cnPilot Home & Small Business Wireless Router User Guide

System Release V4.00

For: R200x and R201x models

Cambium Networks™

Accuracy

While reasonable efforts have been made to assure the accuracy of this document, Cambium Networks assumes no liability resulting from any inaccuracies or omissions in this document, or from use of the information obtained herein. Cambium reserves the right to make changes to any products described herein to improve reliability, function, or design, and reserves the right to revise this document and to make changes from time to time in content hereof with no obligation to notify any person of revisions or changes. Cambium does not assume any liability arising out of the application or use of any product, software, or circuit described herein; neither does it convey license under its patent rights or the rights of others. It is possible that this publication may contain references to, or information about Cambium products (machines and programs), programming, or services that are not announced in your country. Such references or information must not be construed to mean that Cambium intends to announce such Cambium products, programming, or services in your country.

Copyrights

This document, Cambium products, and 3rd Party Software products described in this document may include or describe copyrighted Cambium and other 3rd Party supplied computer programs stored in semiconductor memories or other media. Laws in the United States and other countries preserve for Cambium, its licensors, and other 3rd Party supplied software certain exclusive rights for copyrighted material, including the exclusive right to copy, reproduce in any form, distribute and make derivative works of the copyrighted material. Accordingly, any copyrighted material of Cambium, its licensors, or the 3rd Party software supplied material contained in the Cambium products described in this document may not be copied, reproduced, reverse engineered, distributed, merged or modified in any manner without the express written permission of Cambium. Furthermore, the purchase of Cambium products shall not be deemed to grant either directly or by implication, estoppel, or otherwise, any license under the copyrights, patents or patent applications of Cambium or other 3rd Party supplied software, except for the normal non-exclusive, royalty free license to use that arises by operation of law in the sale of a product.

Restrictions

Software and documentation are copyrighted materials. Making unauthorized copies is prohibited by law. No part of the software or documentation may be reproduced, transmitted, transcribed, stored in a retrieval system, or translated into any language or computer language, in any form or by any means, without prior written permission of Cambium.

License Agreements

The software described in this document is the property of Cambium and its licensors. It is furnished by express license agreement only and may be used only in accordance with the terms of such an agreement.

High Risk Materials

Components, units, or 3rd Party products used in the product described herein are NOT fault-tolerant and are NOT designed, manufactured, or intended for use as on-line control equipment in the following hazardous environments requiring fail-safe controls: the operation of Nuclear Facilities, Aircraft Navigation or Aircraft Communication Systems, Air Traffic Control, Life Support, or Weapons Systems (High Risk Activities). Cambium and its supplier(s) specifically disclaim any expressed or implied warranty of fitness for such High Risk Activities.

Warnings, cautions and notes

The following describes how warnings and cautions are used in this document and in all documents of the Cambium Networks document set.

Warnings

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

⚠	***Warning*** *Warning text and the consequence of not following the provided instructions.*

Cautions

Cautions precede instructions and are used when there is a possibility of damage to systems, software, or individual items of equipment within a system. However, this damage presents no danger to personnel. A caution has the following format:

⚠	***Caution*** *Caution text and consequence for not following the instructions in the caution.*

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:

📌	***Note*** *Note text*

Contents

List of Figures

List of Tables

About This User Guide

Thank you for choosing Cambium cnPilot Home & Small Business WiFi router with ATA and optional PoE support.

This manual provides basic information about how to install and deploy the cnPilot Home R200x or the R201x WiFi routers with VoIP to the Internet.

For remote configuration and deployment, an IP connection is required.

The cnPilot Home & Small Business router with VoIP is a managed device (that yet has the ability to act as a stand-alone router if desired). In addition to WiFi, this product provides high quality voice calls as well as the optional ability to power Cambium's ePMP series subscriber module or the PMP450 series subscriber module by supporting Cambium's (Canopy) PoE. For voice calls, the product is fully compatible with the SIP industry standard and is able to interoperate with many other SIP devices and software on the market.

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.

GNU GPL Information

cnPilot Home R200x/R201x 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.

Contacting Cambium Networks

Support website	http://www.cambiumnetworks.com/support/
Cambium main website	http://www.cambiumnetworks.com/
Sales enquiries	sales@cambiumnetworks.com
Email support	support@cambiumnetworks.com
Telephone numbers	For full list of Cambium support telephone numbers, see: http://www.cambiumnetworks.com/support/contact-support
Address	Cambium Networks 3800 Golf Road, Suite 360 Rolling Meadows, IL 60008

Chapter 1: Overview

This chapter covers:

- Accessing and Configuring cnPilot Devices via cnMaestro
- Accessing and Configuring cnPilot Devices via the local GUI (without cnMaestro)
- cnPilot Home R200x/R201x
- cnPilot Home R200x LED Indicators and Interfaces
- cnPilot Home R201x LED Indicators and Interfaces
- Hardware Installation
- Voice Prompt

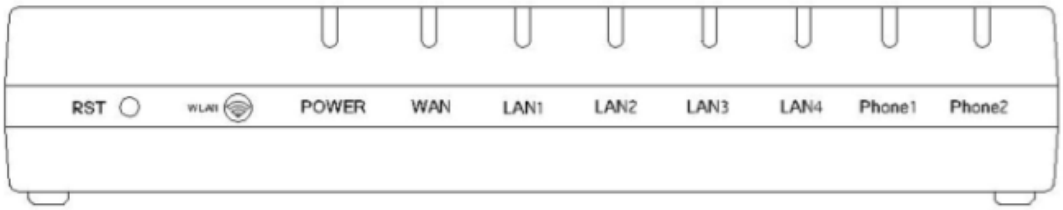
cnPilot Home R200x/R201x

Table 1 Key Features at-a-glance

Port / Interface	cnPilot Home R200	cnPilot Home R200P	cnPilot Home R201	cnPilot Home R201P	cnPilot Home R201W
WAN	1xFE in RJ45		1xGE in RJ45		
LAN	4xFE in RJ45		4xGE in RJ45		
Wi-Fi	2X2 2.4GHz 802.11 b/g/n		2X2 2.4GHz 802.11 b/g/n (300 Mbps)		
	No		2X2 5GHz 802.11ac (867 Mbps)		
USB	1X USB 2.0		1X USB 2.0		
VoIP	2xFXS in RJ11		2xFXS in RJ11		No
Cambium PoE (Power over Ethernet) Out	No	Yes	No	Yes	Yes
Power Adapter	12V/2A	12V/3A	12V/2A	12V/3A	12V/3A
cnMaestro Managed	Yes	Yes	Yes	Yes	Yes

cnPilot Home R200x LED Indicators and Interfaces

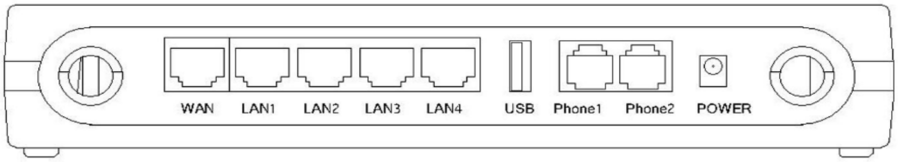
Table 2 cnPilot Home R200x LED Indicators



Front Panel

LED	Status	Explanation
Phone1/2	Blinking (Green)	Not registered
	On (Green)	Registered
LAN 1/2/3/4	On (Green)	Port is connected at 100Mbps
	Off	The port is disconnected
	Blinking (Green)	Transmitting data
WAN	On (Green)	Port is connected with 100Mbps
	Off	The port is disconnected
	Blinking (Green)	Blinks while transmitting data
POWER	On (Green)	The router is powered on and running normally
	Off	The router is powered off
WLAN	On (Green)	Wireless access point is ready
	Blinking (Green)	Blinks while wireless traffic goes through

Table 3 cnPilot Home R200x Interfaces

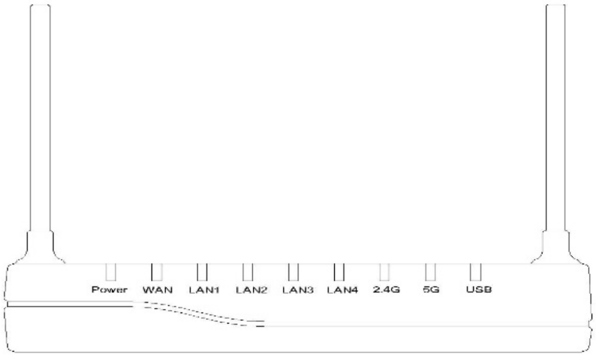


Rear Panel

Interface	Description
POWER	Connector for a power adapter
Phone1/2	ATA Analog phone connector
USB	USB interface
WAN	Connector for accessing the Internet
LAN (1/2/3/4)	Connectors for local networked devices

cnPilot Home R201x LED Indicators and Interfaces

Table 4 cnPilot Home R201x LED Indicators



LED	Status	Explanation
USB	On (Green)	Connected
	Off	Disconnected
2.4G/5G LAN 1/2/3/4	On (Green)	Wireless access point is ready
	Blinking (Green)	The port is passing data
	On (Green)	The port is connected at 100Mbps
	Off	The port is disconnected
WAN	Blinking (Green)	The data is transmitting
	On (Green)	The port is connected at 100Mbps
	Off	The port is disconnected
	Blinking(Green)	The port is transmitting data
POWER	On(Green)	Router is powered on and running normally
	Off	The router is powered off

Table 5 cnPilot Home R201x Interfaces

Interface	Description
ON/OFF	Power Switch
POWER	Connector for a power adapter
USB	USB interface
LAN (1/2/3/4)	Connectors for local networked devices
WAN	Connector for accessing the Internet

Hardware Installation and Setup via cnMaestro

Before configuring your router, please see the procedure below for instructions on connecting the cnPilot Home 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 via your network’s modem/switch/router/ADSL equipment using an Ethernet cable.
3. Connect one end of the power cord to the power port of the device. Connect the other end to the wall outlet.
4. Push the ON/OFF button to power on the router.
5. Check the Power, WAN, and LAN LEDs to confirm network connectivity.
6. The cnPilot R200x/R201x device will not power up and attempt to register with cnMaestro. For further setup instructions please see section Accessing and Configuring cnPilot Devices via cnMaestro

Warning

Please do not attempt to use unsupported power adapters and do not remove power during configuring or updating the cnPilot Home R200x/R201x device. Using other power adapters may damage the cnPilot Home R200x/R201x 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 energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Accessing and Configuring cnPilot Devices via cnMaestro

cnMaestro, Cambium's next generation network management system is the recommended method for managing Cambium's cnPilot access points. As Cambium develops new features, you may find the latest information on operating these features at the Cambium Community Forum.

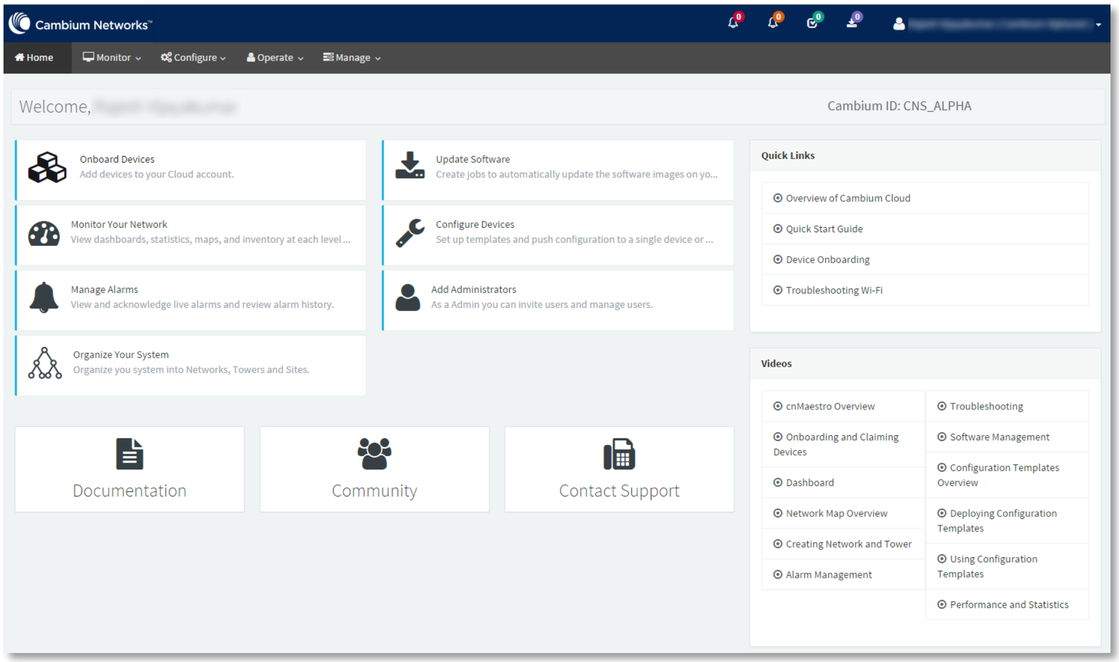
Register at Cambium's support forum (http://community.cambiumnetworks.com/) for instructions, discussions, and helpful tips on managing cnPilot access points.

Accessing cnMaestro and Beginning Setup/Configuration

To access cnMaestro:

Procedure 2 Accessing cnMaestro

1. Log in to the cnMaestro website (https://cloud.cambiumnetworks.com)
2. Begin setup, including details of your company's its managing accounts
3. Upon successfully registering and claiming the cnPilot access point(s), you may configure and manage cnPilot devices online via cnMaestro (https://cloud.cambiumnetworks.com).



Welcome, [redacted]

Cambium ID: CNS_ALPHA

Onboard Devices
Add devices to your Cloud account.

Update Software
Create jobs to automatically update the software images on yo...

Monitor Your Network
View dashboards, statistics, maps, and inventory at each level ...

Configure Devices
Set up templates and push configuration to a single device or ...

Manage Alarms
View and acknowledge live alarms and review alarm history.

Add Administrators
As a Admin you can invite users and manage users.

Organize Your System
Organize you system into Networks, Towers and Sites.

Quick Links

- Overview of Cambium Cloud
- Quick Start Guide
- Device Onboarding
- Troubleshooting Wi-Fi

Videos

- cnMaestro Overview
- Onboarding and Claiming Devices
- Dashboard
- Network Map Overview
- Creating Network and Tower
- Alarm Management
- Troubleshooting
- Software Management
- Configuration Templates Overview
- Deploying Configuration Templates
- Using Configuration Templates
- Performance and Statistics

Configuration template files (to enable rapid configuration setup) are available to help get started quickly with cnMaestro at (http://community.cambiumnetworks.com). After loading these configuration files, you may override configuration parameter values and manage software setup via cnMaestro.

Accessing and Configuring cnPilot Devices via the local GUI (without cnMaestro)

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

Procedure 3 Configuring the Router

1. Connect analog phone to ATA Port with an RJ11 cable.
2. Connect the WAN port to the Internet via your network's modem/switch/router/ADSL equipment using an Ethernet cable.
3. If desired, connect one of 4 available LAN ports to your PC or networked device with an Ethernet cable. cnPilot Home devices allow you to connect up to 4 PCs (or other Ethernet-connected devices) directly.
4. Connect one end of the power cord to the power port of the device. Connect the other end to the wall outlet.
5. Push the ON/OFF button to power on the router.
6. Check the Power, WAN, and LAN LEDs to confirm network connectivity.

Warning

Please do not attempt to use unsupported power adapters and do not remove power during configuring or updating the cnPilot Home R200x/R201x device. Using other power adapters may damage the cnPilot Home R200x/R201x 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 energy and, if not installed and used in accordance with the instructions, may cause harmful interference to radio communications. However, there is no guarantee that interference will not occur in a particular installation.

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

Reorient or relocate the receiving antenna.

Increase the separation between the equipment and receiver.

Connect the equipment into an outlet on a circuit different from that to which the receiver is connected.

Consult the dealer or an experienced radio/TV technician for help.

Voice Prompt

cnPilot Home 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 6 Voice Menu Setting Options

Operation code	Menu Navigation
1 WAN Port Connection Type	1. Pick up phone and press "****" to start IVR 2. Choose "1", and cnPilot Home R200x/R201x 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 cnPilot Home device returns to the prompt "please enter your option ..." 6. To quit, enter "*"
2 WAN Port IP Address	1. Pick up phone and press "****" to start IVR 2. Choose "2", and cnPilot Home R200x /R201x reports current WAN Port IP Address 3. Input the new WAN port IP address and press "#" key: Use "*" to replace ".", for exampleuser can input 192*168*20*168 to set the new IP address 192.168.20.168 4. Press # key to indicate that you have finished Report "operation successful" if user operation is ok. 5. To quit, enter "**".
3 WAN Port Subnet Mask	1. Pick up phone and press "****" to start IVR 2. Choose "3", and cnPilot Home R200x /R201x reports current WAN port subnet mask 3. Input a new WAN port subnet mask and press # key: Use "*" to replace ".", user can input 255*255*255*0 to set the new WAN port subnet mask 255.255.255.0 4. Press "#" key to indicate that you have finished Report "operation successful" if user operation is ok. 5. To quit, enter "**".

