP address of WAN port>`. The following login page will be opened to enter username and password.

For administrator mode operation, type admin/admin on Username/Password and click Login to begin configuration. For user mode operation, type user/user on Username/Password and click Login to begin configuration.



Note

If you fail to access to the web configuration, see Chapter 6: Troubleshooting Guide for more information.

The web management interface automatically logs out the user after 5 minutes of inactivity.

Web Management Interface Details

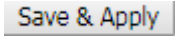

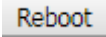
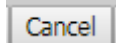
Table 5 Web management interface

The screenshot displays the 'INTERNET' configuration page in a web management interface. The top navigation bar (1) includes tabs for Status, Network, Wireless 2.4GHz, Wireless 5GHz, SIP, FXS1, FXS2, Security, and Application. The sub-navigation bar (2) shows tabs for WAN, LTE, LAN, IPv6 Advanced, IPv6 WAN, IPv6 LAN, VPN, Port Forward, DMZ, VLAN, and DDNS. The main configuration area (3) is titled 'INTERNET' and contains the following fields and options:

- Connect Name:** 1_INTERNET_R_VID (with a 'Delete Connect' button)
- Service:** INTERNET
- IP Protocol Version:** IPv4
- WAN IP Mode:** DHCP
- DHCP Server:** (empty text field)
- MAC Address Clone:** Disable
- NAT Enable:** Enable
- VLAN Mode:** Disable
- VLAN ID:** 1 (range 1-4094)
- DNS Mode:** Auto
- Primary DNS:** (empty text field)
- Secondary DNS:** (empty text field)
- DHCP:**
 - DHCP Renew:** Renew
 - DHCP Vendor (Option 60):** (empty text field)
- Port Bind:**
 - ☒ Port_1
 - ☒ Port_2
 - ☐ Port_3
 - ☐ Port_4
 - ☒ Wireless (SSID)
 - ☒ Wireless (SSID1)
 - ☒ Wireless (SSID2)
 - ☒ Wireless (SSID3)

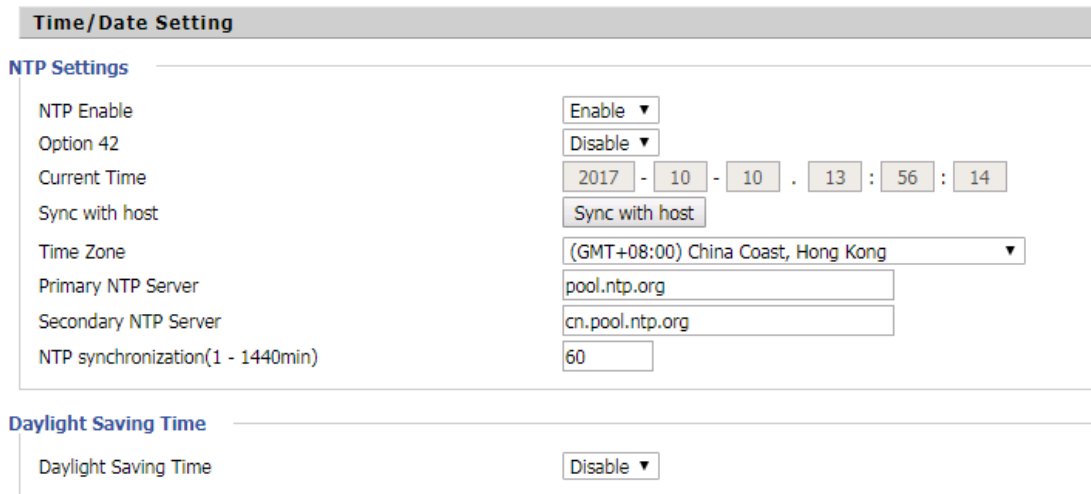
A note at the bottom states: 'Note: LAN (local) ports can only be bound to one WAN (Internet) connection at a time!'. At the bottom of the page are buttons for 'Save & Apply', 'Save', 'Cancel', and 'Reboot'.

Field Name	Descripti
Top Navigation bar	Click an option in Top Navigation bar (area marked as “1”). Multiple options in the Sub-navigation bar are displayed
Sub-navigation bar	Click the Sub-navigation bar to choose a configuration page (area marked as “2”)
Parameter configuration	This area displays the current parameters for configuration (e.g., area marked as “3”)

	After changing the parameters need to click this button to save & apply, modify the parameters immediately take effect.
	Any time changes are made click "Save" to confirm and save the changes. On click of “Save” button, a red message will be displayed as shown below to notify a reboot.
	Reboot the device to ensure that the modification parameters take effect
	To cancel the changes.

Setting the Time Zone

Table 6 Setting time zone



Time/Date Setting

NTP Settings

NTP Enable: Enable ▼

Option 42: Disable ▼

Current Time: 2017 - 10 - 10 . 13 : 56 : 14

Sync with host: Sync with host

Time Zone: (GMT+08:00) China Coast, Hong Kong ▼

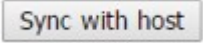
Primary NTP Server: pool.ntp.org

Secondary NTP Server: cn.pool.ntp.org

NTP synchronization(1 - 1440min): 60

Daylight Saving Time

Daylight Saving Time: Disable ▼

Field Name	Description
NTP Enable	Enable NTP (Network Time Protocol) to automatically retrieve time and date settings for the device
Current Time	When NTP Enable is set to “Disable” , manually configure the time and date via the Current Time parameter
Sync with host	Press  button to synchronize the host PC date, time and time zone
Primary NTP Server	Primary and secondary NTP server address for clock synchronization. A valid NTP server must be reachable for full NTP functionality
Secondary NTP Server	
NTP Synchronization (1- 1440m)	The synchronization period with NTP (1-1440 minutes), default is 60

Configuring an Internet Connection

From the Network > WAN page, WAN connections may be inserted or deleted. For more information on Internet Connection setting, see Table 10below.

Table 7 Configuring an internet connection

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Administration			
WAN	LTE	LAN	VPN	Port Forward	DMZ	DDNS	QoS	MAC Clone	Port Setting	Routing	Advance
Eoip Tunnel											

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

NAT Enable
Enable

VLAN Mode
Disable

VLAN ID
1 (1-4094)

DNS Mode
Auto

Primary DNS

Secondary DNS

DHCP

DHCP Renew
Renew

DHCP Vendor(Option 60)

Port Bind

☒ Port_1
☒ Port_2
☒ Port_3
☒ Port_4

☒ 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 !

Help


WAN IP Mode:

Static IP - Set the IP Address, Subnet Mask and Default Gateway that you have gotten from your ISP.

DHCP - You will get an IP Address, Subnet Mask and Default Gateway from some DHCP server.

PPPoE - Set the PPPoE Username and Password that you have gotten from your ISP provider.

Field Name	Description
Connect Name	Use keywords to indicate WAN port service model (the parameters are defined in Network--> multi-WAN page)
Service	Choose the service mode for the created connection
IP Protocol Version	IPv4 and IPv6 are supported
WAN IP Mode	Choose Internet connection mode, DHCP, PPPoE, or Bridge
NAT Enable	Enable or disable NAT

VLAN ID	<div>Note Multiple WAN connections may be created with the same VLAN ID</div>
DNS Mode	<p>Select DNS mode, options are Auto and Manual:</p> <p>When DNS mode is Auto, the device under LAN port will automatically obtains the preferred DNS and alternate DNS.</p> <p>When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS</p>
Primary DNS	Enter the preferred DNS address
Secondary DNS	Enter the secondary DNS address
DHCP	(Displayed when WAN IP Mode is set to DHCP)
DHCP Renew	Refresh the DHCP IP
DHCP Vendor (Option60)	Specify the DHCP Vendor field Display the vendor and product name

Setting up Wireless Connections

To set up the wireless connection, please perform the following steps.

Enable Wireless and Setting SSID

Open Wireless > Basic webpage as shown below:

Table 8 Wireless > Basic web page (user view)

The screenshot shows the 'Basic Wireless Settings' page for the 'Wireless 2.4GHz' section. The page is divided into two main tabs: 'Basic' and 'Advanced'. The 'Basic' tab is currently selected. The settings are organized into a table-like structure with labels on the left and configuration options on the right.

Field Name	Description
Radio On/Off	Radio On (selected)
Wireless Connection Mode	AP (selected)
Network Mode	11b/g/n mixed mode (selected)
Multiple SSID	Wireless_AP0E6788, Enable (checked), Hidden (unchecked), Isolated (unchecked), Max Client 16
Multiple SSID1	[Empty], Enable (unchecked), Hidden (unchecked), Isolated (unchecked), Max Client 16
Multiple SSID2	[Empty], Enable (unchecked), Hidden (unchecked), Isolated (unchecked), Max Client 16
Multiple SSID3	[Empty], Enable (unchecked), Hidden (unchecked), Isolated (unchecked), Max Client 16
broadcast (SSID)	Enable (selected), Disable (unchecked)
AP Isolation	Enable (unchecked), Disable (selected)
MBSSID AP Isolation	Enable (unchecked), Disable (selected)
BSSID	00:21:F2:0E:67:88
Frequency (Channel)	Auto (selected)
HT Physical Mode	Mixed Mode (selected), Green Field (unchecked)
Operating Mode	20 (unchecked), 20/40 (selected), Auto (unchecked)
Channel BandWidth	

Field Name	Description
Radio On/Off	Select "Radio Off" to disable wireless operation Select "Radio on" to enable wireless operation Please note: "Save" required for this parameter change
Network Mode	Choose one network mode from the drop-down list.
SSID	The logical name of the wireless connection (text, numbers or various special characters)
Multiple SSID 1-4	Multiple SSID 1 - 4, configure up to 4 unique SSIDs
broadcast(SSID)	Enabled: The device SSID is broadcast at regular intervals Disabled: The device SSID is not broadcast at regular intervals, disallowing wi-fi clients from automatically connecting to the AC1100MSF

AP Isolation	<p>Enabled: Devices connected to the router are isolated from one another on virtual networks</p> <p>Disabled: Devices connected to the router are visible on the network to each other</p>
MBSSID AP Isolation	<p>Enabled: Devices connected to the router via one of the Multiple SSIDs are isolated from one another on virtual networks</p> <p>Disabled: Devices connected to the router via one of the Multiple SSIDs are visible on the network to each other</p>
BSSID	Basic Service Set Identifier – AP MAC Address Listing
Frequency (Channel)	Select the channel of operation for the device from the drop-down list
HT Physical Mode	
Operating Mode	<p>Mixed Mode: Packet preamble (only) is transmitted in a format compatible with legacy 802.11a/g (for 802.11a/g receivers).</p> <p>Green Field: High throughput packet preambles do not contain legacy formatting (802.11n only network)</p>
Channel Bandwidth	20: the device operates with a 20 MHz channel size 20/40: the device operates with a 40 MHz channel size

Encryption

Open Wireless/Wireless Security webpage to configure custom security parameters.

Table 9 Wireless Security web page

Wi-Fi Security Settings	
<div> <div>BasicWireless SecurityWMMWDSWPSStation InfoAdvanced</div> <div> <div>Select SSID</div> <div> <div>SSID choiceWireless_AP0E6788</div> <div>"Wireless_AP0E6788"</div> <div>Security ModeWPA-PSK</div> <div> <div>WPA</div> <div>WPA Algorithms <div> <div><input type="radio"/> TKIP</div> <div><input checked="" type="radio"/> AES</div> <div><input type="radio"/> TKIPAES</div> </div> <div>Pass Phrase <div>*****</div> </div> <div>Key Renewal Interval <div> <div>3600</div> <div>sec</div> <div>(0 ~ 86400)</div> </div> </div> <div>Access Policy <div>Policy <div>Disable</div> </div> <div>Add a station MAC <div> <div></div> <div>(The maximum rule count is 64)</div> </div> </div> </div> </div> </div></div></div></div>	
Field Name	Description
SSID Choice	Choose the SSID from the drop-down list for which security will be configured
Security Mode	<p>Select an appropriate encryption mode to improve the security and privacy of your wireless data packets.</p> <p>Each encryption mode will launch an additional web page and ask you to offer additional configuration.</p> <p>For high security, the device can be configured for Security Mode as WPA2-PSK and WPA Algorithms as AES.</p>
WPA Algorithms	This parameter is used to select the encryption of wireless home gateway algorithms; options are TKIP, AES and TKIPAES.
Pass Phrase	Configure the WPA-PSK security password.
Key Renewal Interval	Set the key scheduled update cycle, default is 3600s.
Access Policy	
Policy	<p>Disable: Access policy rules are not enforced</p> <p>Allow: Only allow the clients in the station MAC list to access Rejected: Block the clients in the station MAC list from registering</p>
Add a Station MAC	Enter the MAC address of the clients which you want to allow or reject

Configuring Session Initiation Protocol (SIP)

SIP Accounts

The device has 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

Table 10 Configuring SIP the Web Management Interface

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
<div>SIP Account Preferences</div>								
<div>Basic</div>								
<div>Basic Setup</div> <div> <div>Line Enable</div> <div>Enable ▼</div> </div> <div> <div>Outgoing Call without Registration</div> <div>Disable ▼</div> </div>								
<div>Proxy and Registration</div> <div> <div>Proxy Server</div> <div></div> </div> <div> <div>Outbound Server</div> <div></div> </div> <div> <div>Backup Outbound Server</div> <div></div> </div> <div> <div>Allow DHCP Option 120 to Override SIP Server</div> <div>Disable ▼</div> </div> <div> <div>Proxy Port</div> <div>5060</div> </div> <div> <div>Outbound Port</div> <div>5060</div> </div> <div> <div>Backup Outbound Port</div> <div>5060</div> </div>								
<div>Subscriber Information</div> <div> <div>Display Name</div> <div></div> </div> <div> <div>Account</div> <div></div> </div> <div> <div>Phone Number</div> <div></div> </div> <div> <div>Password</div> <div></div> </div>								

Procedure

1. Open the FXS1/SIP Account webpage, as illustrated above.
2. Fill the SIP Server address and SIP Server port number (from administrator or provider) into Proxy Server Name and into Proxy Port parameters.
3. Fill 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 webpage to save changes.

**Note**

Upon the following dialogue:

Please **REBOOT** to make the changes effective!

Please press  button to make changes effective.

Viewing the Registration Status

Table 11 Registration status

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
Basic	LAN Host	Syslog	LAN Host Statistics					

Product Information	
Product Information	
Product Name	AC1100MSF
Internet (WAN) MAC Address	00:01:9F:42:04:09
PC (LAN) MAC Address	00:01:9F:42:04:08
Hardware Version	V3.1
Loader Version	V3.37(Feb 25 2019 15:04:51)
Firmware Version	V3.32 (202004111810)
Serial Number	11MSF000030

SIP Account Status	
SIP Account Status	
FXS 1 SIP Account Status	Disable
Primary Server	0.0.0.0
Backup Server	0.0.0.0

Procedure

To view the SIP account status of device, open the Status webpage and view the value of registration status.

Making a Call

Calling phone or extension numbers

To make a phone or extension number call:

- Both ATA and the other VoIP device (i.e., another ATA or other SIP products) must have public IP addresses, or
- Both ATA and the other VoIP device (i.e., another ATA or other SIP products) are on the same LAN using private or public IP addresses, or
- Both ATA and the other VoIP device (i.e., another ATA or other SIP products) can be connected through a router using a public or private IP addresses.

To make a call, first pick up the analog phone or turn on the speakerphone on the analog phone, input the IP address directly, end with #.

Direct IP calls

Direct IP calling allows two phones, that is, an ATA with an analog phone and another VoIP Device, to talk to each other without a SIP proxy. VoIP calls can be made between two phones if:

- Both ATA and the other VoIP device (i.e., another ATA or other SIP products) have public IP addresses, or
- Both ATA and the other VoIP device (i.e., another ATA or other SIP products) are on the same LAN using private or public IP addresses.
- Both ATA and the other VoIP device (i.e., another ATA or other SIP products) can be connected through a router using public or private IP addresses.

To make a direct IP call, first pick up the analog phone or turn on the speakerphone on the analog phone, Input the IP address directly, with the end “#” .

Call Hold

While in conversation, pressing the “*77” to put the remote end on hold, then you will hear the dial tone and the remote party will hear hold tone at the same time.

Pressing the “*77” again to release the previously hold state and resume the bi-directional media.

Blind Transfer

Assume that call party A and party B are in conversation. Party A wants to Blind Transfer B to C:

Party A dials “*78” to get a dial tone, then dials party C’s number, and then press immediately key # (or wait for 4 seconds) to dial out. A can hang up.

Attended Transfer

Assume that call party A and B are in a conversation. A wants to Attend Transfer B to C:

Party A dials “*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 dials “*78” to transfer to C, then B and C now in 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, for conference.

Chapter 3: Web Interface

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

- [Login](#)
- [Status](#)
- [Network and Security](#)
- [Wireless](#)
- [SIP](#)
- [FXS1](#)
- [FXS2](#)
- [Security](#)
- [Application](#)
- [Administration](#)
- [Management](#)
- [System Log](#)
- [Logout](#)
- [Reboot](#)

Login

Table 12 Login details

Procedure

1. Connect the LAN port of the router 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

Table 13 Status Page

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application	Storage	Administration
Basic	LAN Host	Syslog	LAN Host Statistics							
Product Information										Help
Product Information										Product Information: It shows the basic information of the product.
Product Name AC1100MSF										Line Status: Displays current line registration status, as well as primary and back-up SIP server IP address information.
Internet (WAN) MAC Address 00:01:9F:42:04:09										Network Status: Displays the network status and detailed information about WAN, LAN, Wi-Fi & VPN.
PC (LAN) MAC Address 00:01:9F:42:04:08										
Hardware Version V3.1										
Loader Version V3.37(Feb 25 2019 15:04:51)										
Firmware Version V3.32 (202004111810)										
Serial Number 11MSF000030										

SIP Account Status**SIP Account Status**

FXS 1 SIP Account Status	Registered 1100
Primary Server	192.168.10.88
Backup Server	192.168.10.88
FXS 2 SIP Account Status	Registered 1111
Primary Server	192.168.10.88
Backup Server	192.168.10.88

FXS Port Status**FXS Port Status**

FXS 1 Hook State	On
FXS 1 Port Status	Idle
FXS 2 Hook State	On
FXS 2 Port Status	Idle

Network Status**Active WAN Interface**

Connection Type	DHCP
IP Address	192.168.10.124 <input type="button" value="Renew"/>
Link-local IPv6 Address	
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
Primary DNS	192.168.10.1
Secondary DNS	192.168.18.1
IPv6 PD Prefix	
IPv6 Domain Name	
IPv6 Primary DNS	
IPv6 Secondary DNS	
WAN Port Status	100Mbps Full
WAN Down Speed	212B/s
WAN Up Speed	628B/s

1 TR069_VOICE_INTERNET Vlan Status

Connection Type	DHCP
MAC Address	00:21:F2:0E:67:89
IP Address	192.168.10.124
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
Primary DNS	192.168.10.1
Secondary DNS	192.168.18.1

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	Link Down
LAN2	1000Mbps Full
LAN3	Link Down
LAN4	Link Down

Wireless Info**Wireless 2.4GHz**

Radio On/Off	On
Network Mode	11b/g/n mixed mode
Current Channel	4
Channel Bandwidth	40MHz

Wireless 5GHz

Radio On/Off	On
Network Mode	11vht AC/AN/A
Current Channel	36
Channel Bandwidth	40MHz

Wireless_AP0E6788 (2.4GHz)

BSSID	00:21:F2:0E:67:88
Number of Device	0

Wireless_5G0E6788 (5GHz)

BSSID	00:21:F2:0E:67:8C
Number of Device	0

System Status**System Status**

Current Time	2017-11-02 14:06:38
Elapsed Time	4 Hours, 14 Mins

Description

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

Network and Security

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.

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.

Table 14 Internet

Static	
IP Address	192.168.10.173
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
DNS Mode	Manual ▼
Primary DNS	192.168.10.1
Secondary DNS	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 Router has a built-in DHCP server that assigns private IP address to each local client.

The DHCP feature allows to the router 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.

Table 15 DHCP

INTERNET		Help
WAN		
Connect Name	1_MANAGEMENT_VOICE_INTERNET_R_VID ▼	WAN IP Mode: <i>Static IP</i> - Set the IP Address, Subnet Mask and Default Gateway provided by your ISP. <i>DHCP</i> - IP Address, Subnet Mask and Default Gateway will be issued by the local DHCP Server. <i>PPPoE</i> - Set the PPPoE Account and PPPoE Password provided by your ISP. <i>NAT</i> - The product will be the same as a router. <i>Bridge</i> - The LAN port is the same as the WAN port.
Service	MANAGEMENT_VOICE_INTERNET ▼	
IP Protocol Version	IPv4 ▼	
WAN IP Mode	DHCP ▼	
MAC Address Clone	Disable ▼	
NAT Enable	Enable ▼	
VLAN Mode	Disable ▼	
VLAN ID	1 (1-4094)	
DNS Mode	Auto ▼	
Primary DNS		
Secondary DNS		
DHCP		
DHCP Renew	Renew	
DHCP Vendor (Option 60)	ReadyNet_AC1100MSI	
Port Bind		
<input checked="" type="checkbox"/> Port_1	<input checked="" type="checkbox"/> Port_2	<input checked="" type="checkbox"/> Port_3
<input checked="" type="checkbox"/> Wireless (SSID)	<input checked="" type="checkbox"/> Wireless (SSID1)	<input checked="" type="checkbox"/> Wireless (SSID2)
		<input checked="" type="checkbox"/> Port_4
		<input checked="" type="checkbox"/> Wireless (SSID3)
Note: LAN (local) ports can only be bound to one WAN (Internet) connection at a time!		

Field Name	Description
DNS Mode	<p>Select DNS mode, options are Auto and Manual:</p> <p>When DNS mode is Auto, the device under LAN port will automatically obtain the preferred DNS and alternate DNS.</p> <p>When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS</p>
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.

Table 16 PPPoE

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	
Secondary DNS	
PPPoE	
PPPoE Account	
PPPoE Password	••••••••
Confirm Password	••••••••
Service Name	
	Leave empty to autodetect
Operation Mode	Keep Alive ▼
Keep Alive Redial Period(0-3600s)	5

Field Name	Description
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	<p>Select the mode of operation, options are Keep Alive, On Demand and Manual:</p> <p>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;</p> <p>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;</p> <div> <div>Operation Mode</div> <div>On Demand ▼</div> </div> <div> <div>On Demand Idle Time(0-60m)</div> <div>5</div> </div> <p>When the mode is Manual, there are no additional settings to configure</p>
Keep Alive Redial Period	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.

Table 17 Bridge Mode

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 <input checked="" type="checkbox"/> Port_1 <input checked="" type="checkbox"/> Port_2 <input checked="" type="checkbox"/> Port_3 <input checked="" type="checkbox"/> Wireless(SSID) <input checked="" type="checkbox"/> Wireless(SSID1) <input checked="" type="checkbox"/> Wireless(SSID2) <input checked="" type="checkbox"/> 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	Description
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.
	<div>  <div> Note Multiple WAN connections may be created with the same VLAN ID </div> </div>
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.

Table 18 LAN port

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN
Advance								

PC Port(LAN)

PC Port(LAN)

Local IP Address: 192.168.1.1
Local Subnet Mask: 255.255.255.0
Local DHCP Server: Enable ▾
DHCP Start Address: 192.168.1.2
DHCP End Address: 192.168.1.254
DNS Mode: Auto ▾
Primary DNS: 192.168.1.1
Secondary DNS: 192.168.10.1
Client Lease Time (0-86400s): 86400
DHCP Client List
DHCP Static Allotment

NO.	MAC	IP Address
Delete Selected Add Edit		

DNS Proxy: Enable ▾

Save & Apply Save Cancel Reboot

Field Name	Description
IP Address	Enter the IP address of the router on the local area network. All the IP addresses of the computers which are in the router'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 router'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	<p>Select DNS mode, options are Auto and Manual:</p> <p>When DNS mode is Auto, the device under LAN port will automatically obtains the preferred DNS and alternate DNS.</p> <p>When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS.</p>
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 router has a built-in DHCP server that assigns private IP address to each local client.

DHCP stands for Dynamic Host Configuration Protocol. The router, 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 router enabled as a DHCP server if you do not have a DHCP server for your network.

Table 19 DHCP server settings

PC Port(LAN)	
PC Port(LAN)	
Local IP Address	192.168.11.1
Local Subnet Mask	255.255.255.0
Local DHCP Server	Enable ▼
DHCP Start Address	192.168.11.2
DHCP End Address	192.168.11.254
DNS Mode	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.

Table 20 DHCP server, DNS and Client Lease Time

Primary DNS	192.168.11.1
Secondary DNS	8.8.8.8
Client Lease Time(0-86400s)	86400
	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 router 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 router 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 router 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.

LTE

Table 21 LTE

The screenshot displays the LTE configuration interface of a router. At the top, there are navigation tabs: Status, Network, Wireless, SIP, FXS1, FXS2, Security, Application, and Administration. The 'Network' tab is selected, and within it, the 'LTE' sub-tab is active. Below the tabs, there is a 'Help' button. The main content area is titled 'LTE Setting' and is divided into three sections: 'Basic Setting', 'Internet Setting', and 'Binding Set'.

Basic Setting:

- LTE Modem Enable: Enable (dropdown)
- GSM Call Enable: Disable (dropdown)
- 4G Connection Type: Auto (dropdown)
- APN: CMNET (text field)
- Dial Number: *99*1# (text field)
- Username: admin (text field)
- Password: (password field)

Internet Setting:

- Internet connection: Auto (dropdown)
- Lock status: Cell Unlock (text field)
- Targeted Scell ID: (text field)
- Lock Cell: Disable (dropdown)

Binding Set:

- Current Status: PIN Disable (text field)
- SIM Bind: (text field)
- The remaining number of unlock: (text field)
- Binding: (button)

Field Name	Description
Basic Setting	
LTE Modem Enable	Enable the LTE Modem
GSM Call Enable	Enable the GSM Cal
4G Connection Type	Choose the 4G connection method, Auto or Manual
APN	The APN default to CMNET
Dial Number	
Username	Enter the username
Password	Enter the Password
Internet Setting	
Internet connection	Choose the internet connection in Auto/4G only/3G only/
Lock status	Check the lock status of the cell
Targeted Sell ID	Here is Targeted Sell ID
Lock Cell	Enable or Disable lock cell
Binding Set	
Current Status	Check the status of the current PIN here
SIM Bind	Fill in the phone number and Bind the SIM Card

VPN

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

Table 22 VPN

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application		
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN	QoS	Rate
Advance										

VPN Settings

Administration

VPN Enable

Disable
Disable
PPTP
L2TP
OpenVPN

Save & Apply
Save
Cancel
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.