4 Gateway	1. Pick up phone and press “****” to start IVR 2. Choose “4”, and cnPilot Home R200x/R201x reports current gateway 3. Input the new gateway and press “#” key: Use “*” to replace “.”, user can input 192*168*20*1 to set the new gateway 192.168.20.1. 4. Press “#” key to indicate that you have finished. Report “operation successful” if user operation is ok. 5. To quit, press “**”.
5 DNS	1. Pick up phone and press “****” to start IVR 2. Choose “5”, and cnPilot Home R200x /R201x reports current DNS 3. Input the new DNS and press # key: Use “*” to replace “.”, user can input 192*168*20*1 to set the new gateway 192.168.20.1. 4. Press “#” key to indicate that you have finished. Report “operation successful” if user operation is ok. 5. If you want to quit , press “**”.
6 Factory Reset	1. Pick up phone and press “****” to start IVR 2. Choose “6”, and cnPilot Home R200x /R201x 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 “*”. Prompt “operation successful” if password is right and then cnPilot Home R200x/R201x will be in factory default configuration. 5. Press “7” reboot to make changes effective.
7 Reboot	1. Pick up phone and press “****” to start IVR 2. Choose “7”, and cnPilot Home R200x/R201x reports “Reboot” 3. Prompt "Please enter password", the method of inputting password is same as operation 1. 4. cnPilot Home R200x/R201x reboots if password is right and operation is ok.
8 WAN Port Login	1. Pick up phone and press “****” to start IVR 2. Choose “8”, and cnPilot Home R200x/R201x 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 “*”. 5. Report “operation successful” if user operation is ok.
9 WEB Access Port	1. Pick up phone and press “****” to start IVR 2. Choose “9”, and cnPilot Home R200x /R201x reports “ WEB Access Port” 3. Prompt “Please enter password”, the method of inputting password is same as operation 1. Report “operation successful” if user operation is ok. 4. Report the current WEB Access Port 5. Set the new WEB access port and press “#” key. 6. Report “operation successful” if user operation is successful.

0 Firmware Version	1. Pick up phone and press “****” to start IVR 2. Choose “0” and CnPilot Home R200x/R201x reports the current Firmware version

Note

While using Voice menu, press * (star) to return to main menu.

If any changes made in the IP assignment mode, the router must be rebooted in order for the settings to take effect.

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

> *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.*

Use the # (hash) key to indicate that you have finish entering the IP address or subnet mask

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 cnPilot Home R200x/R201x is connected.

The default LAN port IP address of cnPilot Home R200x/R201x is 192.168.11.1 and this address should not be assigned to the WAN port IP address of cnPilot Home R200x/R201x in the same network segment of LAN port.

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’,*
>
> *E.g. password is ‘admin-admin’, press ‘236460263’*

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.

cnPilot Home R200x/R201x supports two-level management: administrator and user. For administrator mode operation, please type "admin/admin" on Username/Password and click Login button to begin configuration. For user mode operation, please type "user/user" on Username/Password and click Login button to begin configuration.

Web Management Interface

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

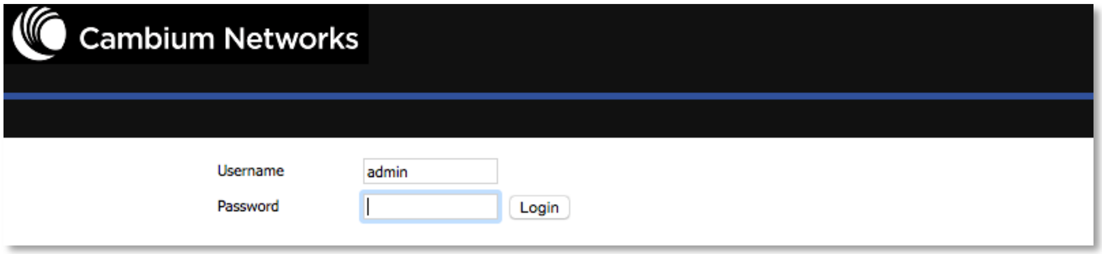
Logging in from the LAN port

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 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.

Figure 1 Login Prompt – LAN Port



Username admin

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 Troubleshooting Guide for more information.

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

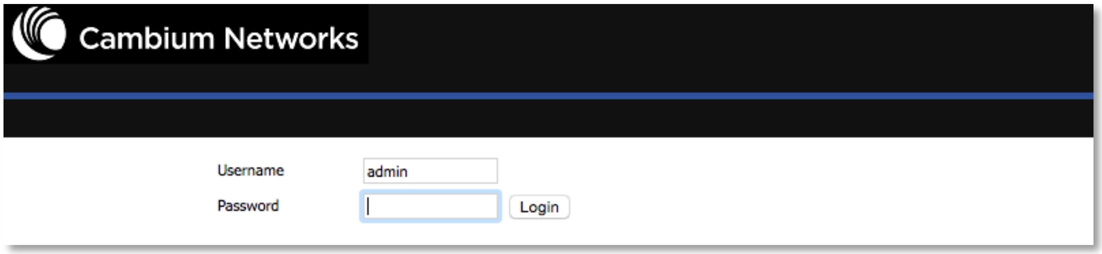
Logging in from the WAN port

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.

Figure 2 Login Prompt – WAN Port



Username admin

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.

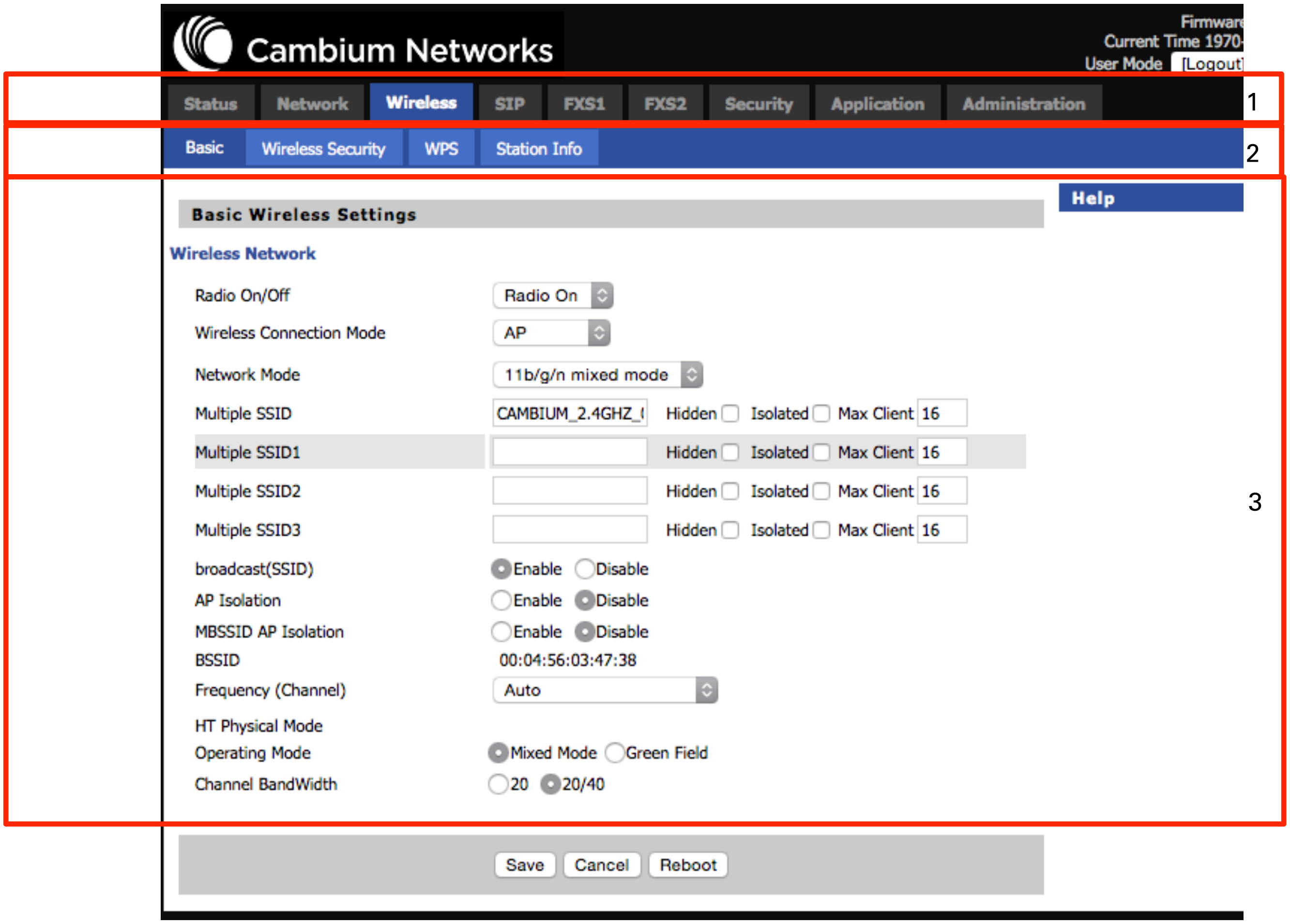
Note

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

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

Web Management Interface Details

Table 7 Web management interface



Basic Wireless Settings

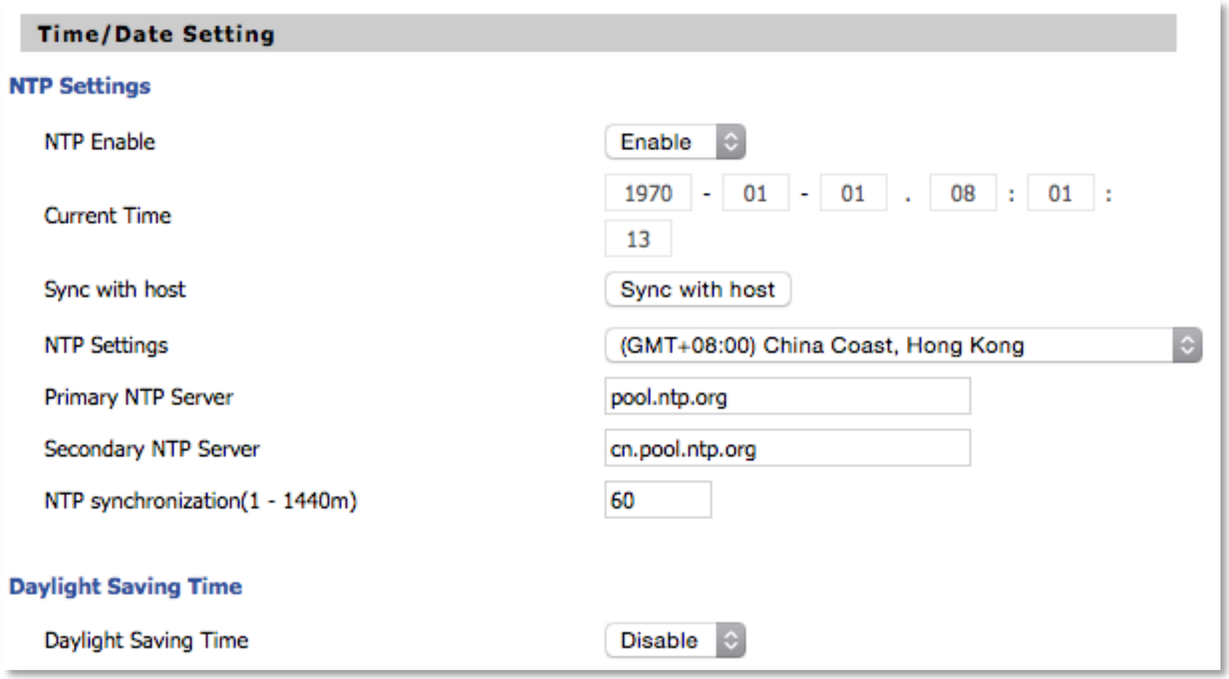
Wireless Network

Radio On/Off	Radio On
Wireless Connection Mode	AP
Network Mode	11b/g/n mixed mode
Multiple SSID	CAMBIUM_2.4GHZ_(Hidden □ Isolated □ Max Client 16
Multiple SSID1	Hidden □ Isolated □ Max Client 16
Multiple SSID2	Hidden □ Isolated □ Max Client 16
Multiple SSID3	Hidden □ Isolated □ Max Client 16
broadcast(SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	00:04:56:03:47:38
Frequency (Channel)	Auto
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40

Field Name	Description
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")
Save	1. Any time changes are made click "Save" to confirm and save the changes. 2. On click of "Save" button, a red message will be displayed as shown below to notify a reboot. Please REBOOT to make the changes effective!
Cancel	To cancel the changes.

Setting the Time Zone

Table 8 Setting time zone



Time/Date Setting

NTP Settings

NTP Enable	Enable
Current Time	1970 - 01 - 01 . 08 : 01 : 13
Sync with host	Sync with host
NTP Settings	(GMT+08:00) China Coast, Hong Kong
Primary NTP Server	pool.ntp.org
Secondary NTP Server	cn.pool.ntp.org
NTP synchronization(1 - 1440m)	60

Daylight Saving Time

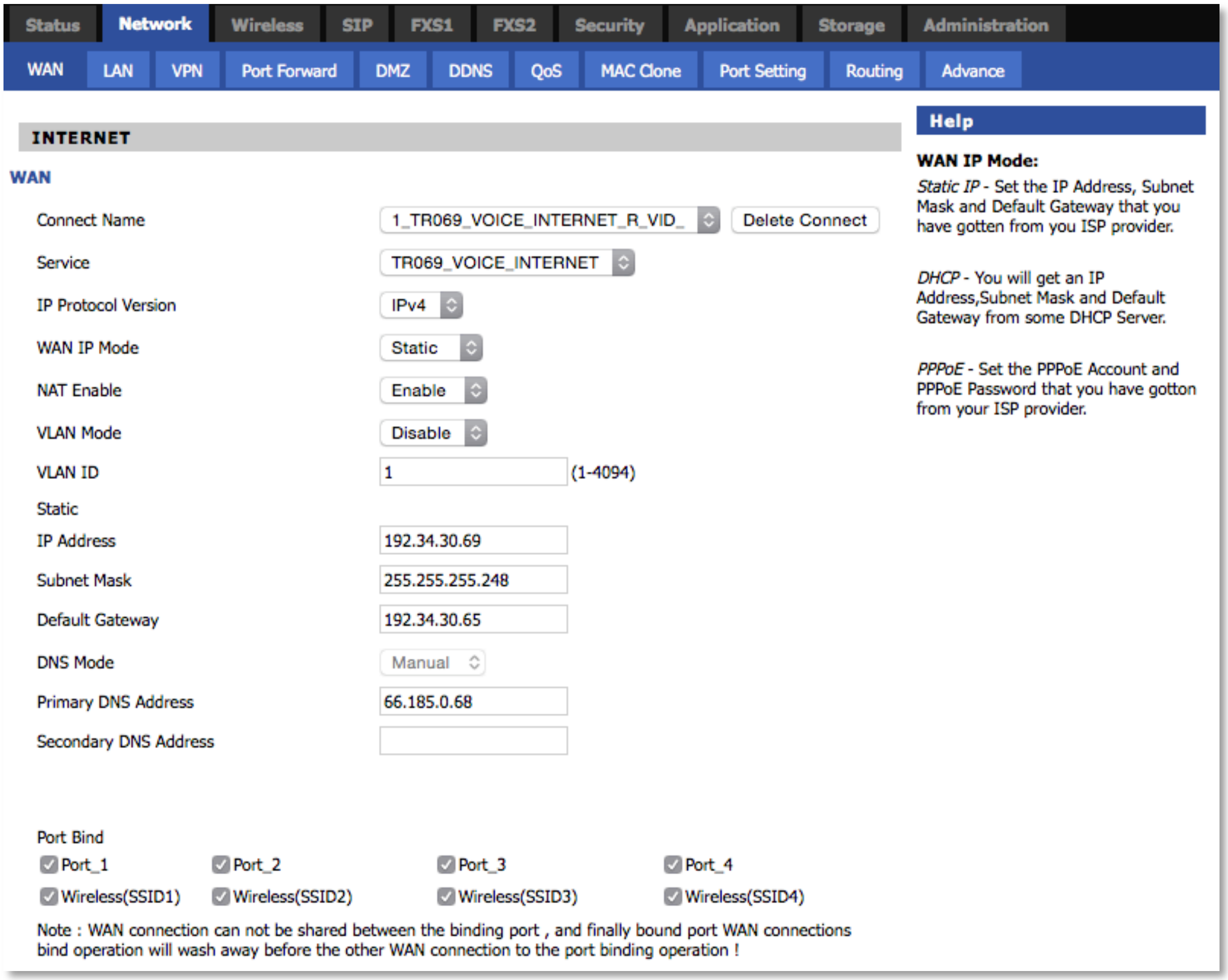
Daylight Saving Time	Disable

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 Sync with host 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 9* below.

Table 9 Configuring an internet connection



INTERNET

WAN

Connect Name	1_TR069_VOICE_INTERNET_R_VID_
Service	TR069_VOICE_INTERNET
IP Protocol Version	IPv4
WAN IP Mode	Static
NAT Enable	Enable
VLAN Mode	Disable
VLAN ID	1 (1-4094)
Static	
IP Address	192.34.30.69
Subnet Mask	255.255.255.248
Default Gateway	192.34.30.65
DNS Mode	Manual
Primary DNS Address	66.185.0.68
Secondary DNS Address	

Port Bind

☑ Port_1	☑ Port_2	☑ Port_3	☑ Port_4
☑ Wireless(SSID1)	☑ Wireless(SSID2)	☑ Wireless(SSID3)	☑ Wireless(SSID4)

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 you ISP provider.