Port Forward

Table 22 Port Forward

WAN	LTE	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN	DDNS	QoS	Port Setting
Routing		Advance										

Port Forwarding				
No.	Comment	IP Address	Port Range	Protocol
<div> <input type="button" value="Delete Selected"/> <input type="button" value="Add"/> <input type="button" value="Edit"/> </div>				

Port Forwarding

Comment

IP Address

Port Range -

Protocol

(The maximum rule count is 32)

Virtual Servers					
No.	Comment	IP Address	Public Port	Private Port	Protocol
<div> <input type="button" value="Delete Selected"/> <input type="button" value="Add"/> <input type="button" value="Edit"/> </div>					

Virtual Servers

Comment

IP Address

Public Port

Private Port

Protocol

(The maximum rule count is 32)

Field Name	Description
Comment	Sets the name of a port mapping rule or comment
IP Address	The IP address of devices under the LAN port
Port Range	Set the port range for the devices under the LAN port. (1-65535)
Protocol	You can select TCP, UDP, TCP & UDP three cases
Apply/Cancel	After finish configurations, click apply, the number will be generated under NO. List; click Cancel to if you do not want to make the changes
Comment	To set up a virtual server notes
IP Address	Virtual server IP address
Public Port	Public port of virtual server
Private Port	Private port of virtual servers ports
Protocol	You can select from TCP, UDP, and TCP&UDP
Apply/Cancel	After finish configurations, click apply, the number will be generated under NO. List; click Cancel to if you do not want to make the changes

VLAN

Table 23 VLAN

WANLTELANIPv6 AdvancedIPv6 WANIPv6 LANVPNPort ForwardDMZVLANDDNSQoSPort Setting

RoutingAdvance

VLAN Model Configuration

VLAN Divide Model

Custom

Port VLAN ID Configuration

WAN	LAN1	LAN2	LAN3	LAN4
1	2	2	2	2

VLAN Configuration

VLAN ID	Port				
	WAN	LAN1	LAN2	LAN3	LAN4
<input checked="" type="checkbox"/> 1	Untag	Unset	Unset	Unset	Unset
<input checked="" type="checkbox"/> 2	Unset	Untag	Untag	Untag	Untag
<input type="checkbox"/>	Unset	Unset	Unset	Unset	Unset
<input type="checkbox"/>	Unset	Unset	Unset	Unset	Unset

Field Name	Description
VLAN Divide Model	Select the desired mode
VLAN Configurations	Select the desired configuration, divided into unset / Tagged / unTagged

DMZ

Table 24 DMZ

StatusNetworkWireless 2.4GHzWireless 5GHzSIPFXS1FXS2SecurityApplication

WANLANIPv6 AdvancedIPv6 WANIPv6 LANVPNPort ForwardDMZVLANQoSRate

Advance

Demilitarized Zone (DMZ)

DMZ Setting

DMZ Enable

Enable

DMZ Host IP Address

Get Current PC IP

Save & Apply

Save

Cancel

Reboot

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

DDNS

Table 25 DDNS

WANLTELANIPv6 AdvancedIPv6 WANIPv6 LANVPNPort ForwardDMZVLANDDNS

RoutingAdvance

DDNS Setting

DDNS Setting

Dynamic DNS Provider

NONE

Account

admin

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

Table 26 QoS

WAN LTE LAN IPv6 Advanced IPv6 WAN IPv6 LAN VPN Port Forward DMZ VLAN DDNS **QoS** Port Setting

Routing Advance

QoS setting

QoS setting

Enable QoS Disable ▾
 Upstream (0-102400)kbit/s
 Downstream (0-102400)kbit/s
 Algorithm WFQ ▾

Save Cancel

	Name	Condition									Action					
		Src.IP Address	Dst.IP Address	Protocol	Src.Port Range	Dst.Port Range	Physical Port	DSCP	802.1p	VLAN ID	Remark DSCP	Remark 802.1p	Remark VLAN_ID	Priority	Drop	Rate Limit

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



Note

From system release 4.2 or later, the QoS bandwidth can be configured for Upstream and Downstream

Port Setting

Table 27 Port setting

Field Name	Description
WAN Port speed Nego	Auto-negotiation, options are Auto, 100M full, 100M half-duplex, 10M half and full.
LAN1~LAN3 Port Speed Nego	Auto-negotiation, options are Auto, 100M full, 100M half, 10M half and 10M full.

Routing

Table 28 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

Advance

Table 29 Advance

WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN	QoS	Rate
Advance										

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 Detecting Interval(0-3600s)	600

Field Name	Description
Most Nat connections	The largest value which the AC1100MSF can provide
Mss Mode	Choose Mss Mode from Manual and Auto
Mss Value	Set the value of TCP
AntiDos-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

Wireless 2.4G

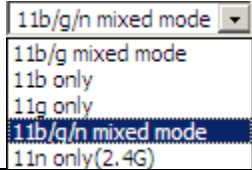
Basic

Table 30 Basic

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application	Storage	Admin
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced				

Basic Wireless Settings	
Wireless Network	
Radio On/Off	Radio On ▼
Wireless Connection Mode	AP ▼
Network Mode	11b/g/n mixed mode ▼
Multiple SSID	Wireless_AP0E6788 Enable <input checked="" type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client 16
Multiple SSID1	<input type="text"/> Enable <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client 16
Multiple SSID2	<input type="text"/> Enable <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client 16
Multiple SSID3	<input type="text"/> Enable <input type="checkbox"/> Hidden <input type="checkbox"/> Isolated <input type="checkbox"/> Max Client 16
broadcast (SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
BSSID	00:21:F2:0E:67:88
Frequency (Channel)	Auto ▼
HT Physical Mode	
Operating Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field
Channel BandWidth	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40 <input type="radio"/> Auto
Guard Interval	<input type="radio"/> Long <input checked="" type="radio"/> Short
Reverse Direction Grant (RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
STBC	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Aggregation MSDU (A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
HT Disallow TKIP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable
20/40 Coexistence	<input checked="" type="radio"/> Disable <input type="radio"/> Enable
HT LDPC	<input checked="" type="radio"/> Disable <input type="radio"/> Enable

Field Name	Description
Radio on/off	Select "Radio off" to disable wireless. Select "Radio on" to enable wireless.
Wireless connection mode	According to the wireless client type, select one of these modes. Default is AP
Network Mode	Choose one network mode from the drop-down list. Default is 11b/g/n mixed mode

	
SSID	It is the basic identity of wireless LAN. SSID can be any alphanumeric or a combination of special characters. It will appear in the wireless network access list.
Multiple SSID1~SSID3	The device supports 4 SSIDs.
Hidden	After the item is checked, the SSID is no longer displayed in the search for the Wi-Fi wireless network connection list
Broadcast(SSID)	After initial State opening, the device broadcasts the SSID of the router to wireless network
AP Isolation	If AP isolation is enabled, the clients of the AP cannot access each other.
MBSSID AP Isolation	AP isolation among the devices which are not belong to this AP and along to, when the option is enabled, the devices which do not belong to this AP cannot access the devices which are within the AP
BSSID	A group of wireless stations and a WLAN access point (AP) consists of a basic access device (BSS), each computer in the BSS must be configured with the same BSSID, that is, the wireless AP logo
Frequency (Channel)	You can select Auto Select and channel 1/2/3/4/5/6/7/8/9/10/11.
HT Physical Mode Operating Mode	Mixed Mode: In this mode, the previous wireless card can recognize and connect to the Pre-N AP, but the throughput will be affected Green Field: high throughput can be achieved, but it will affect backward compatibility, and security of the system
Channel Bandwidth	Select channel bandwidth, default is 20 MHz and 20/40 MHz.
Guard Interval	The default is automatic, in order to achieve good BER performance, you must set the appropriate guard interval
Reverse Direction Grant (RDG)	Enabled: Devices on the WLAN are able to transmit to each other without requiring an additional contention-based request to transfer (i.e., devices are able to transmit to another device on the network during TXOP) Disabled: Devices on the WLAN must make a request for transmit when communicating with another device on the network
STBC	Space-time Block Code

	Enabled: Multiple copies of signals are transmitted to increase the chance of successful delivery
Aggregation MSDU (A-MSDU)	<p>Enabled: Allows the device to aggregate multiple Ethernet frames into a single 802.11n, thereby improving the ratio of frame data to frame overhead</p> <p>Disabled: No frame aggregation is employed at the router</p>
Auto Block Ack	<p>Enabled: Multiple frames are acknowledged together using a single Block Acknowledgement frame.</p> <p>Disabled: Auto block acknowledgement is not used by the device – use this configuration when low throughput/connectivity issues are experienced by mobile devices</p>
Decline BA Request	<p>Enabled: Disallow block acknowledgement requests from devices</p> <p>Disabled: Allow block acknowledgement requests from devices</p>
HT Disallow TKIP	<p>Enabled: Disallow the use of Temporal Key Integrity Protocol for connected devices</p> <p>Disabled: Allow the use of Temporal Key Integrity Protocol for connected devices</p>
HT LDPC	<p>Enabled: Enable Low-Density Parity Check mechanism for increasing chance of successful delivery in challenging wireless environments</p> <p>Disabled: Disable Low-Density Parity Check mechanism</p>

Wireless Security

Table 31 Wireless security

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		

Wi-Fi Security Settings

Select SSID

SSID choice

Wireless_AP0E6788 ▼

"Wireless_AP0E6788"

Security Mode

WPA-PSK ▼

WPA

WPA Algorithms

☐ TKIP
☒ AES
☐ TKIPAES

Pass Phrase

Key Renewal Interval

3600

sec (0 ~ 86400)

Access Policy

Policy

Disable ▼

Add a station MAC
(The maximum rule count is 64)

Field Name	Description
SSID Choice	Choose one SSID from SSID, Multiple SSID1, Multiple SSID2 and Multiple SSID3.
Security Mode	Select an appropriate encryption mode to improve the security and privacy of your wireless data packets. Each encryption mode will bring out different web page and ask you to offer additional configuration.

User can configure the corresponding parameters. Here are some common encryption methods:

OPENWEP: A handshake way of WEP encryption, encryption via the WEP key:

Table 32 Wi-Fi Security Setting

Wi-Fi Security Settings

Select SSID

SSID choice: Wireless_AP0E6788 ▼

"Wireless_AP0E6788"

Security Mode: OPENWEP ▼

Wire Equivalence Protection (WEP)

Default Key: WEP Key 1 ▼

WEP Keys:

WEP Key 1	WEP Key 2	WEP Key 3	WEP Key 4
*****	*****	*****	*****
Hex ▼	Hex ▼	Hex ▼	Hex ▼
64bit ▼	64bit ▼	64bit ▼	64bit ▼

Access Policy

Policy: Disable ▼

Add a station MAC: (The maximum rule count is 64)

Field Name	Description
Security Mode	This is used to select one of the 4 WEP keys, key settings on the clients should be the same with this when connecting.
WEP Keys	Set the WEP key. A-64 key need 10 Hex characters or 5 ASCII characters; choose A-128 key need 26 Hex characters or 13 ASCII characters.
WEP represents Wired Equivalent Privacy, which is a basic encryption method.	

WPA-PSK, the router will use WPA way which is based on the shared key-based .

Table 33 WPA-PSK

Wi-Fi Security Settings	
Select SSID	
SSID choice	Wireless_AP0E6788 ▼
"Wireless_AP0E6788"	
Security Mode	WPA-PSK ▼
WPA	
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase	*****
Key Renewal Interval	3600 sec (0 ~ 86400)
Access Policy	
Policy	Disable ▼
Field Name	Description
WPA Algorithms	This item is used to select the encryption of wireless home gateway algorithms, options are TKIP, AES and TKIPAES.
Pass Phrase	Setting up WPA-PSK security password.

WPAPSKWPA2PSK manner is consistent with WPA2PSK settings:

Table 34 WPAPSKWPA2PSK

Wi-Fi Security Settings	
Select SSID	
SSID choice	Wireless_AP0E6788 ▼
"Wireless_AP0E6788"	
Security Mode	WPAPSKWPA2PSK ▼
WPA	
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase	*****
Key Renewal Interval	3600 sec (0 ~ 86400)
Field Name	Description
WPA Algorithms	The home gateway is used to select the wireless security encryption algorithm options are TKIP, AES, TKIP / AES. 11N mode does not support TKIP algorithms.
Pass Phrase	Set WPA-PSK/WPA2-PSK security code
Key Renewal Interval	Set the key scheduled update cycle, default is 3600s

WPA-PSK/WPA2-PSK WPA/WPA2 security type is actually a simplified version, which is based on the WPA shared key mode, higher security setting is also relatively simple, suitable for ordinary home users and small businesses.

Wireless Access Policy:

Table 35 Wireless Access Policy

Access Policy

Policy: Disable ▼
Disable
Allow
Reject

Add a station MAC (The maximum rule count is 64)

Save Cancel Reboot

Field Name	Description
Access policy	Wireless access control is used to allow or prohibit the specified client to access to your wireless network based on the MAC address.
Policy	<p>Disable : Prohibition: wireless access control policy. Allow: only allow the clients in the list to access.</p> <p>Rejected: block the clients in the list to access.</p>
Add a station MAC	Enter the MAC address of the clients which you want to allow or prohibit
<p>Example: Prohibit the device whose wireless network card MAC address is 00:1F: D0: 62: BA:FF's to access the wireless network, and allow other computers to access the network. Implementation: As shown, the Policy is Reject, add 00:1F: D0: 62: BA: FF to the MAC, click Save and reboot the device settings to take effect.</p>	

WMM

Table 36 WMM

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		

WMM Parameters of Access Point						
	AIFSN	CWMin	CWMax	TXOP	ACM	AckPolicy
AC_BE	3	15 ▼	63 ▼	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_BK	7	15 ▼	1023 ▼	0	<input type="checkbox"/>	<input type="checkbox"/>
AC_VI	1	7 ▼	15 ▼	94	<input type="checkbox"/>	<input type="checkbox"/>
AC_VO	1	3 ▼	7 ▼	47	<input type="checkbox"/>	<input type="checkbox"/>

Description

WMM (Wi-Fi Multi-Media) is the QoS certificate of Wi-Fi Alliance (WFA). This provides you to configure the parameters of wireless multimedia; WMM allows wireless communication to define a priority according to the home gateway type. To make WMM effective, the wireless clients must also support WMM.

WDS

Table 37 WDS

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		

WDS Setting

WDS Config

WDS Mode

Disable

Disable

Lazy Mode

Bridge Mode

Repeater Mode

Save & Apply

Save

Description

WDS stands for Wireless Distribution System, enabling WDS access points to be interconnected to expand a wireless network.

WPS

WPS (Wi-Fi Protected Setup) provides easy procedure to make network connection between wireless station and wireless access point with the encryption of WPA and WPA2.

It is the simplest way to build connection between wireless network clients and wireless access point. Users do not need to select any encryption mode and type any long encryption passphrase to setup a wireless client every time. The only requirement is for the user to press the WPS button on the wireless client, and WPS will connect for client and router automatically.

Table 38 WPS

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		

WPS Setting

WPS Config

WPS Enable ▼

WPS Summary

WPS Current Status	Idle
WPS Configured	Yes
WPS SSID	Safelink_0408

WPS Progress

WPS Mode

☐ PIN
☒ PBC

WPS Status

WPS:Idle

Field Name	Description
WPS Config	
WPS	Enable/Disable WPS function
WPS Summary	
WPS Current Status	Display the current status of WPS
WPS Configured	Display the configure the status information of WPS
WPS SSID	Display WPS SSID
WPS Progress	
WPS Mode	<p>PIN: Enter the PIN code of the wireless device which accesses to this LAN in the following option, and press apply. Then router begins to send signals, turn on the PIN accessing method on the clients, and then it can access the wireless AP automatically.</p> <p>PBC: There are two ways to start PBC mode, user can press the PBC button directly on the device, or select PBC mode on the software and apply. Users can activate WPS connection in WPS mode through these two methods, only when the clients choose PBC access, the clients can connect the AP automatically.</p>

WPS Status	WPS shows status in three ways: WSC: Idle WSC: Start WSC process (begin to send messages) WSC: Success; this means clients have accessed the AP successfully
------------	---

Station Info

Table 39 Station info

StatusNetworkWireless 2.4GHzWireless 5GHzSIPFXS1FXS2SecurityApplication

BasicWireless SecurityWMMWDSWPSStation InfoAdvanced

Wireless Status

Wireless Status

Current ChannelChannel 1

FWR9502-0000C800:21:F2:00:00:10

Wireless Network

Wireless Network

MAC AddressAidPSMMIMO PS TX Rate TxBRSSIStream SNRSnd Rsp SNRLast RX RateConnect Time

Description

This page displays information about the current registered clients’ connections including operating MAC address and operating statistics.

Advanced

Table 40 Advanced

Basic

Wireless Security

WMM

WDS

WPS

Station Info

Advanced

Advanced Wireless

Advanced Wireless

BG Protection Mode

Auto

Beacon Interval

100

ms (range 20 - 999, default 100)

Data Beacon Rate (DTIM)

3

(range 1 - 255, default 3)

Fragment Threshold

2346

(range 256 - 2346, default 2346)

RTS Threshold

2347

(range 1 - 2347, default 2347)

TX Power

100

% (range 1 - 100, default 100)

Short Preamble

Enable

Disable

Short Slot

Enable

Disable

TX Burst

Enable

Disable

Pkt_Aggregate

Enable

Disable

Country Code

NONE

Support Channel

Ch1~14

Tx Beamforming

Disable

Wi-Fi Multimedia

WMM Capable

Multiple SSID

Multiple SSID1

Multiple SSID2

Multiple SSID3

APSD Capable

Multicast-to-Unicast Converter

Multicast-to-Unicast

Enable

Disable

Enable

Disable

Enable

Disable

Enable

Disable

Enable

Disable

Enable

Disable

Field Name

Description

BG Protection Mode

Select G protection mode, options are on, off and automatic.

Beacon Interval

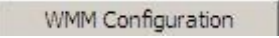
The interval of sending a wireless beacon frame, within this range, it will send a beacon frame for the information of the surrounding radio network.

Data Beacon Rate(DTIM)

Specify the interval of transmitting the indication message, it is a kind of cut down operation, and it is used for informing the next client which is going to receive broadcast multi-cast.

Fragment Threshold

Specify the fragment threshold for the packet, when the length of the packet exceeds this value, the packet is divided.

RTS Threshold	Specify the packet RTS threshold, when the packet exceeds this value, the router will send RTS to the destination site consultation
TX Power	Define the transmission power of the current AP, the greater it is, the stronger the signal is
Short Preamble	Choose enable or disable
Short Slot	Enable/Disable short slot. By default it is enabled, it is helpful in improving the transmission rate of wireless communication
Tx Burst	One of the features of MAC layer, it is used to improve the fairness for transmitting TCP
Pkt_Aggregate	It is a mechanism that is used to enhance the LAN, in order to ensure that the home gateway packets are sent to the destination correctly
Support Channel	Choose appropriate channel
Wi-Fi Multimedia (WMM)	
WMM Capable	Enable/Disable WMM.
APSD Capable	Enable/Disable APSD. Once it is enabled, it may affect wireless performance, but can play a role in energy-saving power
WMM Parameters	Press  , the webpage will jump to the configuration page of Wi-Fi multimedia
Multicast-to-Unicast Converter	Enable/Disable Multicast-to-Unicast. By default, it is Disabled

Wireless 5G

Please refer to the [wireless 2.4G](#).

SIP

SIP Settings

Table 41 SIP settings

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application																																																						
<div>SIP Settings VoIP QoS Dial Rule Blacklist Call Log</div>																																																														
<div>SIP Parameters</div>																																																														
<div>SIP Parameters</div> <table> <tr> <td>SIP T1</td> <td>500</td> <td>ms</td> <td>Max Forward</td> <td>70</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>SIP User Agent Name</td> <td colspan="2"></td> <td>Max Auth</td> <td>2</td> <td></td> <td></td> <td></td> <td></td> </tr> <tr> <td>Reg Retry Intvl</td> <td>30</td> <td>sec</td> <td>Reg Retry Long Intvl</td> <td>60</td> <td>sec</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Mark All AVT Packets</td> <td colspan="2">Enable ▼</td> <td>RFC 2543 Call Hold</td> <td colspan="2">Enable ▼</td> <td></td> <td></td> <td></td> </tr> <tr> <td>SRTP</td> <td colspan="2">Disable ▼</td> <td>SRTP Prefer Encryption</td> <td colspan="2">AES_CM ▼</td> <td></td> <td></td> <td></td> </tr> <tr> <td>Service Type</td> <td colspan="2">Common ▼</td> <td>DNS Refresh Timer</td> <td>0</td> <td>sec</td> <td></td> <td></td> <td></td> </tr> </table>									SIP T1	500	ms	Max Forward	70					SIP User Agent Name			Max Auth	2					Reg Retry Intvl	30	sec	Reg Retry Long Intvl	60	sec				Mark All AVT Packets	Enable ▼		RFC 2543 Call Hold	Enable ▼					SRTP	Disable ▼		SRTP Prefer Encryption	AES_CM ▼					Service Type	Common ▼		DNS Refresh Timer	0	sec			
SIP T1	500	ms	Max Forward	70																																																										
SIP User Agent Name			Max Auth	2																																																										
Reg Retry Intvl	30	sec	Reg Retry Long Intvl	60	sec																																																									
Mark All AVT Packets	Enable ▼		RFC 2543 Call Hold	Enable ▼																																																										
SRTP	Disable ▼		SRTP Prefer Encryption	AES_CM ▼																																																										
Service Type	Common ▼		DNS Refresh Timer	0	sec																																																									

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 The AC1100MSF 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

Table 42 VoIP QoS

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
<div>SIP Settings VoIP QoS Dial Rule Blacklist Call Log</div>								
<div>QoS Settings</div> <div> <div>Layer 3 QoS</div> <div> <div>SIP QoS(0-63)</div> <div>46</div> </div> <div> <div>RTP QoS(0-63)</div> <div>46</div> </div> </div> <div> <div>Save</div> <div>Cancel</div> <div>Reboot</div> </div>								
Field Name	Description							
SIP /RTP QoS	The default value is 0,you can set a range of values is 0~63							

Dial Plan

Parameters and Settings

Table 43 Parameters and settings

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
<div>SIP Settings</div> <div>VoIP QoS</div> <div>Dial Rule</div> <div>Blacklist</div> <div>Call Log</div>								
Dial Rule								
<div>General</div> <div> Dial Rule <div>Disable ▾</div> Unmatched Policy <div>Accept ▾</div> </div>								
No.	FXS	Digit Map	Action	Move Up	Move Down			
1	FXS 1	vb	Deny	▲	▼	<input type="checkbox"/>		
2	FXS 1	rgg	Deny	▲	▼	<input type="checkbox"/>		
FXS <div>FXS 1 ▾</div> Digit Map <div></div> Action <div>Deny ▾</div> <div>OK Cancel</div>								
<div>Save Cancel Reboot</div>								

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 router will reject the matched number, while Dial Out means router 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

Table 44 Adding one dial plan

Dial Plan

General

Dial Plan

Disable ▾

Unmatched Policy

▾

No.

FXS

Digit Map

Action

Move Up

Move Down

FXS

FXS 1 ▾

Digit Map

Action

Deny ▾

OK

Cancel

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

Table 45 Dial Plan

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]	<p>To match one character form sequence. For example:</p> <p>[0-9]: match one digit from 0 to 9</p> <p>[23-5*]: match one character from 2 or 3 or 4 or 5 or *</p>
4	x.	<p>Match to x, xx, xxx, xxxx and so on.</p> <p>For example:</p> <p>“01” can be match to “0”, “01”, “011”...“011111...” and so on</p>
5	<diald:substituted>	<p>Replace dialed with substituted.</p> <p>For example:</p> <p><8:1650>123456: input is “85551212” , output is “16505551212”</p> <p>Make outside dial tone after dialing “x” , stop until dialing character “y”</p> <p>For example:</p> <p>“9,1xxxxxxxxx” :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> <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>
6	x,y	
7	T	

Blacklist

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

Table 46 Blacklist

Blacklist Upload && Download

Blacklist Upload && Download

Local File

Choose File

No file chosen

Upload CSV

Download CSV

Blacklist

Index	Name	Number	
1	Rob	12345	<input type="checkbox"/>
2	Henry	123456	<input type="checkbox"/>

Edit

Add

Delete

Move to phonebook

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

Table 47 Call log

Redial List				
Index	NUMBER	Start Time	Duration	<input type="checkbox"/>
1	123	10/28 10:30	00:00:07	<input type="checkbox"/>
2	010123	10/28 12:02	00:00:01	<input type="checkbox"/>
3	010123	10/28 16:16	00:00:00	<input type="checkbox"/>
4	010123	10/28 16:16	00:00:00	<input type="checkbox"/>
5	123	10/28 16:20	00:00:13	<input type="checkbox"/>
6	123	10/28 16:21	00:00:34	<input type="checkbox"/>
7	123	10/29 10:50	00:00:10	<input type="checkbox"/>
8	123	10/29 14:36	00:00:01	<input type="checkbox"/>
9	123	10/29 15:05	00:00:23	<input type="checkbox"/>
10	123	10/29 15:06	00:00:05	<input type="checkbox"/>
..	<input type="checkbox"/>

Redial List

Answered Calls				
Index	NUMBER	Start Time	Duration	<input type="checkbox"/>
1	22222	10/21 09:56	00:00:40	<input type="checkbox"/>
2	110	10/21 18:14	00:00:03	<input type="checkbox"/>
3	110	10/21 18:15	00:00:07	<input type="checkbox"/>
4	sipp	10/23 13:40	00:00:06	<input type="checkbox"/>
5	sipp	10/24 18:05	00:00:05	<input type="checkbox"/>
6	sipp	10/24 18:05	00:00:05	<input type="checkbox"/>
7	sipp	10/25 15:38	00:00:03	<input type="checkbox"/>
8	sipp	10/25 15:42	00:00:06	<input type="checkbox"/>
9	sipp	10/25 15:55	00:00:10	<input type="checkbox"/>
10	sipp	10/25 16:03	00:00:02	<input type="checkbox"/>
..	<input type="checkbox"/>

Answered Calls

Missed Calls

Index	NUMBER	Start Time	Duration	
1	110	10/21 09:50	00:00:03	
2	555	10/22 12:04	00:00:03	

Missed Calls

FXS1

SIP Account

Basic

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

Table 48 SIP Account - Basic

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application
<div>SIP Account Preferences</div>								
<div>Basic</div>								
<div>Basic Setup</div> <div> <div>Line Enable</div> <div>Enable ▼</div> </div> <div> <div>Outgoing Call without Registration</div> <div>Disable ▼</div> </div>								
<div>Proxy and Registration</div> <div> <div>Proxy Server</div> <div></div> </div> <div> <div>Outbound Server</div> <div></div> </div> <div> <div>Backup Outbound Server</div> <div></div> </div> <div> <div>Allow DHCP Option 120 to Override SIP Server</div> <div>Disable ▼</div> </div> <div> <div>Proxy Port</div> <div>5060</div> </div> <div> <div>Outbound Port</div> <div>5060</div> </div> <div> <div>Backup Outbound Port</div> <div>5060</div> </div>								
<div>Subscriber Information</div> <div> <div>Display Name</div> <div></div> </div> <div> <div>Account</div> <div></div> </div> <div> <div>Phone Number</div> <div></div> </div> <div> <div>Password</div> <div></div> </div>								
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 dial 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 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 Configuration

Table 49 Audio configuration

Audio Configuration	
Codec Setup	
Audio Codec Type 1	G.711U ▼
Audio Codec Type 3	G.729 ▼
Audio Codec Type 5	G.723 ▼
Packet Cycle(ms)	20ms ▼
Echo Cancel	Enable ▼
Audio Codec Type 2	G.711A ▼
Audio Codec Type 4	G.722 ▼
G.723 Coding Speed	5.3k bps ▼
Silence Supp	Disable ▼
Auto Gain Control	Disable ▼
FAX Configuration	
FAX Mode	T.38 ▼
T.38 CNG Detect Enable	Disable ▼
gpmid attribute Enable	Disable ▼
ByPass Attribute Value	fax ▼
T.38 CED Detect Enable	Enable ▼
T.38 Redundancy	Disable ▼

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
gpmc attribute Enable	Enable/Disable gpmc attribute.

Supplementary Service Subscription

Table 50 Supplementary service

Supplementary Service Subscription

Supplementary Services

Call Waiting	<input type="button" value="Enable"/>		Hot Line	<input type="text"/>
MWI Enable	<input type="button" value="Enable"/>		Voice Mailbox Numbers	<input type="text"/>
MWI Subscribe Enable	<input type="button" value="Disable"/>		VMWI Serv	<input type="button" value="Enable"/>
DND	<input type="button" value="Disable"/>			

Speed Dial

Speed Dial 2	<input type="text"/>		Speed Dial 3	<input type="text"/>
Speed Dial 4	<input type="text"/>		Speed Dial 5	<input type="text"/>
Speed Dial 6	<input type="text"/>		Speed Dial 7	<input type="text"/>
Speed Dial 8	<input type="text"/>		Speed Dial 9	<input type="text"/>

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 user 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) If enable, any phone call cannot arrive at the device; default is disable
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

Table 51 Advanced

Advanced	
Advanced Setup	
Domain Name Type	Enable ▼
Signal Port	5060
RFC2833 Payload(>=96)	101
RTP Port	0 (=0 auto select)
Session Refresh Time(sec)	0
Prack Enable	Disable ▼
Primary SER Detect Interval	0
Keep-alive Interval(10-60s)	15
Anonymous Call Block	Disable ▼
Use OB Proxy In Dialog	Disable ▼
Dial Prefix	
Hold Method	ReINVITE ▼
Only Recv Request From Server	Enable ▼
SIP Received Detection	Disable ▼
Country Code	
Caller ID Header	FROM ▼
Carry Port Information	Disable ▼
DTMF Type	RFC2833 ▼
Register Refresh Interval(sec)	3600
Cancel Message Enable	Disable ▼
Refresher	UAC ▼
SIP OPTIONS Enable	Disable ▼
Max Detect Fail Count	3
Anonymous Call	Disable ▼
Proxy DNS Type	A Type ▼
Reg Subscribe Enable	Disable ▼
User Type	IP ▼
Request-URI User Check	Disable ▼
Server Address	
VPN	Disable ▼
Remove Country Code	Disable ▼

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(sec)	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(10-60s)	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 enable, 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.