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

PPPoE - Set the PPPoE Account and PPPoE Password that you have gotton 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	Chose the service mode for the created connection
IP Protocol Version	IPv4 supported
WAN IP Mode	Choose Internet connection mode, DHCP, PPPoE, or Bridge
NAT Enable	Enable or disable NAT
VLAN ID	Set VLAN ID
DNS Mode	Select DNS mode, options are Auto and Manual: 1. When DNS mode is Auto, the device under LAN port will

	automatically obtains the preferred DNS and alternate DNS. 2. When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS
Primary DNS	Enter the preferred DNS address
Secondary DNS	Enter the secondary DNS address
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

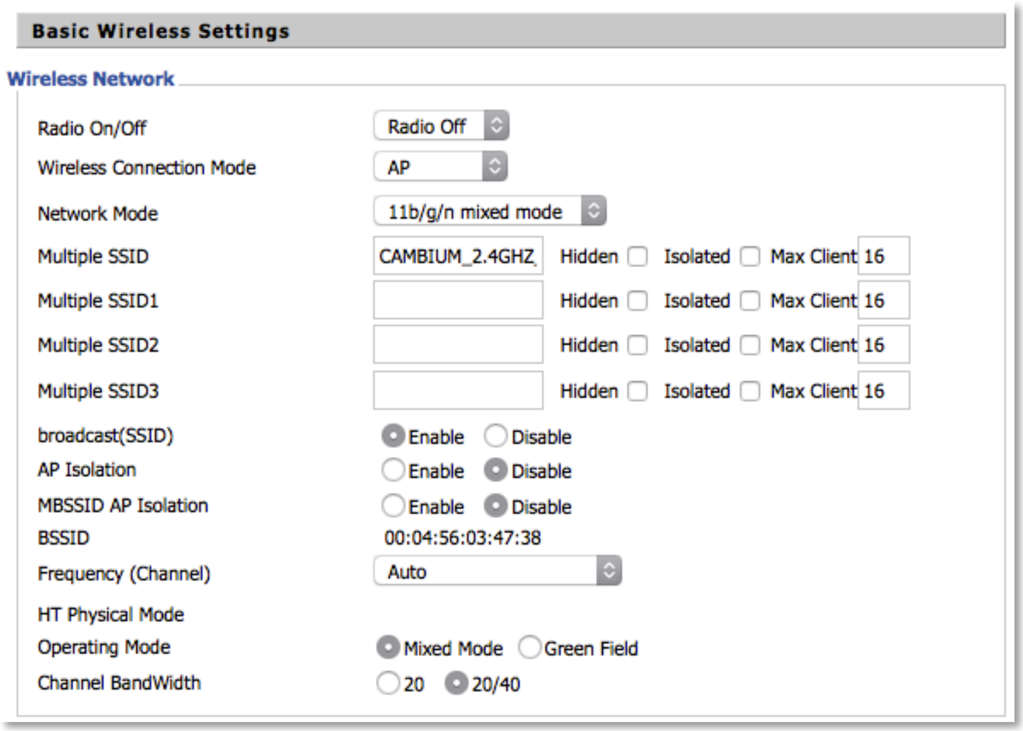
Setting up Wireless Connections

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

Enable Wireless and Setting SSID

Open Wireless > Basic webpage as shown below:

Table 10 Wireless > Basic web page (user view)



Basic Wireless Settings

Wireless Network

Radio On/Off: Radio Off

Wireless Connection Mode: AP

Network Mode: 11b/g/n mixed mode

Multiple SSID: CAMBIUM_2.4GHZ Hidden ☐ Isolated ☐ Max Client 16

Multiple SSID1: Hidden ☐ Isolated ☐ Max Client 16

Multiple SSID2: Hidden ☐ Isolated ☐ Max Client 16

Multiple SSID3: Hidden ☐ Isolated ☐ Max Client 16

broadcast(SSID): ● Enable ○ Disable

AP Isolation: ○ Enable ● Disable

MBSSID AP Isolation: ○ Enable ● Disable

BSSID: 00:04:56:03:47:38

Frequency (Channel): Auto

HT Physical Mode

Operating Mode: ● Mixed Mode ○ Green Field

Channel BandWidth: ○ 20 ● 20/40

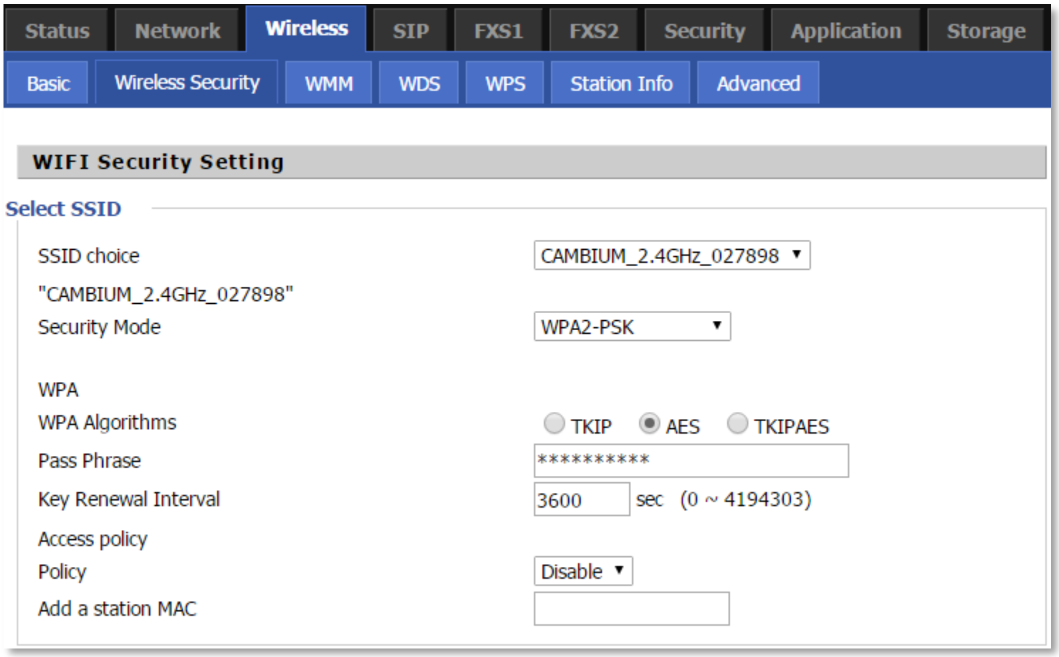
Field Name	Description
Radio On/Off	Select "Radio Off" to disable wireless operation Select "Radio on" to enable wireless operation *Please note: "Save" required for this parameter change*
Network Mode	Choose one network mode from the drop down list.
SSID	The logical name of the wireless connection (text, 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 regulatr intervals, disallowing wi-fi clients from automatically connecting to the cnPilot
AP Isolation	**Enabled**: Devices connected to the router are isolated from one

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

Encryption

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

Table 11 Wireless Security web page



WIFI Security Setting

Select SSID

SSID choice	CAMBIUM_2.4GHz_027898 ▼
"CAMBIUM_2.4GHz_027898"	
Security Mode	WPA2-PSK ▼
WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	**********
Key Renewal Interval	3600 sec (0 ~ 4194303)
Access policy	
Policy	Disable ▼
Add a station MAC	

Field Name	Description
SSID Choice	Choose the SSID from the drop-drown list for which security will be configured
Security Mode	Select an appropriate encryption mode to improve the security and privacy of your wireless data packets. Each encryption mode will launch an additional web page and ask you to offer additional configuration. For high security, the device can be configured for Security Mode as WPA2-PSK and WPA Algorithms as AES.
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	**Disable:** Access policy rules are not enforced **Allow:** Only allow the clients in the station MAC list to access **Rejected:** Block the clients in the station MAC list from registering
Add a Station MAC	Enter the MAC address of the clients which you want to allow or reject

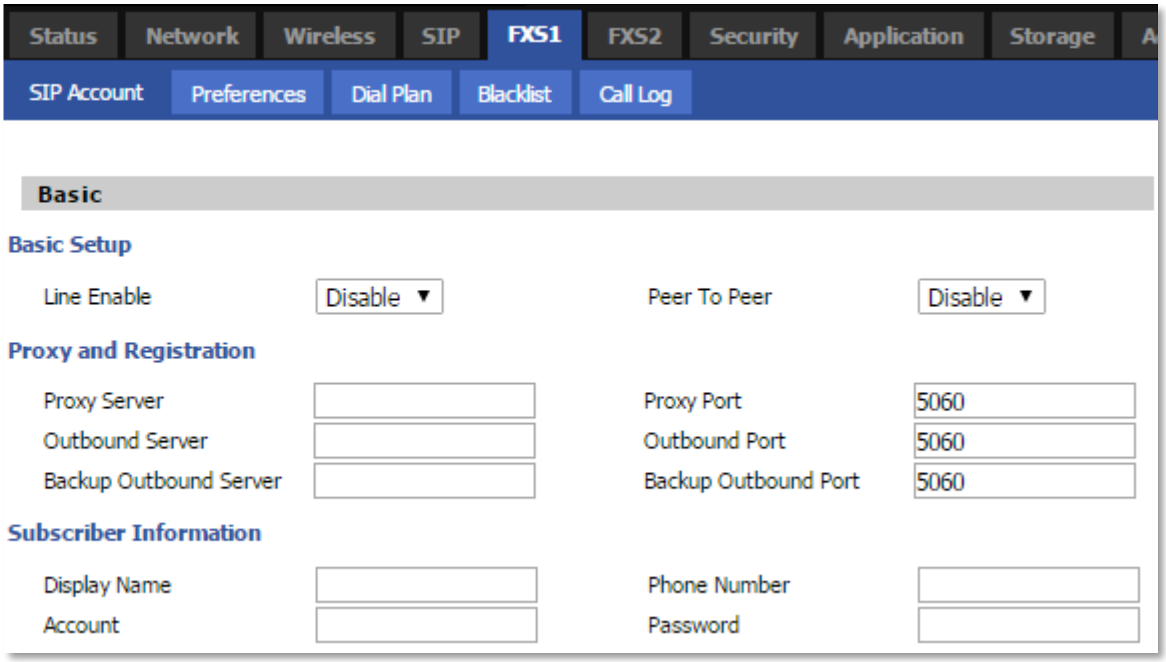
Configuring Session Initiation Protocol (SIP)

SIP Accounts

cnPilot Home devices have 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 12 Configuring SIP via the Web Management Interface



Basic

Basic Setup

Line Enable	Disable ▼	Peer To Peer	Disable ▼

Proxy and Registration

Proxy Server		Proxy Port	5060
Outbound Server		Outbound Port	5060
Backup Outbound Server		Backup Outbound Port	5060

Subscriber Information

Display Name		Phone Number	
Account		Password	

Procedure

1. Open the **FXS1 (FXS2)/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

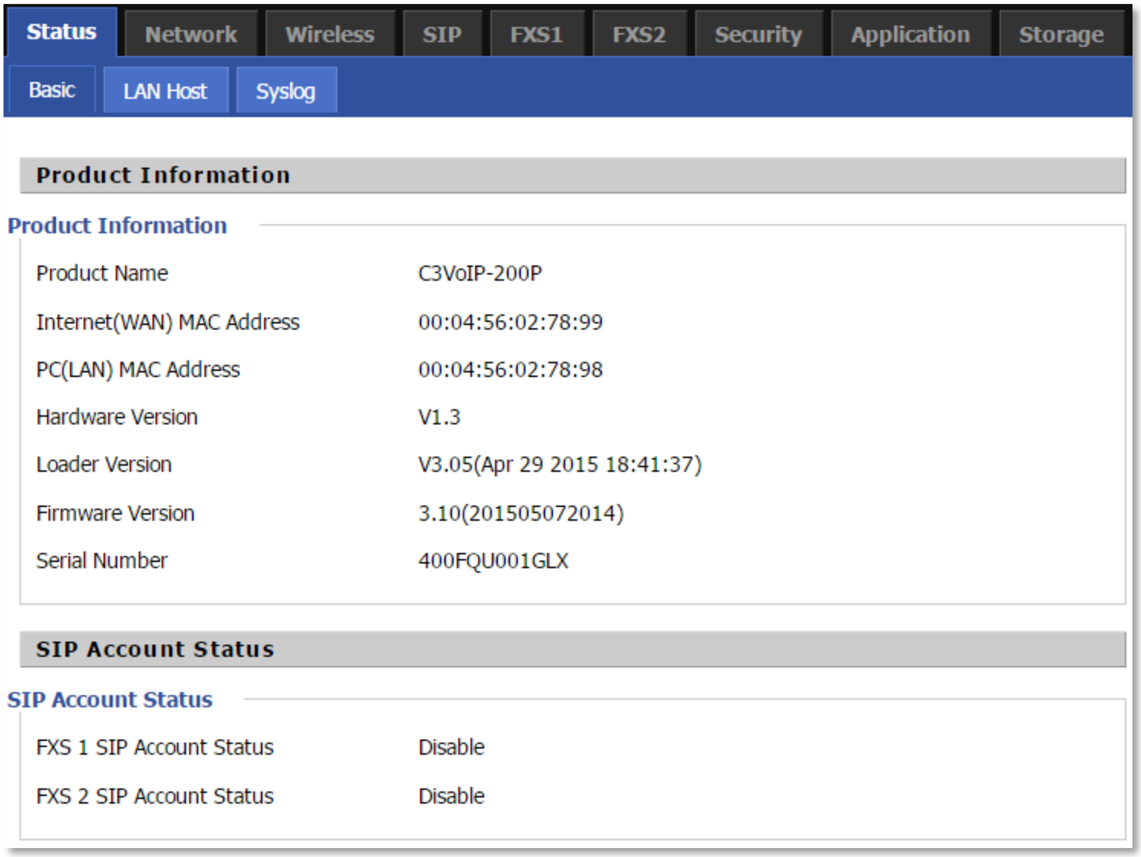
Upon the following dialogue:

Please REBOOT to make the changes effective!

Please press Reboot *button to make changes effective.*

Viewing the Registration Status

Table 13 Registration status



Product Information

Product Information

Product Name	C3VoIP-200P
Internet(WAN) MAC Address	00:04:56:02:78:99
PC(LAN) MAC Address	00:04:56:02:78:98
Hardware Version	V1.3
Loader Version	V3.05(Apr 29 2015 18:41:37)
Firmware Version	3.10(201505072014)
Serial Number	400FQU001GLX

SIP Account Status

SIP Account Status

FXS 1 SIP Account Status	Disable
FXS 2 SIP Account Status	Disable

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, or
- 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 Configuration

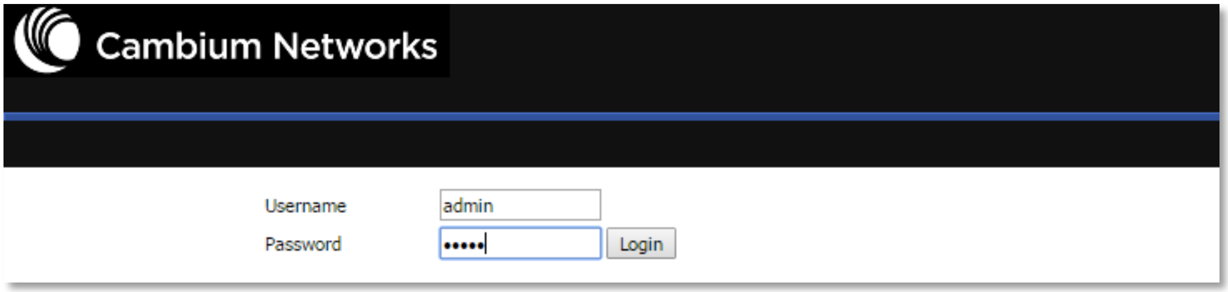
This chapter guides users to execute advanced (full) configuration through admin mode operation.