Preferences

Volume Settings

Table 52 Volume settings

Preferences	
Volume Settings	
Handset Input Gain	5 ▼
Handset Volume	5 ▼

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

Regional

Table 53 Regional

Regional

Tone Type	<input type="text" value="China"/>		
Dial Tone	<input type="text"/>		
Busy Tone	<input type="text"/>		
Off Hook Warning Tone	<input type="text"/>		
Ring Back Tone	<input type="text"/>		
Call Waiting Tone	<input type="text"/>		
Min Jitter Delay(0-600ms)	<input type="text" value="20"/>	Max Jitter Delay(20-1000ms)	<input type="text" value="160"/>
Ringing Time(10-300sec)	<input type="text" value="60"/>		
Ring Waveform	<input type="text" value="Sinusoid"/>	Ring Voltage(40-63 Vrms)	<input type="text" value="45"/>
Ring Frequency(15-30Hz)	<input type="text" value="25"/>	VMWI Ring Splash Len(0.1-10sec)	<input type="text" value="0.5"/>
Flash Time Max(0.2-1sec)	<input type="text" value="0.9"/>	Flash Time Min(0.1-0.5sec)	<input type="text" value="0.1"/>

Field Name	Description
Tone Type	Choose tone type form China, US, Hong Kong and so on
Dial Tone	Dial Tone
Busy Tone	Busy Tone
Off Hook Warning Tone	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

Table 54 Features and call forward

Features			
All Forward	<input type="button" value="Disable"/>	Busy Forward	<input type="button" value="Disable"/>
No Answer Forward	<input type="button" value="Disable"/>		

Call Forward			
All Forward	<input type="text"/>	Busy Forward	<input type="text"/>
No Answer Forward	<input type="text"/>	No Answer Timeout	<input type="text" value="20"/>

Feature Code			
Hold Key Code	<input type="text" value="*77"/>	Conference Key Code	<input type="text" value="*88"/>
Transfer Key Code	<input type="text" value="*98"/>	IVR Key Code	<input type="text" value="****"/>
R Key Enable	<input type="button" value="Disable"/>	R Key Cancel Code	<input type="button" value="R1"/>
R Key Hold Code	<input type="button" value="R2"/>	R Key Transfer Code	<input type="button" value="R4"/>
R Key Conference Code	<input type="button" value="R3"/>	Speed Dial Code	<input type="text" value="*74"/>

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.

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 range from R1 to R9, default value is R1.
R key hold code	Set the R key hold code, options range from R1 to R9, default value is R2.
R key transfer code	Set the R key transfer code, options range from R1 to R9, default value is R4.
R key conference code	Set the R key conference code, options range from R1 to R9, default value is R3.
Speed Dial Code	Speed dial code, default is *74.

Miscellaneous

Table 55 Miscellaneous

Miscellaneous

Codec Loop Current	<input type="text" value="26"/>	Impedance Matching	<input type="text" value="US PBX,Korea,Taiwan(600)"/>
CID Service	<input type="button" value="Enable"/>	CWCID Service	<input type="button" value="Disable"/>
Caller ID Method	<input type="text" value="Bellcore"/>	Polarity Reversal	<input type="button" value="Disable"/>
Dial Time Out(IDT)	<input type="text" value="5"/>	Call Immediately Key	<input type="text" value="#"/>
ICMP Ping	<input type="button" value="Disable"/>	Escaped char enable	<input type="button" value="Disable"/>
Bellcore Style 3-Way Conference	<input type="button" value="Disable"/>		

Field Name	Description
Codec Loop Current	Set off-hook loop current, default is 26.
Impedance Matching	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 enable.
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 form * or #.
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 #.

FXS2

The settings of FXS2 are the same as FXS1. See FXS1 on page 74.

Security

Filtering Setting

Table 56 Filtering setting

Basic Settings	
Basic Settings	
Filtering	Disable ▼
Default Policy	Drop ▼
The packet that don't match with any rules would be Drop	
Save	Cancel

IP/Port Filter Settings	
Interface	LAN ▼
Mac address	<input type="text"/>
Dest IP Address	<input type="text"/>
Source IP Address	<input type="text"/>
Protocol	NONE ▼
Dest. Port Range	<input type="text"/> - <input type="text"/>
Src Port Range	<input type="text"/> - <input type="text"/>
Action	Accept ▼
Comment	<input type="text"/>
(The maximum rule count is 32)	
Save	Cancel

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

Table 57 Content filtering

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application				
<div>Filtering Setting Content Filtering Router Limits</div>												
Basic Settings												
Basic Settings <div> <div>Filtering Disable ▼</div> <div>Default Policy Accept ▼</div> <div> Save Cancel </div> </div>												
Filter List Upload & Download <div> <div>Local File Choose File No file chosen</div> <div> Upload Download </div> </div>												
Web URL Filter Settings												
Current Web URL Filters <table border="1"> <thead> <tr> <th>No.</th> <th>URL</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table> <div> Delete Cancel </div>									No.	URL		
No.	URL											
Add a URL Filter <div> <div>URL <input type="text"/></div> <div>(The maximum rule count is 16)</div> <div> Add Cancel </div> </div>												
Web Host Filter Settings												
Current Website Host Filters <table border="1"> <thead> <tr> <th>No.</th> <th>Keyword</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> </tr> </tbody> </table> <div> Delete Cancel </div>									No.	Keyword		
No.	Keyword											
Add a Host (keyword) Filter <div> <div>Keyword <input type="text"/></div> <div>(The maximum rule count is 16)</div> <div> Add Cancel </div> </div>												

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

Application

Advance NAT

Table58 advance NAT

Advance Nat	UPnP	IGMP
ALG		
ALG Setting		
FTP	Enable ▼	
SIP	Disable ▼	
H323	Disable ▼	
PPTP	Disable ▼	
L2TP	Disable ▼	
IPSec	Disable ▼	
<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Reboot"/>		

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.

Table 59 UPnP

UPnP
UPnP Setting
Enable UPnP <div> Enable ▼ Disable Enable </div>
<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Reboot"/>

Field Name	Description
UPnP enable	Enable/Disable UPnP function.

IGMP

Multicast has the ability to send the same data to multiple devices.

IP hosts use IGMP (Internet Group Management Protocol) report multicast group memberships to the neighboring routers to transmit data, at the same time, the multicast router use IGMP to discover which hosts belong to the same multicast group.

Table 60 IGMP

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Administration
Advance Nat	UPnP	IGMP						
IGMP								
IGMP Setting								
IGMP Proxy enable <input type="button" value="Enable"/> IGMP Snooping enable <input type="button" value="Enable"/>								
<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Reboot"/>								

Field Name	Description
IGMP Proxy enable	Enable/Disable IGMP Proxy function.
IGMP Snooping enable	Enable/Disable IGMP Snooping function.

Storage

Disk Management

This page is used to manage the USB storage device.

Table 61 Disk Management

StatusNetworkWireless 2.4GHzWireless 5GHzSIPFXS1FXS2SecurityApplicationStorage

Disk ManagementFTP SettingSMB Setting

Disk ManagementHelp

Folder List

Directory PathPartitionAddDeleteRemove Disk

Partition Status

PartitionPathFormatReallocate

Field Name	Description
Add	Adding files to the USB storage device
Delete	Remove the USB storage device file
Remove Disk	Transfer files within a USB storage device
Format	Format the USB storage device
Re-allocate	Reset the USB storage device

FTP Setting

Table 62 FTP Setting

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application	Storage
<div>Disk Management FTP Setting SMB Setting</div>									
FTP Setting									Help
FTP Server Setup									
<div> <div>FTP Server</div> <div> <input type="radio"/> Enable <input checked="" type="radio"/> Disable </div> </div> <div> <div>FTP Server Name</div> <div>FTP</div> </div> <div> <div>Anonymous Login</div> <div> <input type="radio"/> Enable <input checked="" type="radio"/> Disable </div> </div> <div> <div>FTP Port</div> <div>21</div> </div> <div> <div>Max. Sessions</div> <div>10</div> </div> <div> <div>Create Directory</div> <div> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </div> </div> <div> <div>Rename File/Directory</div> <div> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </div> </div> <div> <div>Remove File/Directory</div> <div> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </div> </div> <div> <div>Read File</div> <div> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </div> </div> <div> <div>Write File</div> <div> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </div> </div> <div> <div>Download Capability</div> <div> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </div> </div> <div> <div>Upload Capability</div> <div> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </div> </div>									

Field Name	Description
FTP Server	Enable/Disable FTP server
FTP Server Name	Set the FTP server name
Anonymous Login	If or not support anonymous login
FTP Port	Set FTP server port number
Max. Sessions	Maximum number of connections
Create Directory	Enable/Disable create directory
Rename File/Directory	Enable/Disable rename file/directory
Remove File/Directory	Enable/Disable transfer of files/directories
Read File	Enable/Disable read files
Write File	Enable/Disable write files
Download Capability	Enable/Disable download capability function.
Upload Capability	Enable/Disable upload capability function

Smb Setting

Table 63 Smb setting

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application	Storage	Administration								
<div> <div>Disk Management</div> <div>FTP Setting</div> <div>SMB Setting</div> </div>																		
SMB Setting										Help								
SAMBA Server Setup																		
<table border="1"> <tr> <td>SAMBA Server</td> <td> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </td> </tr> <tr> <td>Workgroup</td> <td>AC1100MSF</td> </tr> <tr> <td>NetBIOS Name</td> <td>ReadyNet</td> </tr> <tr> <td>Anonymous Login</td> <td> <input checked="" type="radio"/> Enable <input type="radio"/> Disable </td> </tr> </table>											SAMBA Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable	Workgroup	AC1100MSF	NetBIOS Name	ReadyNet	Anonymous Login	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
SAMBA Server	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																	
Workgroup	AC1100MSF																	
NetBIOS Name	ReadyNet																	
Anonymous Login	<input checked="" type="radio"/> Enable <input type="radio"/> Disable																	
Sharing Directory List																		
<table border="1"> <thead> <tr> <th>Directory Name</th> <th>Directory Path</th> <th>Allowed Users</th> </tr> </thead> <tbody> <tr> <td></td> <td></td> <td></td> </tr> </tbody> </table> <div> <div>Add</div> <div>Edit</div> <div>Delete</div> </div>											Directory Name	Directory Path	Allowed Users					
Directory Name	Directory Path	Allowed Users																
<div> <div>Apply</div> <div>Cancel</div> </div>																		

Field Name	Description
SAMBA Server	Enable/Disable SAMBA server
Workgroup	Enter the working group
NetBIOS Name	Network basic input/output system name
Add	Add a shared file
Edit	Edit a shared file
Del	Delete a shared file
Add	Add a shared file
Edit	Edit a shared file
Del	Delete a shared file

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.

Management

Save config file

Table 64 Save Config File

Management		Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diagnosis
Save Config File								
Config File Upload & Download								
<div>Local File</div> <div> <input type="button" value="Choose File"/> No file chosen </div> <div> <input type="button" value="Upload"/> <input type="button" value="Download"/> </div>								
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

Table 65 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

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

Table 66 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

Daylight Saving Time

Table 67 Daylight Saving Time

Daylight Saving Time

Daylight Saving Time	Enable ▼
Offset	60 Min.
Start Month	April ▼
Start Day of Week	Sunday ▼
Start Day of Week Last in Month	First in Month ▼
Start Hour of Day	2
Stop Month	October ▼
Stop Day of Week	Sunday ▼
Stop Day of Week Last in Month	Last in Month ▼
Stop Hour of Day	2

Procedure

Step 1. Enable Daylight Savings Time.

Step 2. Set value of offset for Daylight Savings Time

Step 3: Set starting Month/Week/Day/Hour in Start Month/Start Day of Week Last in Month/Start Day of Week/Start Hour of Day, analogously set stopping Month/Week/Day/Hour in Stop Month/Stop Day of Week Last in Month/Stop Day of Week/Stop Hour of Day.

Step 4. Press Saving button to save and press Reboot button to active changes.

System Log Setting

Table 68 System log Setting

System Log Setting	
Syslog Setting <div> <div>Syslog Enable</div> <div>Syslog Level</div> <div>Login Syslog Enable</div> <div>Call Syslog Enable</div> <div>Net Syslog Enable</div> <div>Device Management Syslog Enable</div> <div>Device Alarm Syslog Enable</div> <div>Kernel Syslog Enable</div> <div>Remote Syslog Enable</div> <div>Remote Syslog Server</div> <div> <div>Enable ▼</div> <div>INFO ▼</div> <div>Enable ▼</div> <div>Enable ▼</div> <div>Enable ▼</div> <div>Enable ▼</div> <div>Enable ▼</div> <div>Enable ▼</div> <div>Disable ▼</div> <div></div> </div> </div>	
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	Enable/Disable remote syslog function
Remote Syslog server	Add a remote server IP address.
Syslog Enable	Enable/Disable syslog function

Factory Defaults Setting

Table 69 Factory Defaults Setting

Factory Defaults Setting	
Factory Defaults Setting <div> <div>Factory Defaults Lock</div> <div>Disable ▼</div> </div>	
Description	
When enabled, the device may not be reset to factory defaults until this parameter is reset to Disable.	

Factory Defaults

Table 70 Factory Defaults

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

Firmware Upgrade

Table 71 Firmware upgrade

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application	Storage	Administration
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diagnosis	Operating Mode		
Firmware Management										Help
Firmware Upgrade										Firmware Upgrade: Click on the <i>Browse...</i> button to select the firmware file to be uploaded to the router. Click the <i>Upgrade</i> button to begin the upgrade process. Once begun, the Upgrade process must not be interrupted.
Local Upgrade <input type="button" value="Choose File"/> No file chosen										
<input type="button" value="Upgrade"/>										
Description										
1. Click Choose File										
3. Press <input type="button" value="Upgrade"/> to start upgrading										

LTE Upgrade

Table 72 LTE upgrade

Management	Firmware Upgrade	LTE Upgrade	Scheduled Tasks	Provision	SNMP	TR-069	Diagnosis
------------	------------------	-------------	-----------------	-----------	------	--------	-----------

LTE Management

LTE Upgrade

Download URL

Description

You can fill in LTE download URL, upgrade LTE

Scheduled Tasks

Table 73 Scheduled Tasks

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application	Storage	Administration
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diagnosis	Operating Mode		

Scheduled Tasks

Scheduled Wi-Fi

No.	Enable	SSID	Week Select	Open Time	Close Time
<input type="button" value="Delete Selected"/> <input type="button" value="Add"/> <input type="button" value="Edit"/>					

Scheduled Reboot

Scheduled Reboot

Scheduled Mode

Time :

Scheduled PPPoE

Scheduled PPPoE

Scheduled Mode

Time :

Help

Scheduled Tasks:

This function is to set a time to automatically turn on or off the Wi-Fi, or reboot or restart PPPoE.

Field Name	Description
Scheduled Wi-Fi	
Enable	Enable / Disable Timed WI-FI
SSID	This is not optional
Scheduled Mode	Choose work mode, weekly / days
Wi-Fi work time	Set the WI-FI duty cycle
Apply and Cancel	After modifying the parameters, select Apply, or Cancel
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 router 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.

Table 74 Provision

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application	Storage	Administration
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diagnosis	Operating Mode		

Provision

Help

Configuration Profile

Provision Enable

Resync on Reset

Resync Random Delay (sec)

Resync Periodic (sec)

Resync Error Retry Delay (sec)

Forced Resync Delay (sec)

Resync after Upgrade

Resync from SIP

Option 66

Option 67

Config File Name

User Agent

Profile Rule

Firmware Upgrade

Enable Upgrade

Upgrade Error Retry Delay (sec)

Upgrade Rule

Provision:
'Provision' allows a device to automatically resync to a specific configuration file on a TFTP or web server utilising HTTP or HTTPS

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 router 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 router will wait for a period time, the longest is “Forced Resync Delay” , default is 14400s, when the time over, the router 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.

Table 75 Firmware Upgrade**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 router will try upgrading again after “Upgrade Error Retry Delay” period, default is 3600s
Upgrade Rule	URL of upgrade file

SNMP

Table 76 SNMP

Management	Firmware Upgrade	LTE Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069
SNMP Configuration							
SNMP Configuration							
SNMP Service		Enable ▼					
Trap Server Address		183.234.48.155					
Read Community Name		public					
Write Community Name		private					
Trap Community		trap					
Trap Period Interval (sec)		300					
<input type="button" value="Save & Apply"/> <input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Reboot"/>							

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.

Table 77 TR069

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application	Storage	Administration
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR-069	Diagnosis	Operating Mode		

TR-069 Configuration

Help

ACS

TR-069 Enable

CWMP

ACS URL

User Name

Password

Enable Periodic Inform

Periodic Inform Interval

Connection Request

User Name

Password

TR-069 Configuration:
Allows the device to be managed by the ACS server configured in the ACS URL.

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.

Table 78 Diagnosis

Management

Firmware Upgrade

Scheduled Tasks

Certificates

Provision

SNMP

TR-069

Diagnosis

Packet Capture

Packet Capture

Tracking Interface

WAN

Filtering Rule

ALL Packets

Upload Packet Enable

Disable

Packet Capture

start

stop

save

Ping Test

Ping Test

Dest IP/Host Name

WAN Interface

1_MANAGEMENT_VOICE_INTERNET_R_VID

Apply

Cancel

Traceroute Test

Traceroute Test

Dest IP/Host Name

WAN Interface

1_MANAGEMENT_VOICE_INTERNET_R_VID

Apply

Cancel

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

```
PING www.baidu.com (115.239.210.26): 56 data bytes
64 bytes from 115.239.210.26: seq=0 ttl=54 time=43.979 ms
64 bytes from 115.239.210.26: seq=1 ttl=54 time=53.875 ms
64 bytes from 115.239.210.26: seq=2 ttl=54 time=45.226 ms
64 bytes from 115.239.210.26: seq=3 ttl=54 time=49.534 ms
64 bytes from 115.239.210.26: seq=4 ttl=54 time=49.045 ms

--- www.baidu.com ping statistics ---
5 packets transmitted, 5 packets received, 0% packet loss
round-trip min/avg/max = 43.979/48.331/53.875 ms
```

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

```
traceroute to www.google.com (216.58.208.68), 30 hops max, 38 byte packets
 1 10.110.134.254 (10.110.134.254) 1.017 ms 9.507 ms 1.419 ms
 2 ***
 3 ***
 4 ***
 5 ***
 6 ***
 7 ***
 8 ***
 9 ***
10 ***
.. ***
```

Apply

Cancel

Operating Mode

Table 79 Operating mode

Management	Firmware Upgrade	LTE Upgrade	Scheduled Tasks	Provision	SNMP	TR-069	Diagnosis	Operating Mode
Operating Mode Settings								Help
Operating Mode Settings								
<div>Operating Mode</div> <div>Advanced Mode ▼ Basic Mode Advanced Mode</div> <div>Save & ApplyCancelReboot</div>								
Description								
Choose the Operation Mode as Basic Mode or Advanced Mode.								

System Log

Table 80 System log

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application	Storage	Administration
Basic	LAN Host	Syslog	LAN Host Statistics							
<div>RefreshClearSave</div> <div>Manufacturer:READYNET ProductClass:AC1100MSF SerialNumber:11MSF000030 BuildTime:202004111810 IP:192.168.11.1:8080 HWVer:V3.1 SWVer:V3.32 <Mon Nov 25 00:51:44 2019> provision[14828]: Update configuration failed, retry 3600 s later <Mon Nov 25 01:51:44 2019> provision[14828]: start to check config file <Mon Nov 25 01:51:44 2019> provision[14828]: server response without OK msg <Mon Nov 25 01:51:44 2019> provision[14828]: HTTP get configuration file failed <Mon Nov 25 01:51:44 2019> provision[14828]: Update configuration failed, retry 3600 s later <Mon Nov 25 02:51:44 2019> provision[14828]: start to check config file <Mon Nov 25 02:51:44 2019> provision[14828]: server response without OK msg <Mon Nov 25 02:51:44 2019> provision[14828]: HTTP get configuration file failed <Mon Nov 25 02:51:45 2019> provision[14828]: Update configuration failed, retry 3600 s later <Mon Nov 25 03:51:44 2019> provision[14828]: start to check config file <Mon Nov 25 03:51:45 2019> provision[14828]: server response without OK msg <Mon Nov 25 03:51:45 2019> provision[14828]: HTTP get configuration file failed</div>										

Description

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

Logout

Table 81 Logout

<div>ReadyNetCONNECTIVITY SIMPLIFIED</div> <div>AC1100MSF</div> <div>Firmware Version V3.32 Current Time 2020-04-11 10:53:59 Admin Mode [Logout][Reboot]</div>										
Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application	Storage	Administration
Basic	LAN Host	Syslog	LAN Host Statistics							

Description

Press the logout button to logout, and then the login window will appear.

Reboot

Press the

Reboot

 button to reboot the device.

Chapter 4 IPv6 address configuration

The router devices support IPv6 addressing. This chapter covers:

- [Introduction](#)
- [IPv6 Advance](#)
- [Configuring IPv6](#)
- [Viewing WAN port status](#)
- [IPv6 DHCP configuration for LAN/WLAN clients](#)
- [LAN DHCPv6](#)

Introduction

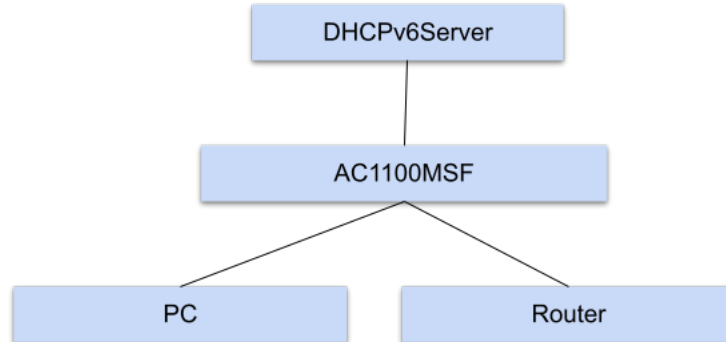
DHCPv6 protocol is used to automatically provision/configure IPv6 capable end points in a local network. In addition to acquiring an IPv6 IP address for the WAN interface and its associated LAN/WLAN clients, the devices are also capable of prefix delegation.

The Routers devices support the following types of modes of IPv6 addresses:

- Stateless DHCPv6
- Statefull DHCPv6

Table 82 IPv6 Modes

Mode	Description
Stateless	In Stateless DHCPv6 mode, the Routers devices listen for ICMPv6 Router Advertisements messages which are periodically sent out by the routers on the local link or requested by the node using a Router Advertisements solicitation message. The device derives a unique IPv6 address using prefix receives from the router and its own MAC address.



Statefull	In Statefull DHCPv6 mode, the client works exactly as IPv4 DHCP, in which hosts receive both their IPv6 addresses and additional parameters from the DHCP server.
-----------	---

IPv6 Advance

To enable IPv6 functionality:

Navigate to Network > IPv6 Advanced page.

Select Enable from the IPv6 Enable drop-down list.

Click Save.

Table 83 Enabling IPv6

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application		
WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN	QoS	Rate
Advance										

IPv6 Advanced Settings

IPv6 Enable

IPv6 Enable

Enable ▼

Save & Apply

Save

Cancel

Reboot

Configuring IPv6

Configuring Statefull IPv6

1. Navigate to Network > IPv6WAN page. The following window is displayed:

Table 84 Configuring Statefull IPv6

WAN

LAN

IPv6 Advanced

IPv6 WAN

IPv6 LAN

VPN

Port Forward

DMZ

VLAN

QoS

Rat

Advance

IPv6 WAN Setting

IPv6 WAN Setting

Connection Type

DHCPv6

DHCPv6 Address Settings

Statefull

Prefix Delegation

Enable

Save

Cancel

Reboot

Field Name	Description
Connection Type	Select connection type
DHCPv6 Address Settings	Set it to statefull mode.
Prefix Delegation	Select Enable.

Configuring Stateless IPv6

Table 85 Configuring Stateless IPv6

WAN

LAN

IPv6 Advanced

IPv6 WAN

IPv6 LAN

VPN

Port Forward

DMZ

VLAN

QoS

Rate

Advance

IPv6 WAN Setting

IPv6 WAN Setting

Connection Type

DHCPv6

DHCPv6 Address Settings

Stateless

Prefix Delegation

Enable

Save

Cancel

Reboot

Field Name	Description
Connection Type	Select connection type
DHCPv6 Address Settings	Set it to stateless mode
Prefix Delegation	Select Enable

Viewing WAN port status

To view the status of WAN port:

Navigate to Status page.

Network Status	
Active WAN Interface	
Connection Type	DHCP
IP Address	192.168.10.174 <input type="button" value="Renew"/>
Link-Local IPv6 Address	
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
Primary DNS	192.168.10.1
Secondary DNS	192.168.18.1
pv6 PD Prefix	
pv6 Domain Name	
pv6 Primary DNS	
pv6 Secondary DNS	
WAN Port Status	100Mbps Full

IPv6 DHCP configuration for LAN/WLAN clients

Wired and wireless clients connected to the Routers can obtain their IPv6 addresses based on how the LAN side DHCPv6 parameters are configured. The Routers can be either configured as a DHCPv6 server in which the LAN/WLAN clients get IPv6 addresses from the configured pool. If DHCP server is disabled on the Routers, the clients will get IPv6 addresses from the external DHCPv6 server configured in the network.

LAN DHCPv6

When IPv6 is enabled, the LAN/WLAN clients of Routers can be configured to receive IPv6 addresses from locally configured IPv6 pool or from an external DHCPv6 server.

To enable LAN DHCPv6 service:

WAN	LAN	IPv6 Advanced	IPv6 WAN	IPv6 LAN	VPN	Port Forward	DMZ	VLAN	QoS	Rate L
Advance										

IPv6 LAN Setting

IPv6 LAN Setting

IPv6 Address	<input type="text" value="fec0::1"/>		
IPv6 Prefix Length	<input type="text" value="64"/>	(0-128)	
DHCPv6 Server			
DHCPv6 Status	<input type="button" value="Disable"/>		
DHCPv6 Mode	<input type="button" value="Stateless"/>		
Domain Name	<input type="text"/>		
Server Preference	<input type="text" value="255"/>	(0-255)	
Primary DNS Server	<input type="text"/>		
Secondary DNS Server	<input type="text"/>		
Lease Time	<input type="text" value="86400"/>	(0-86400sec)	
IPv6 Address Pool	<input type="text"/>	-	<input type="text"/> / <input type="text"/>
Router Advertisement			
Router Advertisement	<input type="button" value="Disable"/>		
Advertise Interval	<input type="text" value="30"/>	(10-1800sec)	
RA Managed Flag	<input type="button" value="Disable"/>		
RA Other Flag	<input type="button" value="Enable"/>		
Prefix	<input type="text"/>	/ <input type="text"/>	
Prefix Lifetime	<input type="text" value="3600"/>	(0-3600sec)	

Chapter 5 Troubleshooting Guide

This chapter covers:

- [Configuring PC to get IP Address automatically](#)
- [Cannot connect to the Web GUI](#)
- [Forgotten Password](#)