This chapter covers:

- *Login*
- *Status*
- *Network and Security*
- *Wireless*
- *SIP*
- *FXS1*
- *FXS2*
- *Security*
- *Application*
- *Administration*
- *Management*
- *System Log*
- *Logout*
- *Reboot*

Login

Table 14 Login details



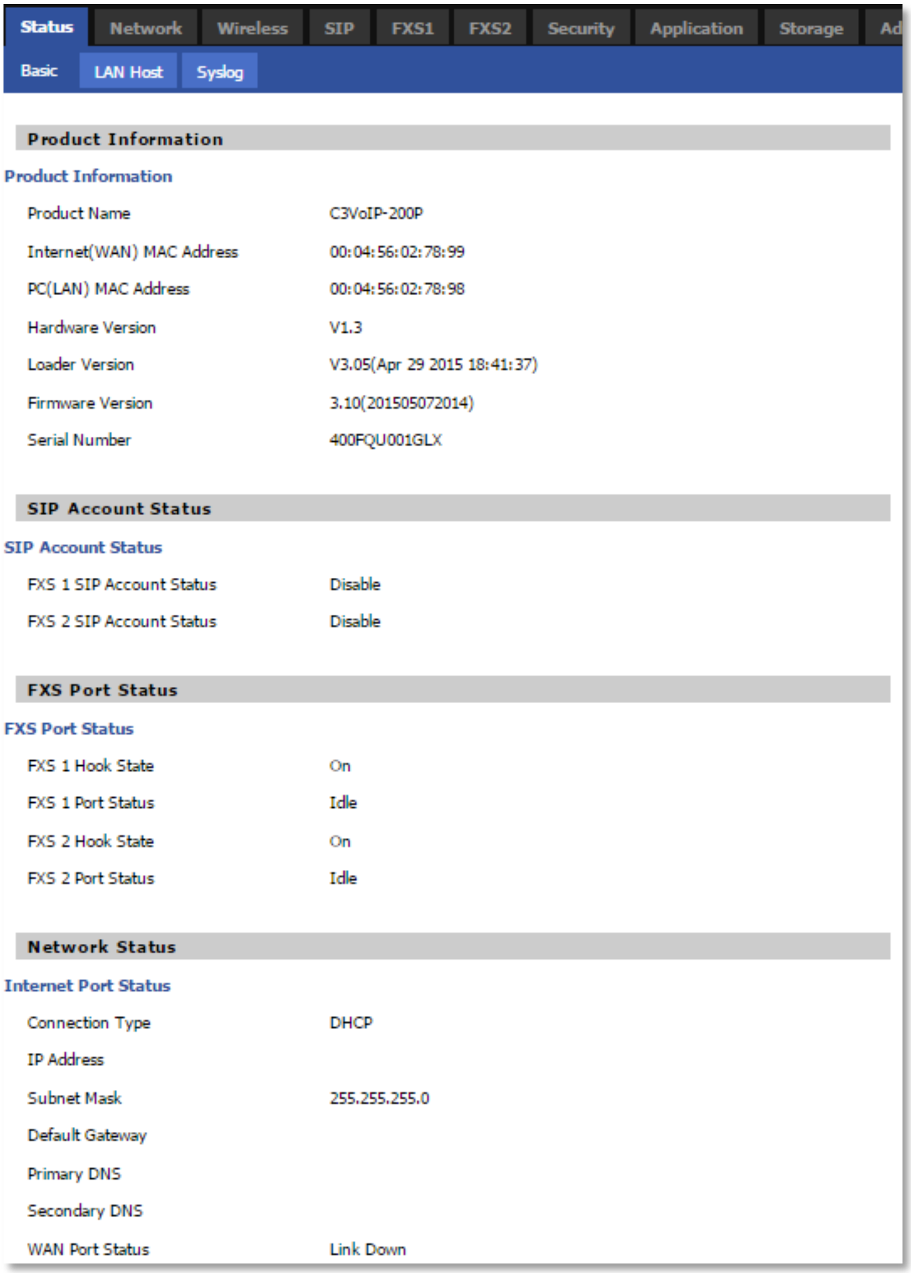
Username: admin

Password: •••••

Procedure
1. Connect the LAN port of the router to your PC vi an Ethernet cable
2. Open a web browser on your PC and type **http://192.168.11.1.**
3. Enter Username **admin** and Password **admin.**
4. Click **Login**

Status

Table 15 Status Page



Product Information

Product Information

Product Name	C3VoIP-200P
Internet(WAN) MAC Address	00:04:56:02:78:99
PC(LAN) MAC Address	00:04:56:02:78:98
Hardware Version	V1.3
Loader Version	V3.05(Apr 29 2015 18:41:37)
Firmware Version	3.10(201505072014)
Serial Number	400FQU001GLX

SIP Account Status

SIP Account Status

FXS 1 SIP Account Status	Disable
FXS 2 SIP Account Status	Disable

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

Internet Port Status

Connection Type	DHCP
IP Address	
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS	
Secondary DNS	
WAN Port Status	Link Down

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

Network and Security

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

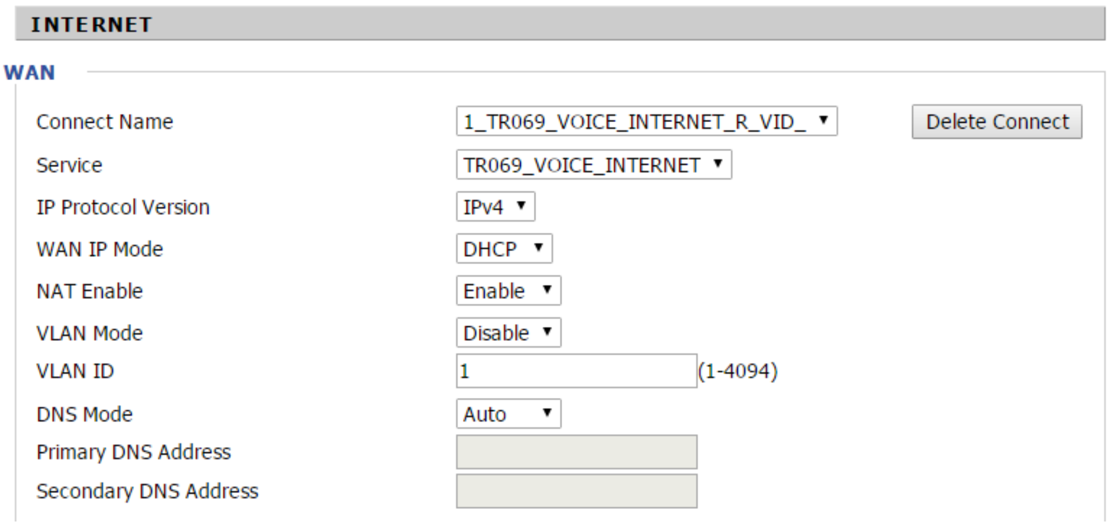
WAN

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 16 Internet



INTERNET

WAN

Connect Name	1_TR069_VOICE_INTERNET_R_VID_ ▼	Delete Connect
Service	TR069_VOICE_INTERNET ▼	
IP Protocol Version	IPv4 ▼	
WAN IP Mode	DHCP ▼	
NAT Enable	Enable ▼	
VLAN Mode	Disable ▼	
VLAN ID	1 (1-4094)	
DNS Mode	Auto ▼	
Primary DNS Address		
Secondary DNS Address		

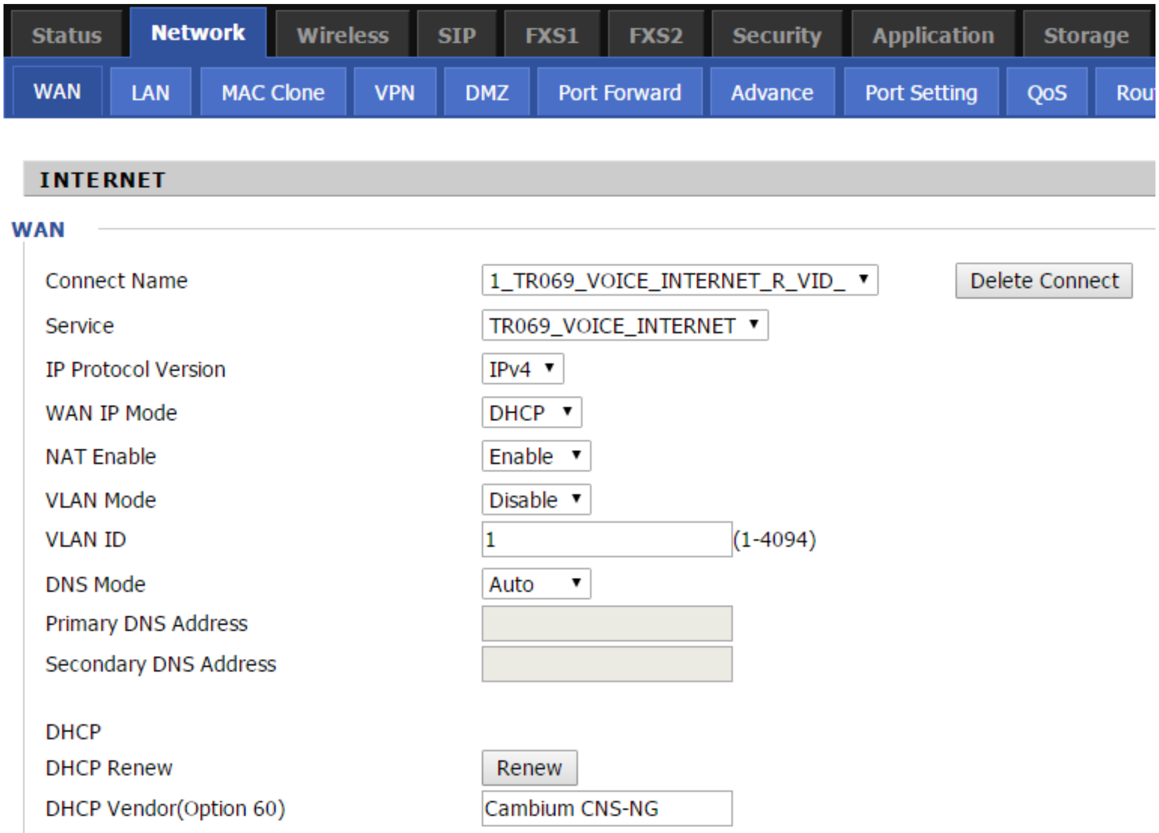
Field Name	Description
IP Address	The IP address of Internet port
Subnet Mask	The subnet mask of Internet port
Default Gateway	The default gateway of Internet port
DNS Mode	Select DNS mode, options are **Auto** and **Manual**: 1. When DNS mode is **Auto**, the device under LAN port will automatically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

DHCP

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

The DHCP feature allows to the cnPilot Home 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 17 DHCP



Connect Name	1_TR069_VOICE_INTERNET_R_VID_
Service	TR069_VOICE_INTERNET
IP Protocol Version	IPv4
WAN IP Mode	DHCP
NAT Enable	Enable
VLAN Mode	Disable
VLAN ID	1 (1-4094)
DNS Mode	Auto
Primary DNS Address	
Secondary DNS Address	
DHCP Renew	Renew
DHCP Vendor(Option 60)	Cambium CNS-NG

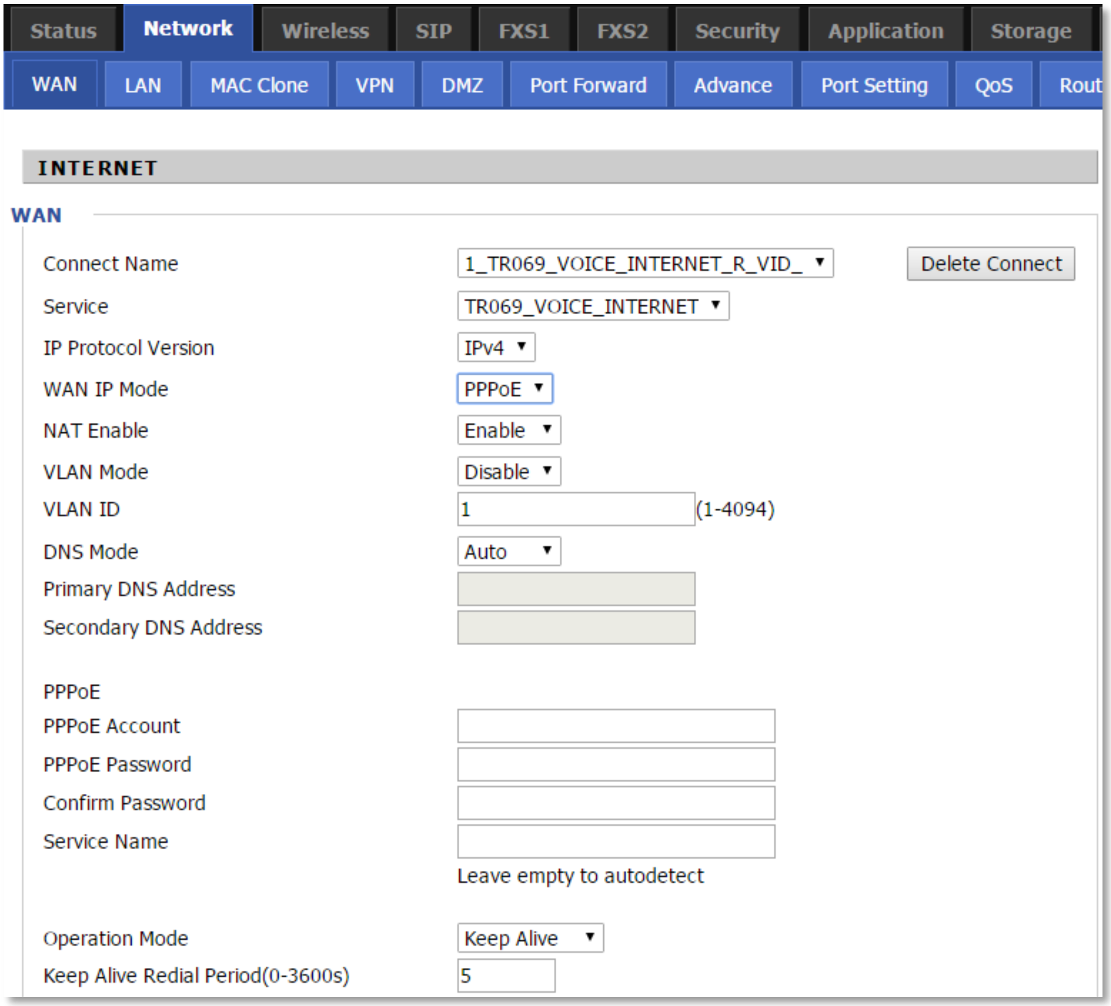
Field Name	Description
DNS Mode	Select DNS mode, options are Auto and Manual: 1. When DNS mode is Auto, the device under LAN port will automatically obtain the preferred DNS and alternate DNS. 2. When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS
Primary DNS Address	Primary DNS of Internet port.
Secondary DNS Address	Secondary DNS of Internet port.
DHCP Renew	Refresh the DHCP IP address
DHCP Vendor (Option60)	Specify the DHCP Vendor field. Display the vendor and product name.

PPPoE

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

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

Table 18 PPPoE



INTERNET

WAN

Connect Name	1_TR069_VOICE_INTERNET_R_VID_ ▼
Service	TR069_VOICE_INTERNET ▼
IP Protocol Version	IPv4 ▼
WAN IP Mode	PPPoE ▼
NAT Enable	Enable ▼
VLAN Mode	Disable ▼
VLAN ID	1 (1-4094)
DNS Mode	Auto ▼
Primary DNS Address	
Secondary DNS Address	
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
Confirm Password	Enter your PPPoE password again
Operation Mode	Select the mode of operation, options are **Keep Alive, On Demand**

	and **Manual**: • When the mode is **Keep Alive**, the user sets the 'keep alive redial period' values range from 0 to 3600s, the default setting is 5 minutes; • When the mode is **On Demand**, the user sets the 'on demand idle time' value in the range of 0-60 minutes, the default setting is 5 minutes; Operation Mode: On Demand ▾ On Demand Idle Time(0-60m): 5 • When the mode is **Manual**, there are no additional settings to configure
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

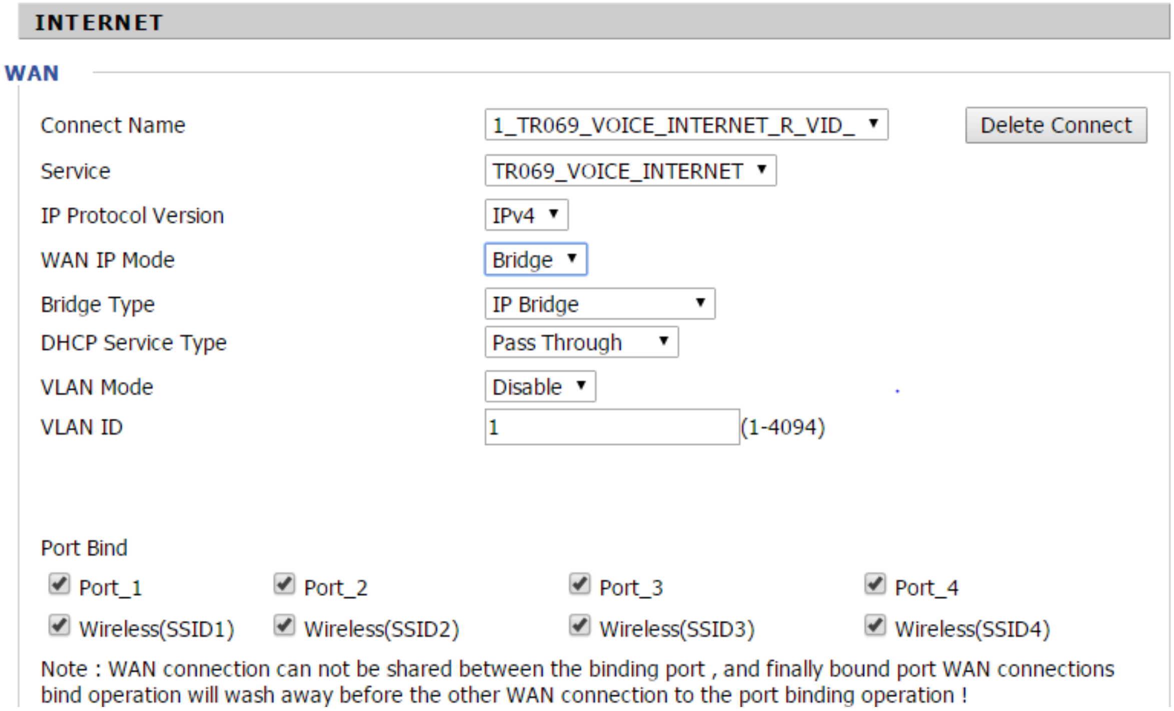
Bridge Mode under Multi WAN is different with traditional bridge setting. Bridge mode employs no IP addressing and the device operates as a bridge between the WAN port and the LAN port. Route Connection has to be built to give IP address to local service on device.