Configuring PC to get IP Address automatically

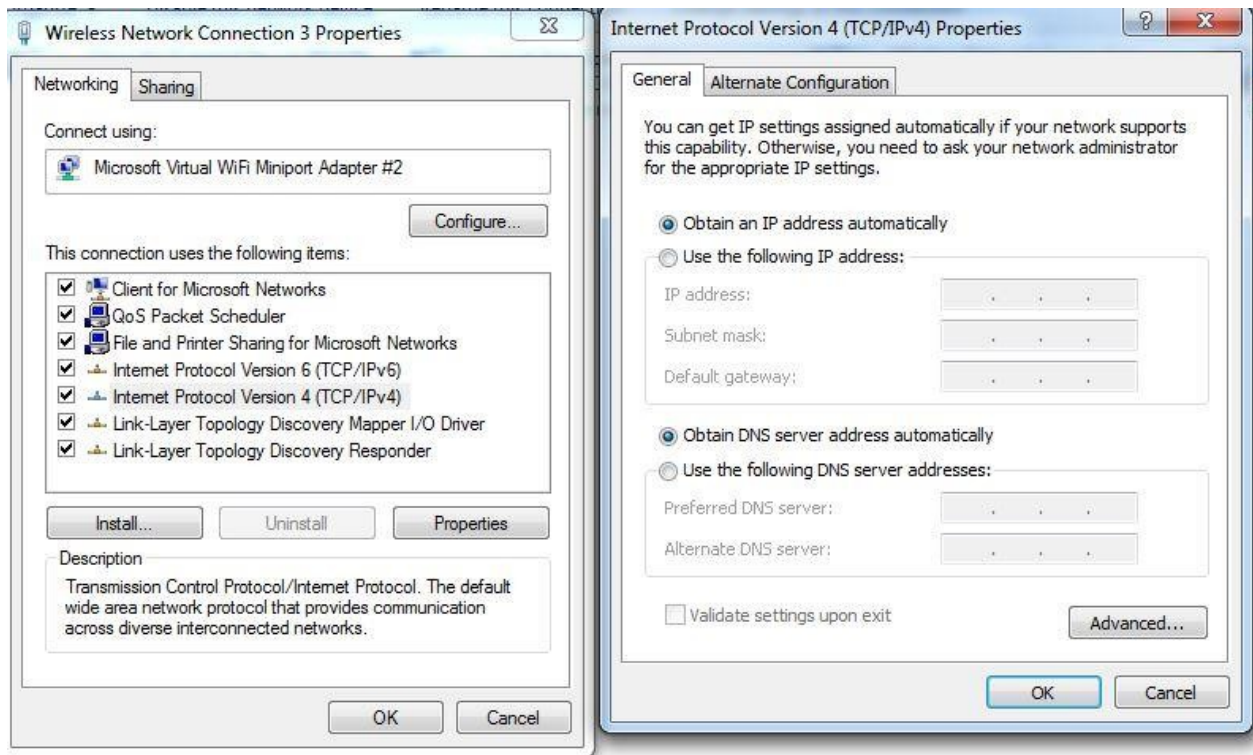
Follow the below process to set your PC to get an IP address automatically:

Step 1 : Click the “Start” button

Step 2 : Select “control panel” , then double click “network connections” in the “control panel”

Step 3 : Right click the “network connection” that your PC uses, select “attribute” and you can see the interface as shown in Figure 3.

Step 4.: Select “Internet Protocol (TCP/IP)” , click “attribute” button, then click the “Get IP address automatically” .



Cannot connect to the Web

Solution:

- Check if the Ethernet cable is properly connected.
- Check if the URL is correct. The format of URL is: http:// the IP address.
- Check on any other browser apart from Internet explorer such as Chrome.
- Contact your administrator, supplier or ITSP for more information or assistance.

Forgotten Password

If you have forgotten the management password, you cannot access the configuration web GUI. Solution:

To factory default: press and hold reset button for 10 seconds.

Appendix A

Auto-Provisioning Manual

AC1100MSF

Table of Contents

<i>Introduction.....</i>	<i>120</i>
<i>Configure Provisioning Parameters</i>	<i>121</i>
<i>Enable Provisioning.....</i>	<i>121</i>
<i>Syntax of Profile Rule and Upgrade Rule.....</i>	<i>122</i>
<i>Macro Expansion.....</i>	<i>123</i>
<i>Provisioning.....</i>	<i>124</i>
<i>Provision with HTTP.....</i>	<i>124</i>
<i>Provision with DHCP and TFTP.....</i>	<i>125</i>
<i>Provisioning Examples</i>	<i>126</i>
<i>Provisioning WAN Parameters.....</i>	<i>126</i>
<i>Provisioning LAN Parameters.....</i>	<i>127</i>
<i>Provisioning SIP Parameters</i>	<i>127</i>
<i>Appendix B.....</i>	<i>133</i>
<i>WAN Network Parameters</i>	<i>133</i>
<i>LAN Network Parameters</i>	<i>129</i>
<i>SIP Parameters</i>	<i>130</i>
<i>Administration Parameters.....</i>	<i>131</i>
<i>Provisioning Parameters</i>	<i>132</i>
<i>Default Provisioning Template File.....</i>	<i>133</i>

Auto-Provisioning of ReadyNet Router ATAs

Introduction

This document is targeted to developers and system integrators who intend to include support for the ReadyNet ATAs in their VoIP provisioning systems. It provides details for auto-provisioning ReadyNet routers with one or more ATA ports. Auto-provisioning is supported via TFTP, HTTP and HTTPS as well as DHCP Option 66, allowing for true zero-touch remote provisioning.

Configure Provisioning Parameters

This section first describes how to enable provisioning via the web interface and then describes the various parameters that can be set to control provisioning.

Enable Provisioning

To enable provisioning, log into the ReadyNet router and navigate to Administration -> Provision. The image below shows the default values for the QX202.

With the default settings, provisioning is enabled but the parameter 'Profile Rule', which is the

The screenshot displays the 'Administration' tab of the ReadyNet router web interface, specifically the 'Provision' sub-tab. The 'Provision' section is titled 'Configuration Profile' and contains the following settings:

Parameter	Value
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
Config File Name	VRT210.cfg
User Agent	ReadyNet_VRT210
Profile Rule	

Below the 'Configuration Profile' section is the 'Firmware Upgrade' section, which contains the following settings:

Parameter	Value
Upgrade Enable	Enable
Upgrade Error Retry Delay(sec)	3600
Upgrade Rule	

provisioning URL, is blank. Similarly, firmware upgrade is enabled but 'Upgrade Rule' has no value.

The table below describes the various provisioning parameters and provides their default values.

Parameter Name	Description	Default Value
Provision Enable	Enable or disable the Provision functions.	Yes
Resync on Reset	Triggers a resync after every reboot except for reboot caused by parameter updates and firmware upgrades.	Yes
Resync Random Delay	The maximum value for a random time interval that the device waits before making its initial contact with the provisioning server. This delay is effective only on the initial configuration attempt following device power-on or reset. The delay is a pseudo-random number between zero and this value. This parameter is in units of 1 second; the default value of 40 represents 40 seconds. This feature is disabled when this parameter is set to zero. It can be used to prevent an overload of the provisioning server when a large number of devices power on simultaneously.	40 seconds
Resync Periodic	The number of seconds between periodic resyncs with the provisioning server. Set this parameter to zero to disable periodic resyncing.	3600 seconds
Resync Error Retry Delay	If the last resync failed, the device will retry resync after the "Resync Error Retry Delay" seconds.	3600 seconds
Forced Resync Delay	Maximum delay in seconds the device waits before performing a resync. The device will not resync while any of its phone lines are active. Because a resync can take several seconds, wait until the device has been idle for an extended period before resyncing. This allows a user to make calls in succession without interruption. The device has a timer that begins counting down when all of its lines become idle. This parameter is the initial value of the counter. Resync events are delayed until this counter decrements to zero.	14400 seconds
Resync After Upgrade	Triggers a resync after every firmware upgrade attempt.	Yes
Option 66	If enabled, the device will also request DHCP Option 66 with its DHCP request. When enabled, the parameter 'Profile Rule' is ignored.	Yes
Config File Name	This parameter is appended to the DHCP Option 66 value returned by the DHCP server to create the TFTP provisioning URL. e.g. if the DHCP Option 66 return value is 123.45.67.89 and the 'Config File Name' parameter is a.conf, then the device will request a provisioning file from the TFTP server located at 123.45.67.89 for a file named, a.conf. This parameter is ignored when the parameter 'Option 66' is set to 'No'.	Changes for different models. For the QX202, it will be QX202.conf. For engineering samples, .cnf
Profile Rule	This parameter is a URI that evaluates to the provisioning resync command. The protocol can be TFTP and HTTP. The file name component of this parameter can make use of macros allowing the device to make requests for unique provisioning files. This parameter is ignored if the parameter 'Option 66' is enabled.	Empty

The table below describes the various firmware upgrade parameters and provides their default values.

Parameter	Description	Default Value
Enable Upgrading	Enables firmware upgrade operations independently of resync actions	Enable
Upgrade Error Retry Delay	The upgrade retry interval (in seconds) applied in case of upgrade failure. The device has a firmware upgrade error timer that activates after a failed firmware upgrade attempt. The timer is initialized with the value in this parameter. The next firmware upgrade attempt occurs when this timer counts down to zero.	3600 seconds
Upgrade Rule	This parameter sets the URL for the new firmware file. It follows the same syntax as the 'Profile Rule' parameter. e.g. http://192.168.100.1/QX202_v3.1.bin	Empty

Syntax of Profile Rule and Upgrade Rule

The two parameters 'Profile Rule' and 'Upgrade Rule' must follow the following syntax.

[scheme://][server IP or domain[:port]]/file_path

The scheme can be one of the following;

http
https
tftp

The 'file_path' component follows macro expansion rules as described in the section 'Macro Expansion' below.

Examples:

tftp://prov.mydomain.com/cpe/\$MAU.conf
http://dev.easyvoip.com:8080/prov/\$PN/\$MA.conf

Macro Expansion

Macro expansion can be used with the parameters 'Profile Rule' and 'Upgrade Rule'. The table below list the macros variables and to what they expand.

Macro Name	Expansion
\$	The form \$\$ expands to a single \$ character. The form \$\$MAU expands to \$00019F16B1B2. The form \$MAU expands to 00019F16B1B2.
MA	MAC address with lower case hex digits, e.g. 00019F16b1b2.
MAU	MAC address with upper case hex digits, e.g. 00019F16B1B2.
MAC	MAC address with lower case hex digits, and colons to separate hex digit pairs, e.g. 00:01:9F:16:B1:B2.
PN	Product Name, e.g. QX202
SN	Serial Number, e.g. QX2123456
IP	WAN IP address , e.g. 123.45.67.89
SWVER	Software version, e.g. v3.0.1
HWVER	Hardware version, e.g. v1.0.1

Macro variables are invoked by prefixing the macro name with the '\$' character (e.g. \$MAC). Macro substitution works even within a quoted sting, without requiring additional escapes. If the macro is immediately followed by an alphanumeric character, enclose the variable name in parentheses (e.g. '\$(MAC)config.conf').

Please note the following additional points with regards to macro expansion;

- 1) During macro expansion, expressions of the form \$NAME and \$(NAME) are replaced by the contents of the named variables. For example, a router with a MAC address of 00:01:9F:16:B1:B2, the macro \$(MAU)config.cfg expands to 00019F16B1B2config.cfg.
- 2) If the macro name is not recognized, it will remain unexpanded. For example, if you try to use STRANGE as a macro name it will remain unexpanded. Thus the expression \$STRANGE\$MAC.cfg expands to \$STRANGE00:01:9F:16:B1:B2.cfg.
- 3) Macro expansion is not applied recursively. This means that the macro expression \$\$MAU expands to \$MAU and not 00019F16B1B2.
- 4) Macro expressions can have optional qualifiers that allow you specify a substring of the macro variable. The syntax for macro substring expansion is \$(NAME:p) and \$(NAME:p:q) where p and q are non-negative integers. The resulting expansion results in the macro variable substring starting at the character offset p, and of length q (or till end-of-string if q is not specified). So, for our example device with a MAC address of 00019F16B1B2, the expression \$(MAU:4) expands to the string 9F13B1B2, and the expression \$(MAU:8:2) expands to the string B1.

Provisioning

Provision with HTTP

Begin by resetting a ReadyNet router to factory defaults.

- 1) Install an HTTP server on the WAN side of the router.
- 2) In the DocumentRoot of the HTTP server, create a directory named 'prov' for provisioning files. So if the path to the DocumentRoot is /var/www/html, the path to the directory for the provisioning files will be /var/www/html/prov .
In the prov directory, create a file named a.cfg with the following contents and save it.

DBID_SUPER_WEB_PASSWORD=newpass1

- 3) From a PC connected to a LAN port of the device, you should be able to view the file

The screenshot shows the 'Administration' tab of a ReadyNet router's web interface, specifically the 'Provision' sub-tab. Under the 'Configuration Profile' section, various provisioning settings are listed with their current values or states. The 'Profile Rule' field at the bottom is highlighted with a blue border.

Setting	Value
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
Config File Name	VRT210.cfg
User Agent	ReadyNet_VRT210
Profile Rule	http://172.16.8.25/prov/a.cfg

contents of a.cfg by browsing to; http://HTTP_SERVER/prov/a.cfg.

4) Log into the ReadyNet router, navigate to Administration -> Provision and set the 'Option 66' field to Disable and in the Profile Rule field enter: `http://HTTP_SERVER/prov/a.cfg` .

Status	Network	Wireless	SIP Account	Phone	Administration
Management	Firmware Upgrade	Provision	SNMP	TR069	

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
Option 66	Disable
Config File Name	VWRT510.cfg
Profile Rule	<code>http://172.16.8.25/prov/a.cfg</code>

- 5) Click save and then do a reboot.
- 6) When the device boots and its WAN interface is up, it will retrieve the file located at Profile Rule. The ATA will reboot to apply the new parameters.
- 7) When you now login to the web interface with the user 'admin' you will need to enter the password: newpass1.

Provision with DHCP and TFTP

In the example above, we had to manually configure the Profile Rule of the router by logging into the web interface of the device as the admin user and entering a valid location for the provisioning URI. Using DHCP Option 66 together with a TFTP server, the Profile Rule parameter can be automatically set. The ReadyNet router with its default, out-of-the-box configuration is set for 1) DHCP on the WAN interface and 2) Option 66 enabled. A correctly configured DHCP server will provide the IP address of a TFTP server when the router includes a request for Option 66 together with its DHCP request. e.g. if the DHCP server sends back '172.16.8.25' as the Option 66 response and **DBID_PRV_CONFIGFILE** is 'QX202.cfg', the device will make a TFTP request to the server at IP address 172.16.8.25, for a file named 'QX202.cfg'.

- 8) Configure DHCP server to include Option 66 response.
- 9) Configure TFTP server. Create the initial provisioning file named '.cfg' with the following contents.


```
DBID_RESYNC_PERIODIC=60
DBID_PRV_OPTION66_ENABLED=0
DBID_PROFILE_RULE=http://172.16.8.25/prov/\$MAU.conf
```

Note: We change DBID_RESYNC_PERIODIC to 60 seconds only during testing and development.