Under is example of bridge mode:

1_TR069_VOICE_INTERNET_R_VID_ is router connection for local service.

2_Other_B_VID_ is bridge connection for host of LAN port.

Table 19 Bridge Mode



INTERNET

WAN

Connect Name	1_TR069_VOICE_INTERNET_R_VID_ ▼
Service	TR069_VOICE_INTERNET ▼
IP Protocol Version	IPv4 ▼
WAN IP Mode	Bridge ▼
Bridge Type	IP Bridge ▼
DHCP Service Type	Pass Through ▼
VLAN Mode	Disable ▼
VLAN ID	1 (1-4094)

Port Bind

☑ Port_1 ☑ Port_2 ☑ Port_3 ☑ Port_4

☑ Wireless(SSID1) ☑ Wireless(SSID2) ☑ Wireless(SSID3) ☑ Wireless(SSID4)

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.
802.1p	Set the priority of VLAN, Options are 0~7.

Connect Name and Service

Table 20 Connect name

Content	Define	Comment
No	1～99	WAN Connection identifier
Service	TR069	The connection supports management applications i.e. R069, WEB, SNMP and Provision
	INTERNET	The connection solely supports internet service
	TR069_INTERNET	The connection supports management and internet applications
	VOICE	The connection supports voice applications, like SIP and RTP
	TR069_VOICE	The connection supports both management and voice applications
	VOICE_INTERNET	The connection supports voice and internet applications
	TR069_VOICE_INTERNET	The connection supports management, voice and internet applications
	Other	The connection support STB
NAT Mode	B	Bridge
	R	Router
VLAN ID	VID	VLAN ID

For example:
1_TR069_R_VID_2 (First Interface, Service is TR069, NAT Mode, VLAN ID is 2)
2_INTERNET_B_VID_(Second Interface, Service is INTERNET, Bridge Mode, VLAN is disabled)

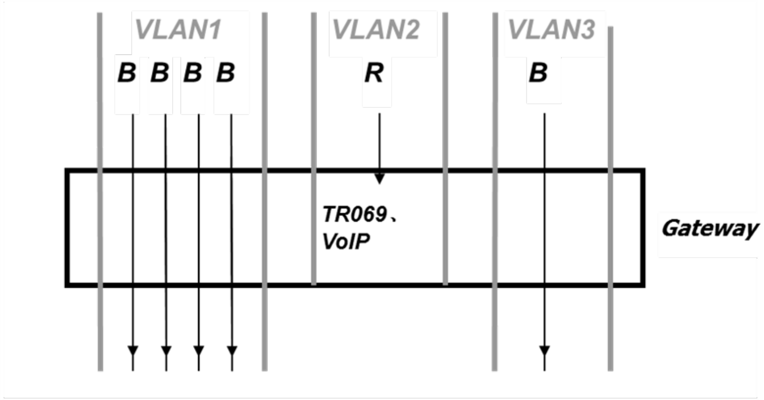
Multi WAN Setting

Overview

Multi WAN is used to implement the distribution of different kinds of services, and device's Multi WAN supports the distribution of data services, voice services and management services. By setting different VLANs, different kinds of data is distributed to the corresponding networks.

For example, INTERNET and Other VLAN supports data transmission, VOICE VLAN supports voice transmission and TR069 VLAN supports WEB, Telnet and TR069 services transmission.

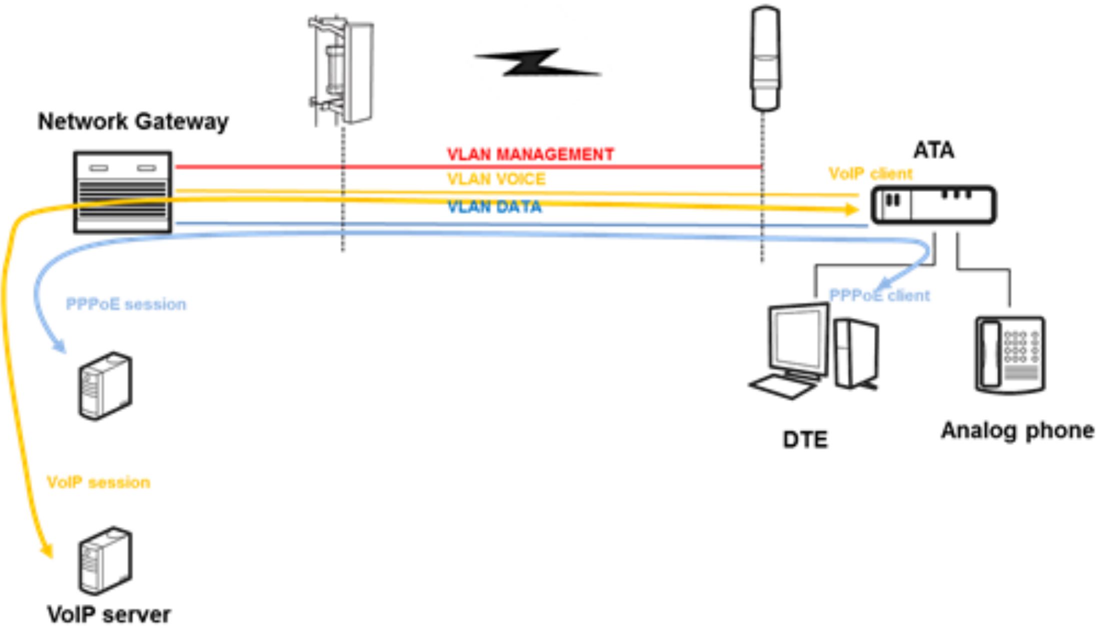
Figure 3 Multi VLAN



There are several advanced functions available when using Multi WAN setting:

- PPPoE Bridge allows PPPoE-only packets to pass, which can prohibit Layer 2 packets from flooding the device LAN ports.
- Hardware Bridge operates as a Layer 2 Switch to increase throughput between WAN and LAN.
- VLAN Trunk allows tagged packets to be switched to LAN ports directly.
- IPTV may be supported with other VLAN-configured LAN ports.

Figure 4 Multi WAN network

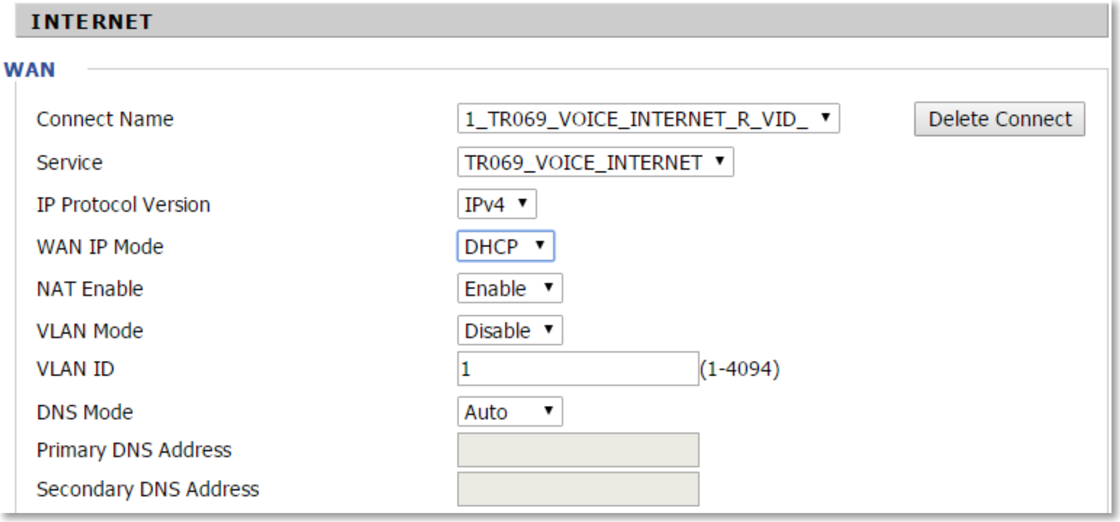


Setting up the Internet Connection

From the WAN page, a multi WAN connection can be created or deleted. See below for more information on configuring these settings.

Connect Name and Service

Table 21 Internet



INTERNET

WAN

Connect Name	1_TR069_VOICE_INTERNET_R_VID_ ▾	Delete Connect
Service	TR069_VOICE_INTERNET ▾	
IP Protocol Version	IPv4 ▾	
WAN IP Mode	DHCP ▾	
NAT Enable	Enable ▾	
VLAN Mode	Disable ▾	
VLAN ID	1 (1-4094)	
DNS Mode	Auto ▾	
Primary DNS Address		
Secondary DNS Address		

Content	Define	Comment
No	1 to 99	WAN Connection identifier

Service	TR069	The connection supports management applications including TR069, WEB, SNMP and Provision
	INTERNET	The connection supports Internet service
	TR069_INTERNET	The connection supports management and internet applications
	VOICE	The connection support voice applications like SIP and RTP
	TR069_VOICE	The connection supports both management and voice applications
	VOICE_INTERNET	The connection supports voice and Internet applications
	TR069_VOICE_INTERNET	The connection supports management, voice and Internet applications
	Other	The connection support STB
NAT Mode	B	Bridge
	R	Router
VLAN ID	VID	VLAN ID

For example:

1_TR069_R_VID_2 (First Interface, Service is TR069, NAT Mode, VLAN ID is 2)

2_INTERNET_B_VID_(Second Interface, Service is INTERNET, Bridge Mode, VLAN is disabled)

Bridge Mode

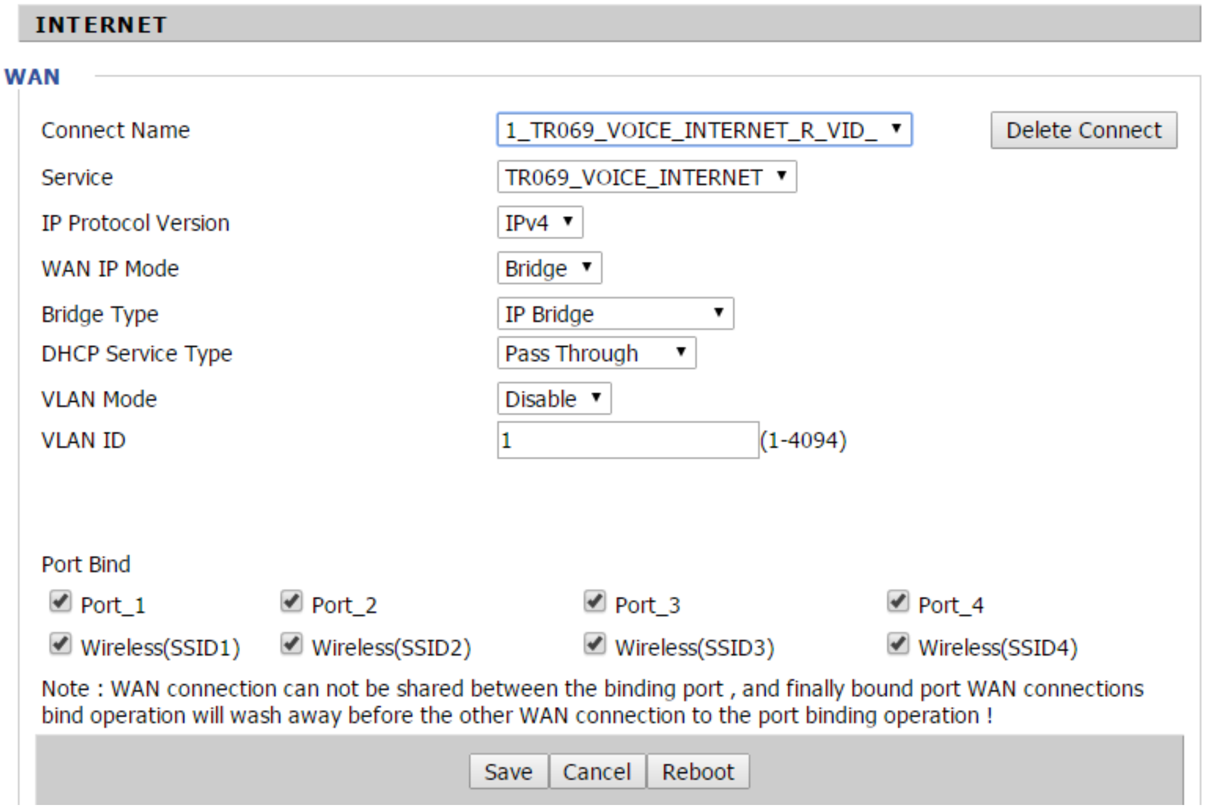
Bridge Mode under Multi WAN is different with traditional bridge setting. Bridge mode has no IP address and the device operates as a bridge between the WAN port and the LAN ports. Route Connection must be built to give IP address to local service on device.

Under is example of bridge mode:

1_TR069_VOICE_INTERNET_R_VID_ is router connection for local service.

2_Other_B_VID_ is bridge connection for host of LAN port.

Table 22 Bridge Mode



INTERNET

WAN

Connect Name	1_TR069_VOICE_INTERNET_R_VID_ ▾
Service	TR069_VOICE_INTERNET ▾
IP Protocol Version	IPv4 ▾
WAN IP Mode	Bridge ▾
Bridge Type	IP Bridge ▾
DHCP Service Type	Pass Through ▾
VLAN Mode	Disable ▾
VLAN ID	1 (1-4094)

Port Bind

☑ Port_1 ☑ Port_2 ☑ Port_3 ☑ Port_4

☑ Wireless(SSID1) ☑ Wireless(SSID2) ☑ Wireless(SSID3) ☑ Wireless(SSID4)

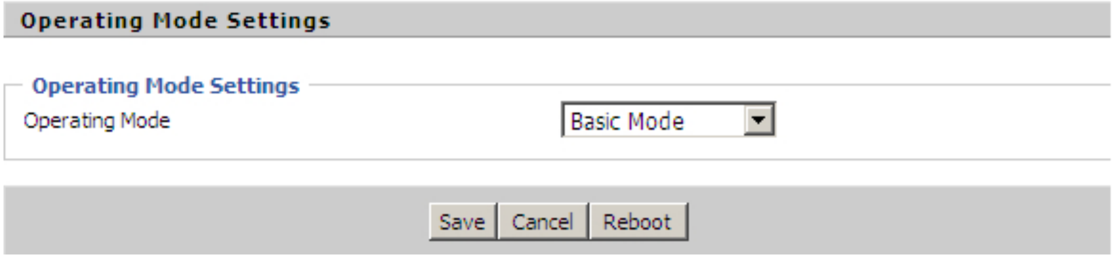
Note : WAN connection can not be shared between the binding port , and finally bound port WAN connections bind operation will wash away before the other WAN connection to the port binding operation !

Field Name	Description
Bridge Type	
IP Bridge	Allows all Ethernet packets to pass. A PC can connect to upper network directly.
PPPoE Bridge	Only Allows PPPoE packets pass. The PC needs PPPoE dial-up software.
Hardware IP Bridge	Packets pass through hardware switch at wired speed. Does not support wireless port binding.
DHCP Service Type	
Pass Through	DHCP packets are forwarded between the WAN interface and the LAN interface, the DHCP server in the device will not allocate IP to clients of the LAN port.
DHCP Snooping	When the device forwards DHCP packets from the LAN interface to the WAN interface it will add option82 to DHCP packet, and it will remove option82 when forwarding DHCP packets from the WAN interface to the LAN interface. Local DHCP service will not allocate IP to hosts of LAN port.
Local Service	The device will not forward DHCP packets between the LAN interface and the WAN interface, and it also blocks DHCP packets from the WAN port. Clients of the LAN port can retrieve IP addressing from the DHCP

	server in the device.
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 the WAN interface and the LAN interface.

Fast Bridge Setting

Step 1 Login to the web management interface of the cnPilot Device. Navigate to Page **Administration->Operating Mode**. Set **Operating** mode to **Basic Mode**. Click **Save**.

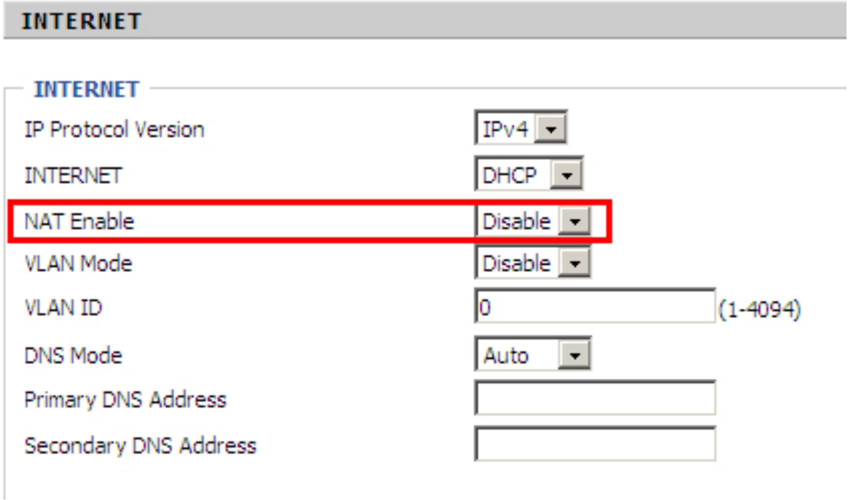


Operating Mode Settings

Operating Mode Settings

Operating Mode	Basic Mode

Step 2 Open **Network->WAN**, Change **NAT Enable** to **Disable**. Click **Save** then **Reboot**. The device is now operating in Bridge mode.

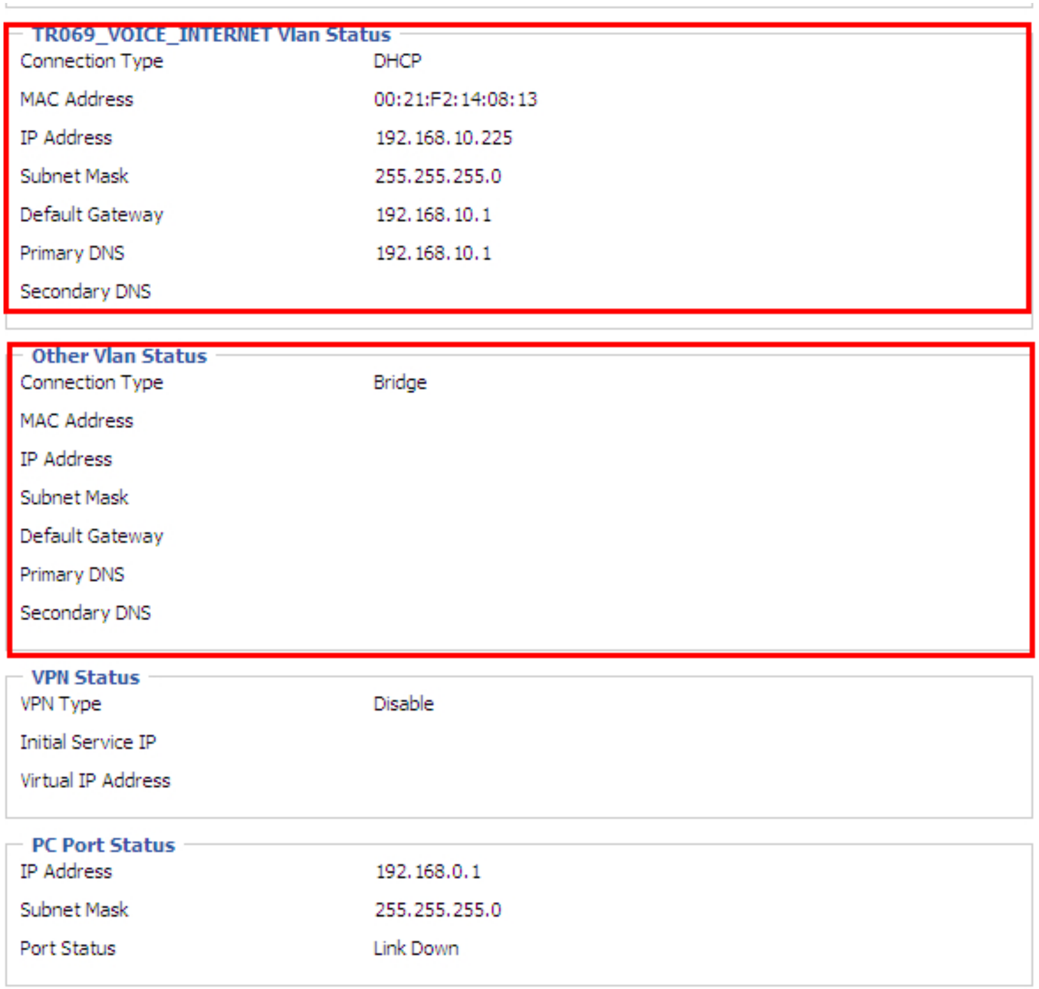


INTERNET

INTERNET

IP Protocol Version	IPv4
INTERNET	DHCP
NAT Enable	Disable
VLAN Mode	Disable
VLAN ID	0 (1-4094)
DNS Mode	Auto
Primary DNS Address	
Secondary DNS Address	

Step 3 Log into the device via the WAN port. Below is example of Page **Status->Basic** displaying device configuration.



TR069_VOICE_INTERNET Vlan Status

Connection Type	DHCP
MAC Address	00:21:F2:14:08:13
IP Address	192.168.10.225
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
Primary DNS	192.168.10.1
Secondary DNS	

Other Vlan Status

Connection Type	Bridge
MAC Address	
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	

VPN Status

VPN Type	Disable
Initial Service IP	
Virtual IP Address	

PC Port Status

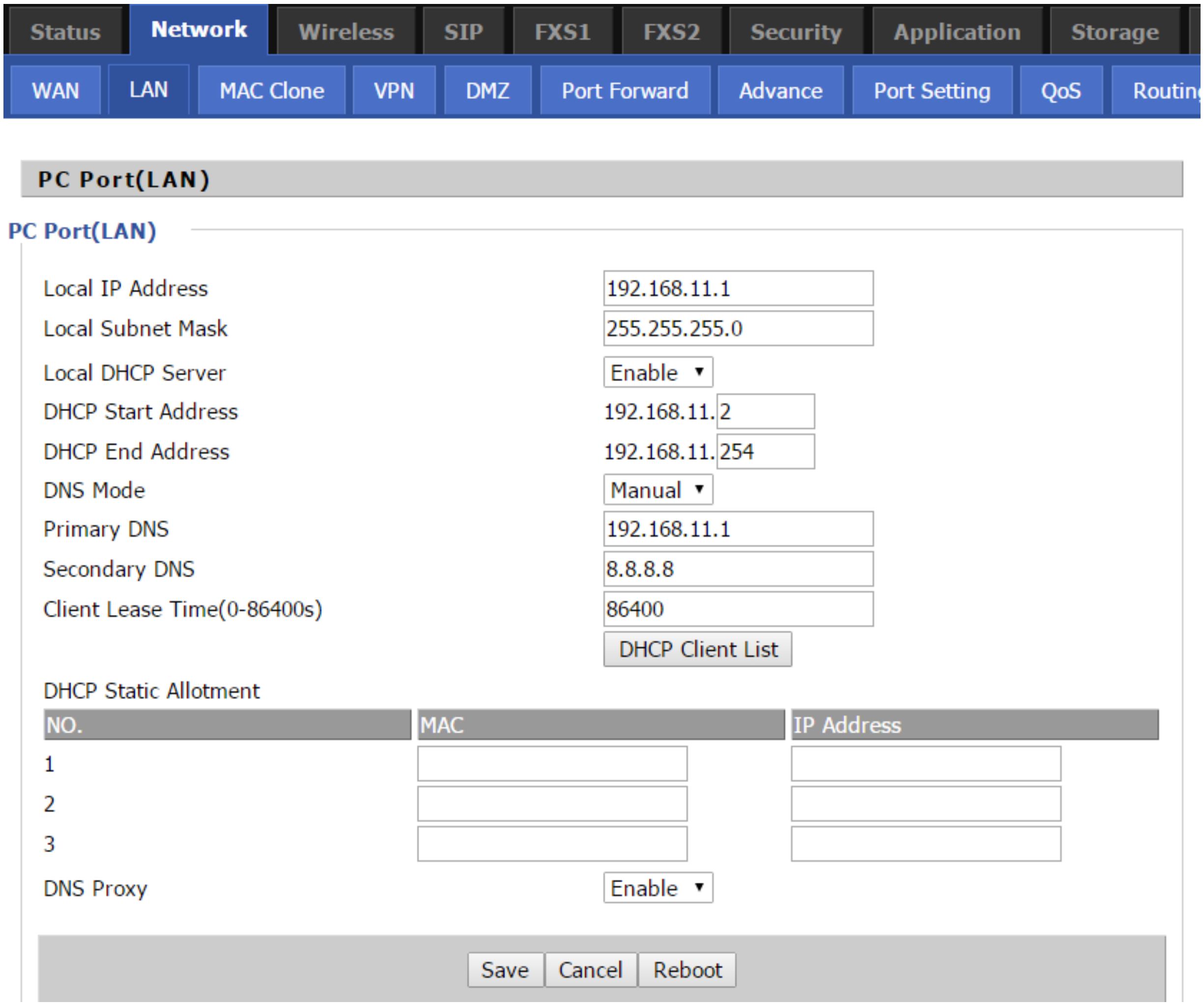
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Port Status	Link Down

LAN

LAN Port

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

Table 23 LAN port



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

DHCP Static Allotment

NO.	MAC	IP Address
1		
2		
3		

DNS Proxy: Enable

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

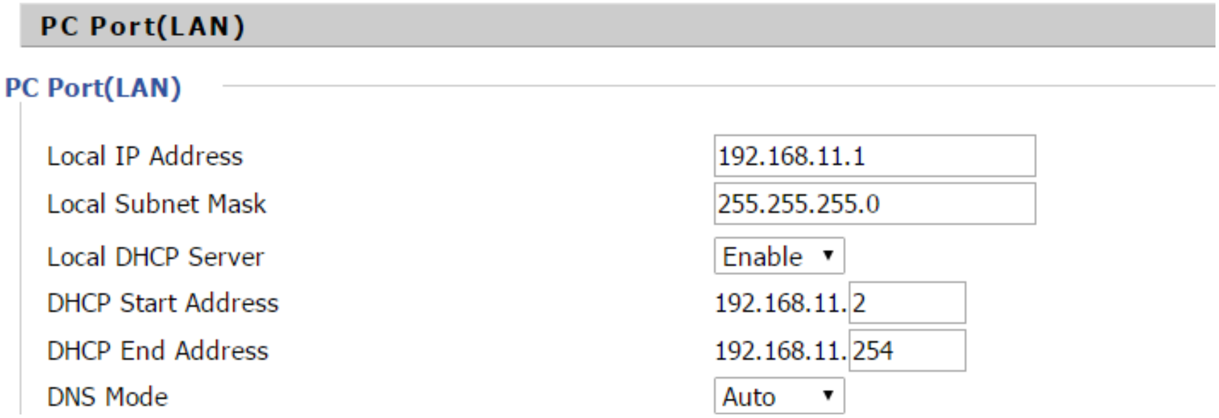
	address.
DHCP End Address	Enter a valid IP address as an end IP address of the DHCP server.
DNS Mode	Select DNS mode, options are Auto and Manual: 1. When DNS mode is Auto, the device under LAN port will automatically obtains the preferred DNS and alternate DNS. 2. When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS.
Primary DNS	Enter the preferred DNS address.
Secondary DNS	Enter the secondary DNS address.
Client Lease Time	This option defines how long the address will be assigned to the computer within the network. In that period, the server does not assign the IP address to the other computer.
DNS Proxy	Enable or disable; If enabled, the device will forward the DNS request of LAN-side network to the WAN side network.

DHCP Server

The 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 24 DHCP server settings



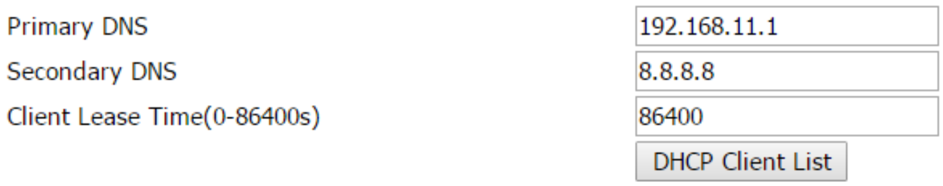
PC Port(LAN)

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 25 DHCP server, DNS and Client Lease Time



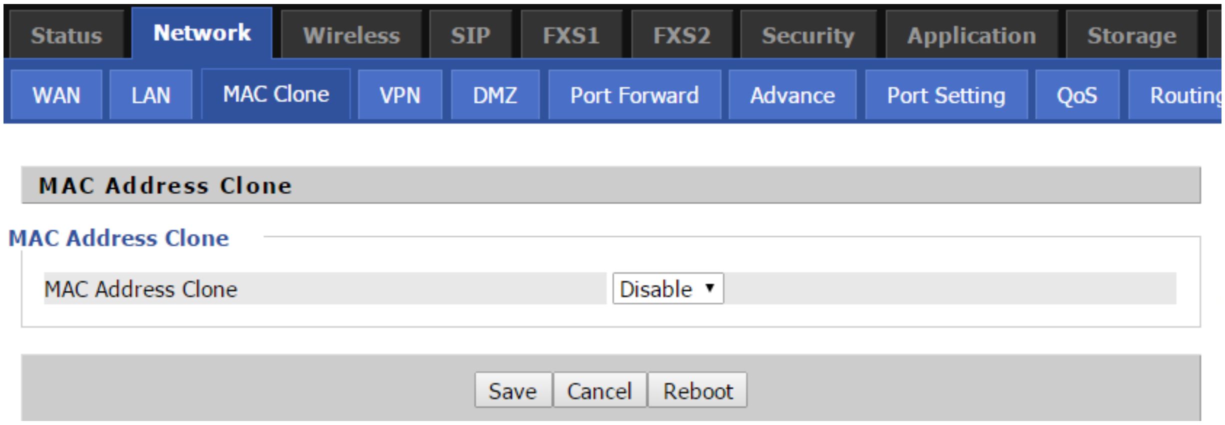
Primary DNS	192.168.11.1
Secondary DNS	8.8.8.8
Client Lease Time(0-86400s)	86400

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.

MAC Clone

Some ISPs will require you to register your MAC address. If you do not wish to re-register your MAC address, you can have the router clone the MAC address that is registered with your ISP. To use the Clone Address button, the computer accessing the web management interface will have the MAC address automatically entered in the Clone WAN MAC field.

Table 26 MAC clone



MAC Address Clone

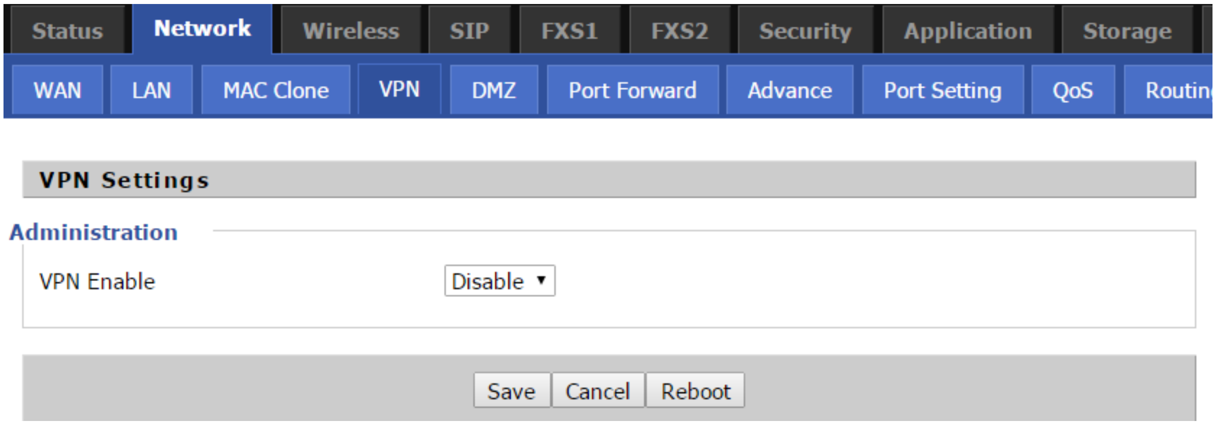
MAC Address Clone: Disable

Field Name	Description
Procedure	
1. Press the button Get Current PC MAC gets PC's MAC address	
2. Press the button Save to save your changes if users don't want to use MAC clone, press the button Cancel to cancel the changes	
3. Press the button Reboot to make the changes effective.	

VPN

The cnPilot Home supports VPN connections with PPTP-based VPN servers.