- 10) In the prov directory of the HTTP server create a file named 00019F16XXXX.conf, replacing XX:XX in the file name to match the WAN MAC address of the router.

```
DBID_SUPER_WEB_PASSWORD=newpass2
```

So if the WAN MAC address is 00:01:9F:16:00:01, the file would be named, '00019F160001.conf'.

- 11) Reset the router to factory defaults. On boot-up, we should expect the following events to occur;
 - a. The ReadyNet router includes Option 66 in its DHCP request on the WAN port.
 - b. The DHCP server includes the Option 66 response with the other DHCP parameters.
 - c. The router makes a TFTP connection to the IP address that it received as the Option 66 value and requests a file named .cfg.
 - d. On receiving the file named '.cfg', the device will set the Option 66 parameter to 'Disable' and set the Profile Rule to '[http://172.16.8.25/prov/\\$MAU.conf](http://172.16.8.25/prov/$MAU.conf)' and do a reboot.
 - e. This time when the device boots up, it will not include Option 66 with its DHCP request. Once the WAN interface is up, the router will expand the macro \$MAU to its WAN MAC address in uppercase. So if the WAN MAC address of the router is 00:01:9F:16:00:01, then the device will request a provisioning file from the URI; <http://172.16.8.25/prov/00019F160001.conf>.
 - f. The request URI uniquely identifies the device allowing the provisioning server to customize the provisioning file returned. In this example we set the password for the user admin to 'newpass2'.
 - g. The device will reboot again.
- 12) When you now log in to the web interface with the user 'admin', you will need to enter the password 'newpass2'.

Provisioning Examples

This section provides example provisioning files for the ReadyNet router. Refer to the Appendix for a listing of the provisioning parameters and their descriptions.

Note 1: The provisioning file only contains the parameters that need changing.

Note 2: The ATA calculates a checksum of the provisioning file. It compares this checksum with the checksum of each new provisioning file it receives. If the checksums are different, the ATA will apply the changes in the new provisioning file and reboot.

Provisioning WAN Parameters

In this example provisioning file, the WAN connection mode is changed from DHCP to STATIC. Further we change, mdns_mode from 0 (Auto) to 1 ('Manual') and define a primary and secondary DNS server that the router itself will use.

```
mwanConnectionMode=STATIC
mwan_ipaddr=172.16.8.60
mwan_netmask=255.255.255.0
mwan_gateway=172.16.8.1
mdns_mode=1
```



```
mwan_primary_dns=8.8.8.8
```

Provisioning LAN Parameters

This remote provisioning example file changes the network parameters on the LAN side of the router. In addition, this file changes the username and passwords of the two administrative access levels of the web interface of the router.

```
lan_ipaddr=192.168.88.1
lan_netmask=255.255.255.0
dhcpGateway=192.168.88.1
dhcpStart=192.168.88.200
dhcpEnd=192.168.88.220
dhcpLease=3600
NormalUser=Alice
DBID_NORMAL_WEB_PASSWORD=Alice123Pass
AdminUser=Jack
DBID_SUPER_WEB_PASSWORD=Jack123pass
```

Provisioning SIP Parameters

This example provisioning file configures the SIP port of the router. You will need to change the actual parameters in the file to match your SIP server.

```
DBID_DNSSRV_DOMAIN=12.34.56.78
DBID_SIP_SERVER_HOST_NAME=12.34.56.79
DBID_SIP_DIS_NAME=Customer Name
DBID_SIP_PHONE_NUM=1234
DBID_SIP_ACCOUNT=1234
DBID_SIP_PASSWORD=SIPpass
```


Appendix B

WAN Network Parameters

Parameter	Valid Values	Description
mwanConnectionMode	DHCP STATIC PPPOE	This parameter defines the WAN connection method. It can be one of the following; Static, DHCP or PPPOE.
mdns_mode	0 1	With the default setting of 0, the device will use the DNS server provided by the DHCP server. Setting this parameter to 1 allows you to define mwan_primary_dns and mwan_secondary_dns manually.
mwan_primary_dns	<i>IP Address</i>	When mdns_mode is set to 1 or mwanConnectionMode is set to Static, this parameter can be defined to set the primary DNS server used by the router.
mwan_secondary_dns	<i>IP Address</i>	When mdns_mode is set to 1 or mwanConnectionMode is set to Static, this parameter can be defined to set the secondary DNS server used by the router.
mwan_ipaddr	<i>IP Address</i>	This parameter sets the WAN IP address and must be set when mwanConnectionMode is set to Static.
mwan_netmask	<i>Netmask</i>	This parameter sets the WAN Netmask and must be set when mwanConnectionMode is set to Static.
mwan_gateway	<i>IP Address</i>	This parameter sets the WAN Netmask and must be set when mwanConnectionMode is set to Static.
mwan_pppoe_user	Empty	This parameter is the PPPoE username and must be defined when mwanConnectionMode is set to PPPoE.
mwan_pppoe_pass	Empty	This parameter is the PPPoE password and must be defined when mwanConnectionMode is set to PPPoE.
mwan_pppoe_opmode	KeepAlive On Demand Manual	This parameter is the PPPoE Operation mode and defaults to KeepAlive.
mwan_pppoe_optime	60	This parameter defines the PPPoE Keep Alive Redial period in seconds when PPPoE is the wanConnectionMode . Range is between 0 - 3600.

LAN Network Parameters

Parameter	Valid Values	Description
natEnabled	NAT Bridge	When in natEnabled is set to NAT, the router operates as a router and when set to Bridge, all network interfaces are bridged.
lan_ipaddr	IP Address	This parameter sets the IP address of the LAN interface when natEnabled is set to NAT. This IP address is also the gateway address for the devices connected to the LAN side of the router.
lan_netmask	<i>Subnet Mask</i>	This parameter sets the subnet mask of the LAN subnet when natEnabled is set to NAT.
dhcpEnabled	Enable Disable	Use this parameter to enable or disable running a DHCP server on the router.
dhcpStart	<i>IP Address</i>	If dhcpEnabled is set to Enable, this parameter sets the starting IP address of the DHCP pool.
dhcpGateway	<i>IP Address</i>	dhcpGateway defines the gateway address for DHCP requests from the LAN network.
dhcpEnd	<i>IP Address</i>	If dhcpEnabled is set to Enable, this parameter sets the ending IP address of the DHCP pool.
dhcpDnsMode	Auto Manual	When this parameter is set to Auto, DHCP clients are assigned the
dhcpPriDns		When dhcpDnsMode is set to Manual, this parameter defines the IP address of DNS server that will be provided as the primary DNS server with DHCP requests.
dhcpSecDns		When dhcpDnsMode is set to Manual, this parameter defines the IP address of DNS server that will be provided as the secondary DNS server with DHCP requests.
dhcpLease	86400	This parameter defines the DHCP lease time.
lan_vid	1	This parameter defines the VLAN ID of the LAN port. VLAN IDs are defined under Network -> VLAN in the web interface.

SIP Parameters

These parameters configure the SIP settings and correspond to the settings seen on the 'SIP Account' menu of the web interface.

Parameter	Description
DBID_DNSSRV_DOMAIN	This parameter defines the 'Proxy Server' for the SIP account.
DBID_SIP_OUTBOUND_PORT	This parameter defines the 'Proxy Port'. The default port is 5060.
DBID_SIP_SERVER_HOST_NAME	This parameter defines the 'Outbound Server' for the SIP account.
DBID_SIP_SERVER_PORT	This parameter defines the 'Outbound Port'. Default value is 5060.
DBID_ALTER_SIP_SERVER_HOSTNAME	This parameter defines the 'Backup Outbound Server' for the SIP account.
DBID_ALTER_SIP_SERVER_PORT	This parameter defines the 'Backup Outbound Port'. The default port is 5060.
DBID_SIP_DIS_NAME	This parameter defines the 'Display name' for the SIP account.
DBID_SIP_PHONE_NUM	This parameter defines the 'Phone Number' for the SIP account.
DBID_SIP_ACCOUNT	This parameter defines the 'Account' attribute associated with the SIP account.
DBID_SIP_PASSWORD	This parameter defines the 'Password' assigned to the particular SIP account.
DBID_SIP_TOS	This parameter sets the DHCP mark for Layer 3 QoS for SIP packets. Range is 0 through 63.
DBID_RTP_TOS	This parameter sets the DHCP mark for Layer 3 QoS for RTP packets. Range is 0 through 63.
DBID_DATA_TOS	This parameter sets the DHCP mark for Layer 3 QoS for Data packets. Range is 0 through 63.
sip_vid	This parameter defines the VLAN ID over which SIP packets will be sent. VLAN IDs are defined under Network -> VLAN in the web interface. The default is 2.
rtp_vid	This parameter defines the VLAN ID over which RTP packets will be sent. VLAN IDs are defined under Network -> VLAN in the web interface. The default is 2.

Administration Parameters

Parameter		Description
BasicUser	useradmin	This parameter defines a web login username of type 'Basic'.
BasicPass	admin	This parameter defines the password for BasicUser .
NormalUser	user	This parameter defines a web login username of type 'Normal'.
DBID_NORMAL_WEB_PASSWORD	user	This parameter defines the password for NormalUser.
AdminUser	admin	This parameter defines a web login username of type 'Admin'.
DBID_SUPER_WEB_PASSWORD	admin	This parameter defines the password for AdminUser.
DBID_LAN_LOGIN_ONLY	0	The default for this parameter is 0 which allows access to the web interface of the device from the WAN interface. To only allow access to the web interface set this parameter to 1.
DBID_WEB_PORT	80	This parameter set the port that web server on the device listens to requests on both the LAN side and WAN (if DBI_LAN_LOGIN_ONLY =0) side.
DBID_WEB_IDLE_TIMEOUT	5	Whilst logged into the web interface of the device this parameter sets the value in minutes of inactivity that results in getting logged out.

Provisioning Parameters

Parameter	Default	Description
DBID_PROVISION_ENABLED	1 0	The default value for this parameter is 1 which enables provisioning for the device.
DBID_RESYNC_ON_RESET	1 0	The default value for this parameter is 1 which triggers a resync after every reboot except for reboot caused by parameter updates and firmware upgrade.
DBID_RANDOM_DELAY	40	This parameter defines the maximum number of seconds the device waits before making its initial contact with the provisioning server. This delay is effective only on the initial configuration attempt following device power-on or reset. The delay is a pseudo-random number between zero and this value. The default value is 40 and setting this parameter to 0, disables this feature.
DBID_RESYNC_PERIODIC	3600	This parameter is used to define the number of seconds between periodic resyncs with the provisioning server. Set this parameter to zero to disable periodic resyncing.
DBID_RESYNC_RETRY_DELAY	3600	This parameter defines the number of seconds the device will wait to retry a resync after the last attempt to resync failed.
DBID_RESYNC_DELAY	14400	This is the starting value of a counter in seconds that is decremented when all its line become idle. Resync events are delayed until this counter decrements to zero.
DBID_RESYNC_AFTER_UPGRADE	1 0	When set to 1, the device will trigger a resync after every firmware upgrade attempt. Set this parameter to disable.
DBID_PRV_OPTION66_ENABLED	1 0	When this parameter is set to 1 (default), the device will include DHCP Option 66 with its DHCP request. When enabled, the parameter DBID_PROFILE_RULE is ignored.
DBID_PRV_CONFIGFILE	.cfg	This is the name of the provisioning file retrieved from the TFTP server when DHCP Option 66 is enabled.
DBID_PROFILE_RULE		This parameter sets the URI that the device will retrieve its provisioning file from. This parameter is ignored when DBID_PRV_OPTION66_ENABLED is set to 0.
DBID_UPGRADE_ENABLED	1 0	The default value for this parameter is 1, which enables firmware upgrades. Set to 0 to disable this function.
DBID_UPGRADE_RETRY_DELAY	3600	On a firmware upgrade failure this parameter is set to the value defined in seconds and a countdown begins. Once the timer reaches zero, the next attempt at firmware upgrade will occur.
DBID_UPGRADE_RULE		This parameter sets the URI from which the new firmware file is requested from.

Default Provisioning Template File

```
mwanConnectionMode=DHCP
dhcpDnsMode=Auto
mwan_primary_dns=
mwan_secondary_dns=
mwan_ipaddr=
mwan_netmask=
wan_gateway=
wan_pppoe_user=
wan_pppoe_pass=
wan_pppoe_opmode=KeepAlive
wan_pppoeoptime=5
wan_vid=2
natEnabled=1
lan_ipaddr=192.168.11.1
lan_netmask=255.255.255.0
dhcpEnabled=1
dhcpStart=192.168.11.2
dhcpEnd=192.168.11.24
dhcpGateway=192.168.11.1
dhcpDnsMode=Auto
dhcpPriDns=192.168.11.1
dhcpSecDns=8.8.8.8
dhcpLease=86400
lan_vid=1
DBID_DNSSRV_DOMAIN=
DBID_SIP_OUTBOUND_PORT=5060
DBID_SIP_SERVER_HOST_NAME=
DBID_SIP_SERVER_PORT=5060
DBID_ALTER_SIP_SERVER_HOSTNAME=
DBID_ALTER_SIP_SERVER_PORT=5060
DBID_SIP_DIS_NAME=
DBID_SIP_PHONE_NUM=
DBID_SIP_ACCOUNT=
DBID_SIP_PASSWORD=
DBID_SIP_TOS=0
DBID_RTP_TOS=0
DBID_DATA_TOS=0
sip_vid=2
rtp_vid=2
DBID_PROVISION_ENABLED=1
DBID_RESYNC_ON_RESET=1
DBID_RANDOM_DELAY=40
```


DBID_RESYNC_PERIODIC=3600
DBID_RESYNC_RETRY_DELAY=3600
DBID_RESYNC_DELAY=14400
DBID_RESYNC_AFTER_UPGRADE=1
DBID_PRV_OPTION66_ENABLED=1
DBID_PRV_CONFIGFILE=QX202.cfg
DBID_PROFILE_RULE=
DBID_UPGRADE_ENABLED=0
DBID_UPGRADE_RETRY_DELAY=3600
DBID_UPGRADE_RULE=