Table 27 VPN



VPN Settings

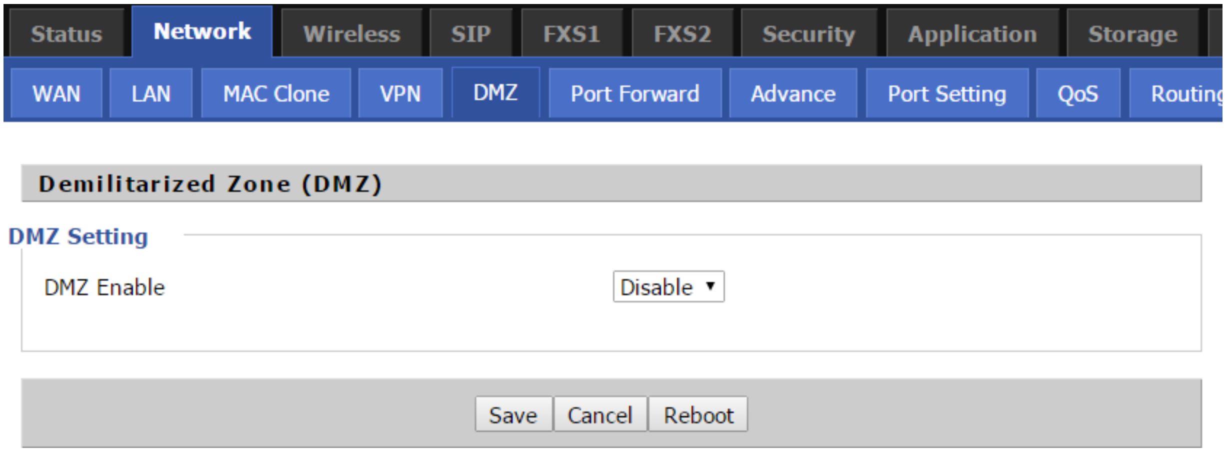
Administration

VPN Enable: Disable

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

DMZ

Table 28 DMZ



Demilitarized Zone (DMZ)

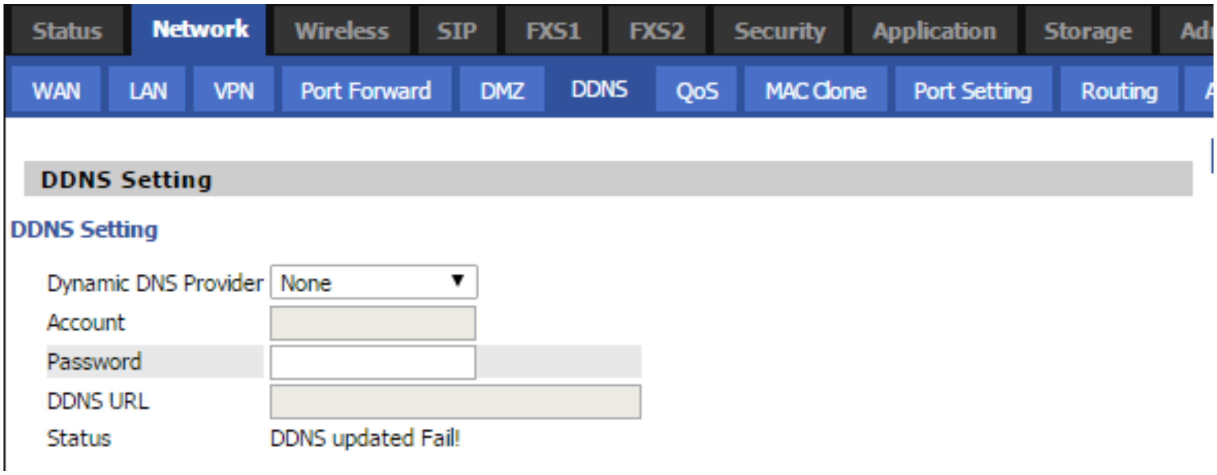
DMZ Setting

DMZ Enable: Disable

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

DDNS Setting

Table 29 DDNS setting



DDNS Setting

DDNS Setting

Dynamic DNS Provider: None ▼

Account

Password

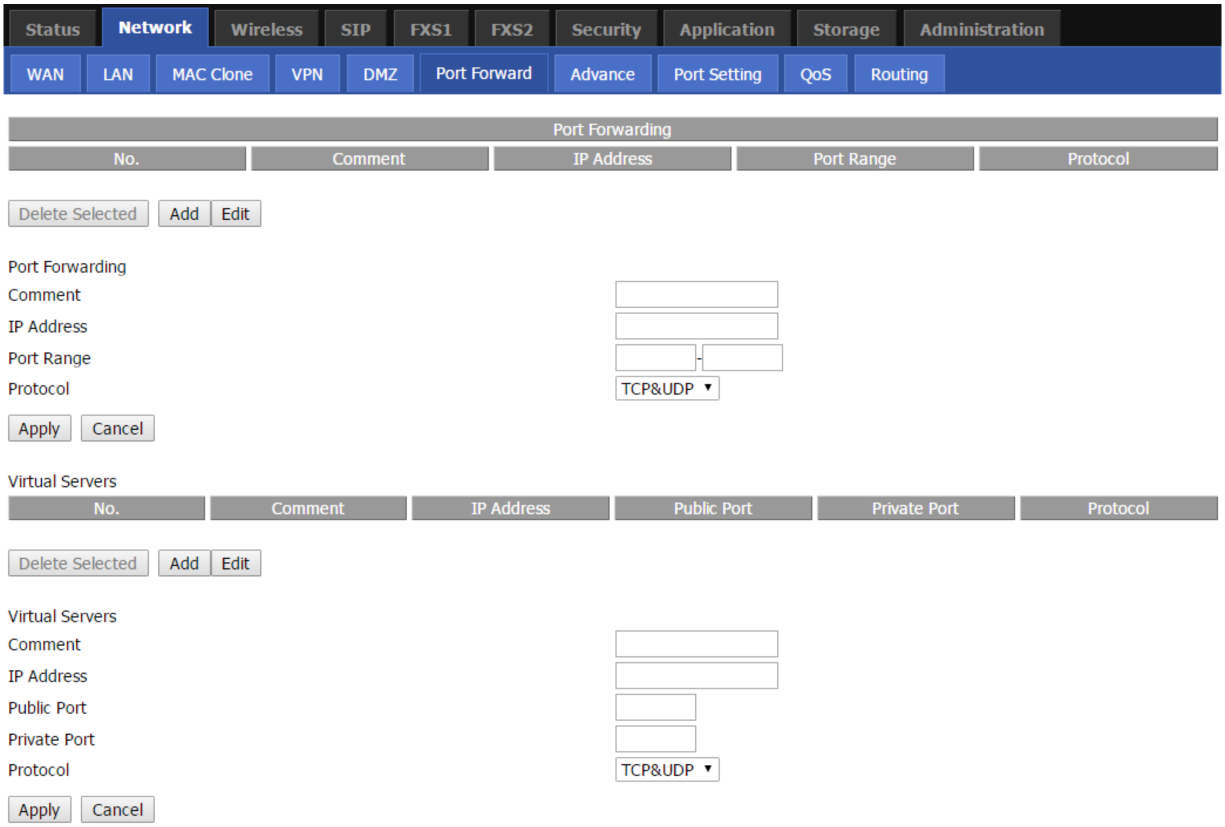
DDNS URL

Status: DDNS updated Fail!

Field Name	Description
Dynamic DNS Provider	DDNS is enabled and select a DDNS service provider.
Account	Enter the DDNS service account.
Password	Enter the DDNS service account password.
DDNS	Enter the DDNS domain name or IP address.
Status	See if DDNS is successfully upgraded.

Port Forward

Table 30 Port Forward



Port Forwarding

No.	Comment	IP Address	Port Range	Protocol

Port Forwarding

Comment	
IP Address	
Port Range	-
Protocol	TCP&UDP ▾

Virtual Servers

No.	Comment	IP Address	Public Port	Private Port	Protocol

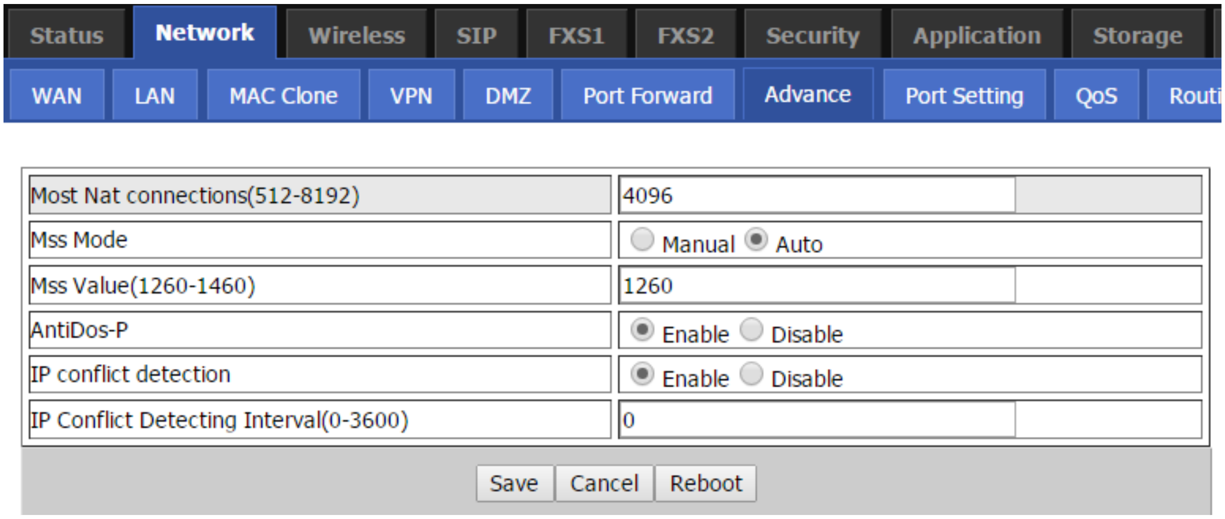
Virtual Servers

Comment	
IP Address	
Public Port	
Private Port	
Protocol	TCP&UDP ▾

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.

Advance

Table 31 Advance

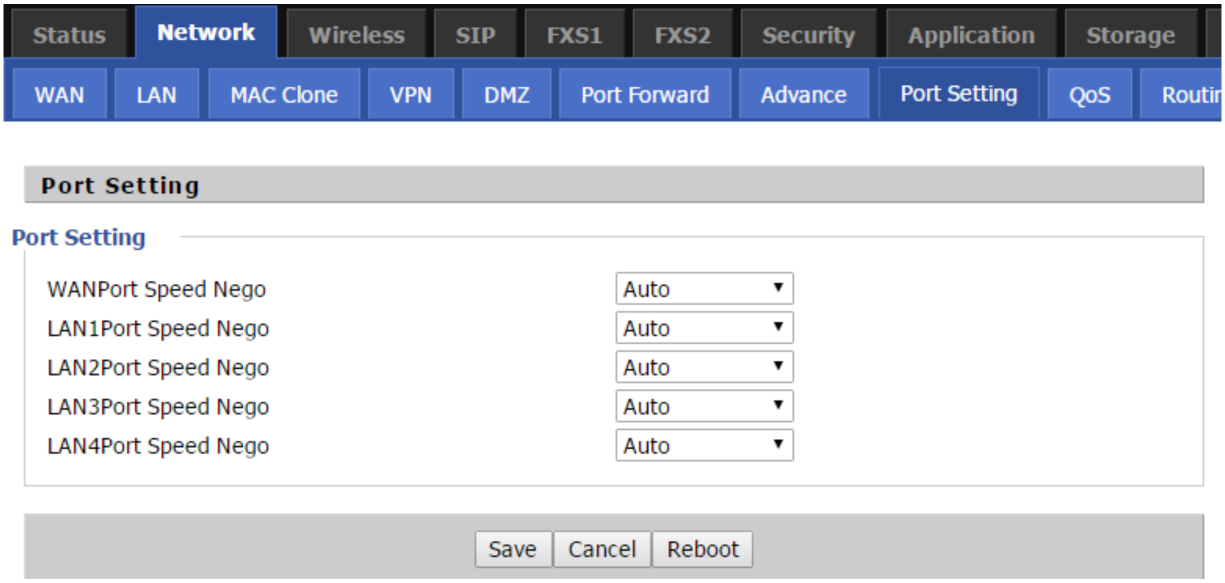


Most Nat connections(512-8192)	4096
Mss Mode	○ Manual ● Auto
Mss Value(1260-1460)	1260
AntiDos-P	● Enable ○ Disable
IP conflict detection	● Enable ○ Disable
IP Conflict Detecting Interval(0-3600)	0

Field Name	Description
Most Nat connections	The largest value which the cnPilot Home R200x 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

Port Setting

Table 32 Port setting

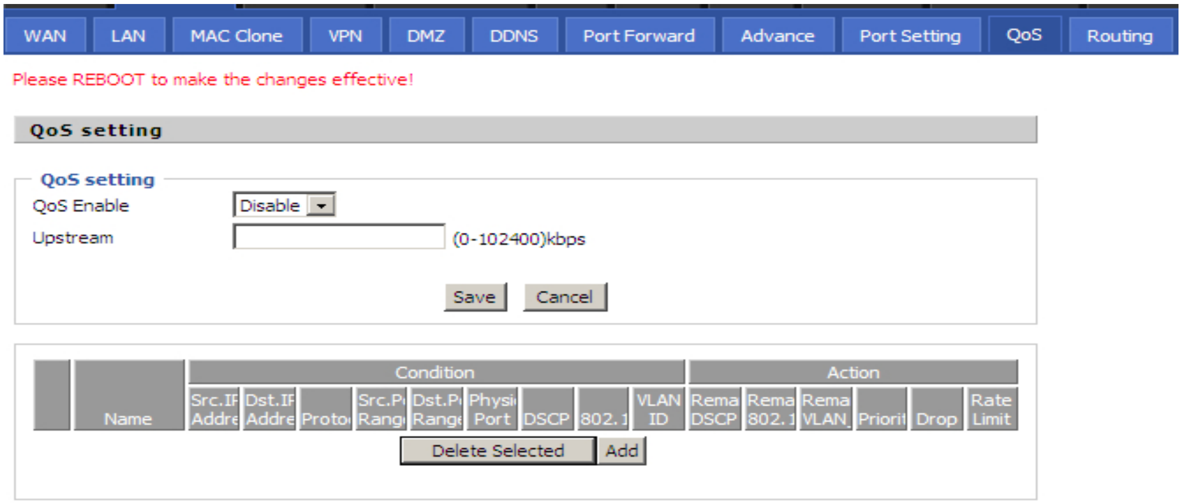


WANPort Speed Nego	Auto ▾
LAN1Port Speed Nego	Auto ▾
LAN2Port Speed Nego	Auto ▾
LAN3Port Speed Nego	Auto ▾
LAN4Port Speed Nego	Auto ▾

Field Name	Description
WAN Port speed Nego	Auto-negotiation, options are Auto, 100M full, 100M half-duplex, 10M half and full.
LAN1~LAN4 Port Speed Nego	Auto-negotiation, options are Auto, 100M full, 100M half, 10M half and 10M full.

QoS

Table 33 QoS



Please REBOOT to make the changes effective!

QoS setting

QoS setting

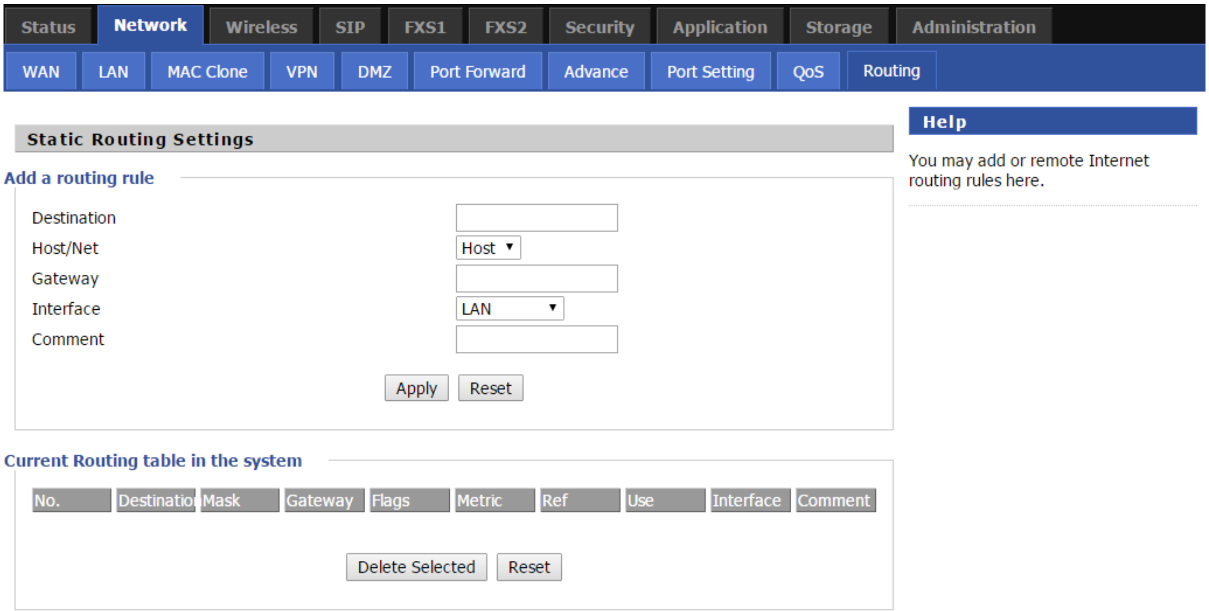
QoS Enable	Disable
Upstream	(0-102400)kbps

		Condition										Action					
	Name	Src.IP Addre	Dst.IP Addre	Proto	Src.P Rang	Dst.P Range	Physi Port	DSCP	802.1	VLAN ID	Rema DSCP	Rema 802.1	Rema VLAN_	Priorit	Drop	Rate Limit

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

Routing

Table 34 Routing



Static Routing Settings

Add a routing rule

Destination	
Host/Net	Host ▾
Gateway	
Interface	LAN ▾
Comment	

Apply Reset

Current Routing table in the system

No.	Destinatio	Mask	Gateway	Flags	Metric	Ref	Use	Interface	Comment

Delete Selected Reset

Help

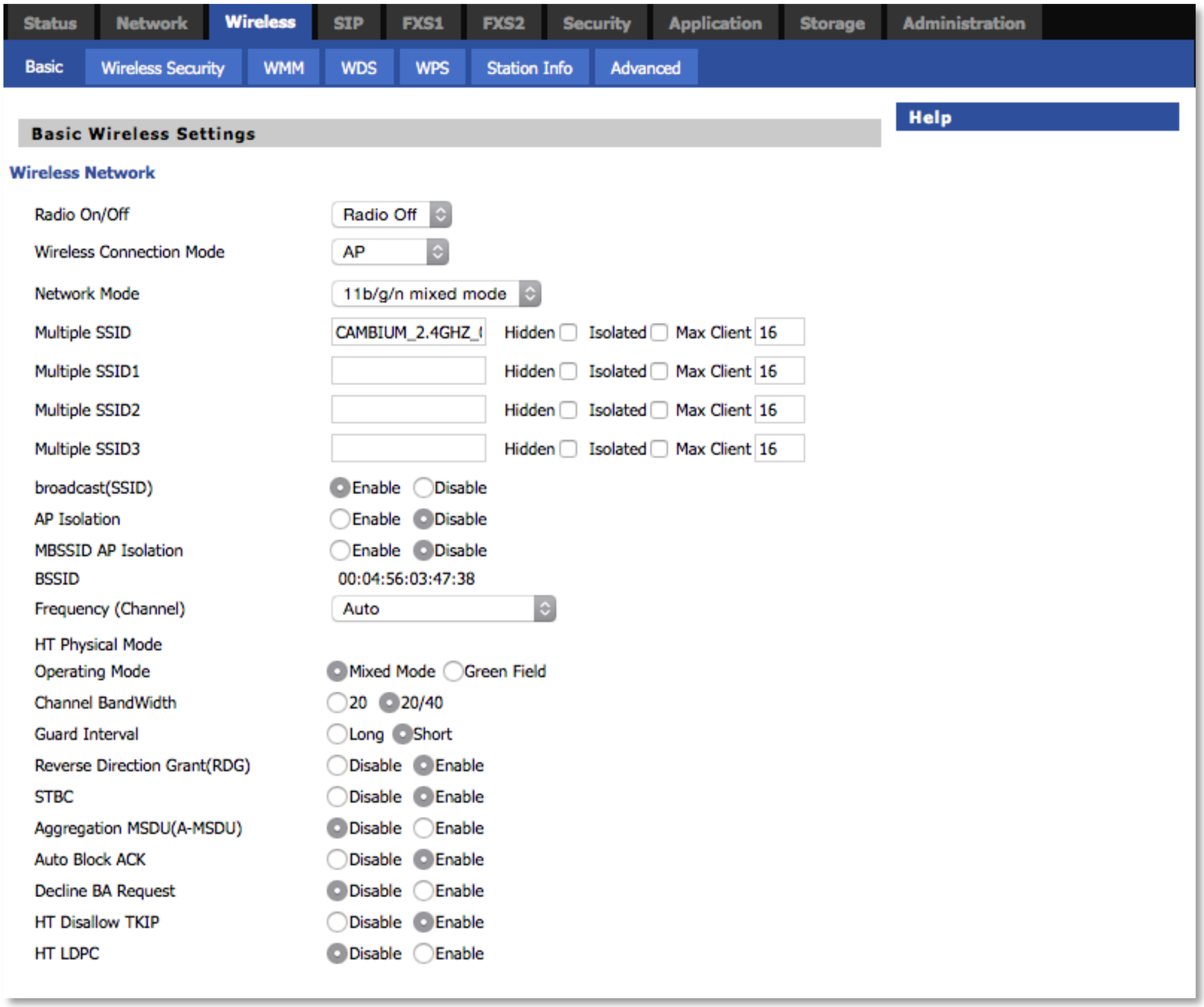
You may add or remote Internet routing rules here.

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

Wireless

Basic

Table 35 Basic

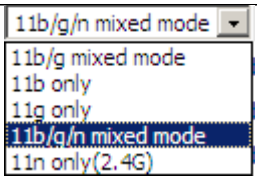


Basic Wireless Settings

Wireless Network

Radio On/Off	Radio Off
Wireless Connection Mode	AP
Network Mode	11b/g/n mixed mode
Multiple SSID	CAMBIUM_2.4GHZ_(Hidden □ Isolated □ Max Client 16
Multiple SSID1	Hidden □ Isolated □ Max Client 16
Multiple SSID2	Hidden □ Isolated □ Max Client 16
Multiple SSID3	Hidden □ Isolated □ Max Client 16
broadcast(SSID)	● Enable ○ Disable
AP Isolation	○ Enable ● Disable
MBSSID AP Isolation	○ Enable ● Disable
BSSID	00:04:56:03:47:38
Frequency (Channel)	Auto
HT Physical Mode	
Operating Mode	● Mixed Mode ○ Green Field
Channel BandWidth	○ 20 ● 20/40
Guard Interval	○ Long ● Short
Reverse Direction Grant(RDG)	○ Disable ● Enable
STBC	○ Disable ● Enable
Aggregation MSDU(A-MSDU)	● Disable ○ Enable
Auto Block ACK	○ Disable ● Enable
Decline BA Request	● Disable ○ Enable
HT Disallow TKIP	○ Disable ● Enable
HT LDPC	● Disable ○ Enable

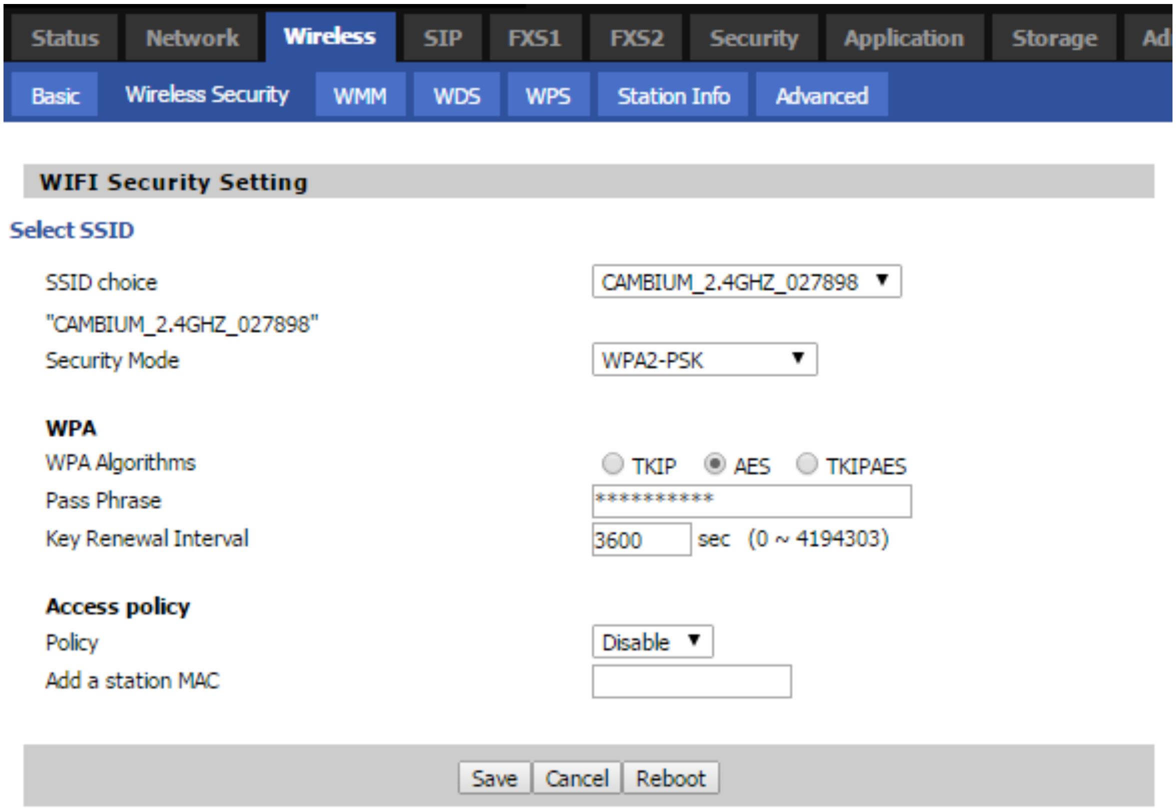
Field Name	Description
Radio on/off	Select "Radio off" to disable wireless. Select "Radio on" to enable wireless.
Wireless connection mode	According to the wireless client type, select one of these modes. Default is AP
Network Mode	Choose one network mode from the drop down list. Default is 11b/g/n mixed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

	 11b/g/n mixed mode 11b/g mixed mode 11b only 11g only 11b/g/n mixed mode 11n only(2.4G)
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	CnPilot Home R200x 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	1. Mixed Mode: In this mode, the previous wireless card can recognize and connect to the Pre-N AP, but the throughput will be affected 2. 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 Dirction 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

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

Wireless Security

Table 36 Wireless security



WIFI Security Setting

Select SSID

SSID choice	CAMBIUM_2.4GHZ_027898 ▼
"CAMBIUM_2.4GHZ_027898"	
Security Mode	WPA2-PSK ▼
WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	***********
Key Renewal Interval	3600 sec (0 ~ 4194303)
Access policy	
Policy	Disable ▼
Add a station MAC	

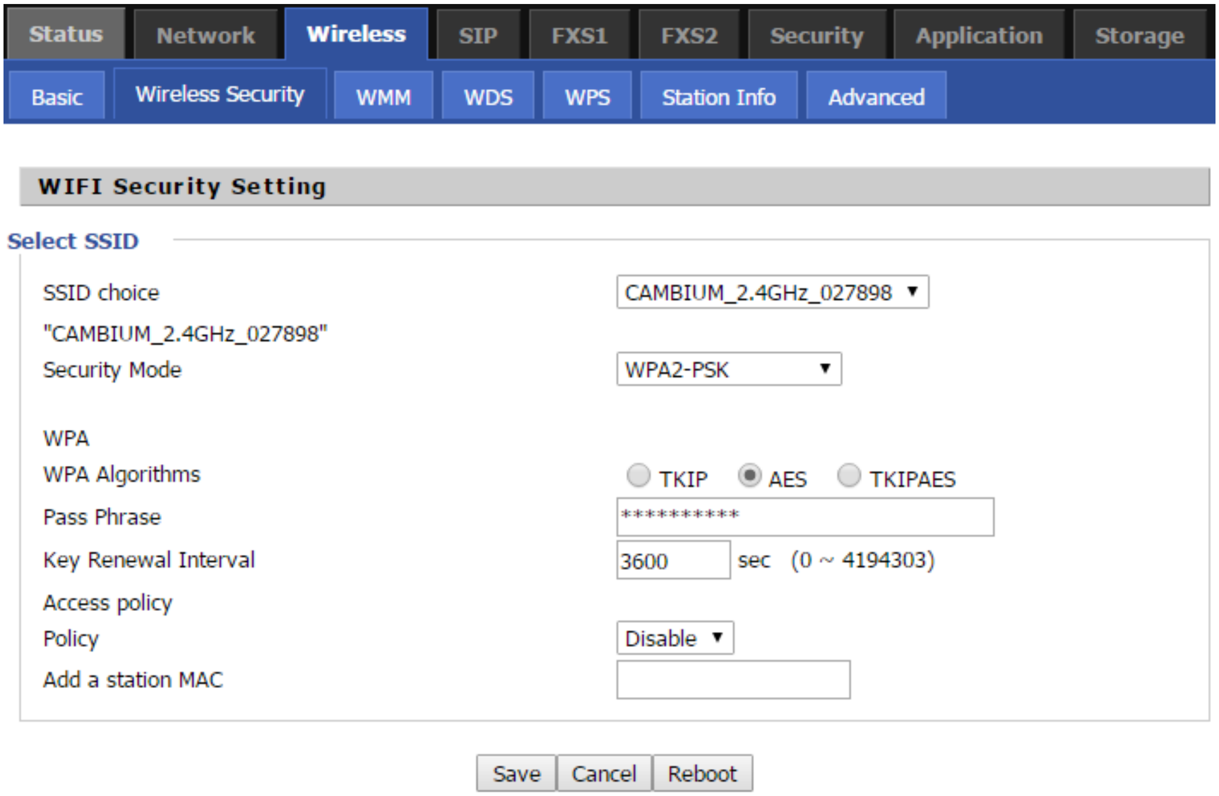
Save Cancel Reboot

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 privac 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 37 WiFI Security Setting



WIFI Security Setting

Select SSID

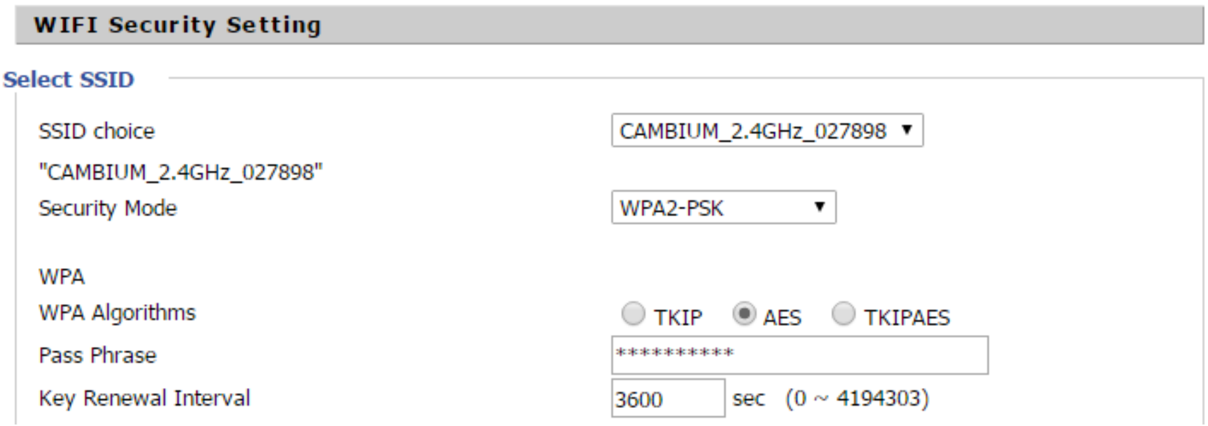
SSID choice	CAMBIUM_2.4GHz_027898 ▼
"CAMBIUM_2.4GHz_027898"	
Security Mode	WPA2-PSK ▼
WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	**********
Key Renewal Interval	3600 sec (0 ~ 4194303)
Access policy	
Policy	Disable ▼
Add a station MAC	

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 mode:

Table 38 WPA-PSK



WIFI Security Setting

Select SSID

SSID choice: CAMBIUM_2.4GHz_027898 ▼

"CAMBIUM_2.4GHz_027898"

Security Mode: WPA2-PSK ▼

WPA

WPA Algorithms: ○ TKIP ● AES ○ TKIPAES

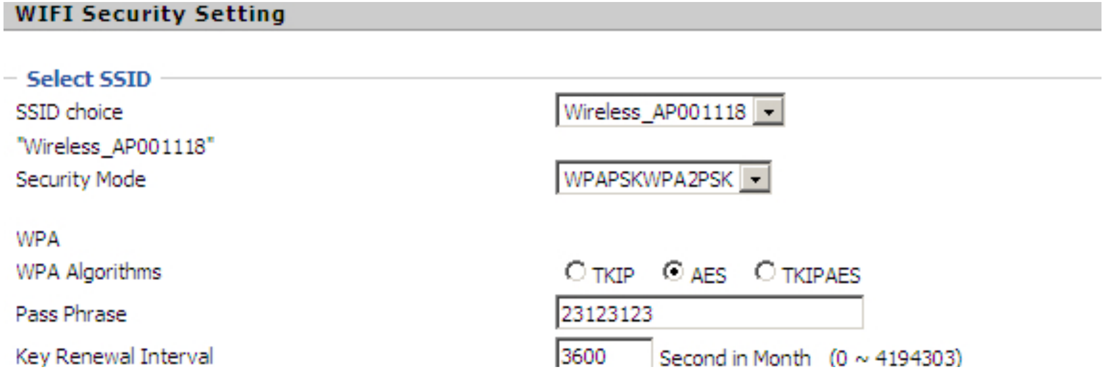
Pass Phrase: **********

Key Renewal Interval: 3600 sec (0 ~ 4194303)

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.
Key Renewal Interval	Set the key scheduled update cycle, default is 3600s.

WPAPSKWPA2PSK manner is consistent with WPA2PSK settings:

Table 39 WPAPSKWPA2PSK



WIFI Security Setting

Select SSID

SSID choice: Wireless_AP001118

"Wireless_AP001118"

Security Mode: WPAPSKWPA2PSK

WPA

WPA Algorithms: ○ TKIP ● AES ○ TKIPAES

Pass Phrase: 23123123

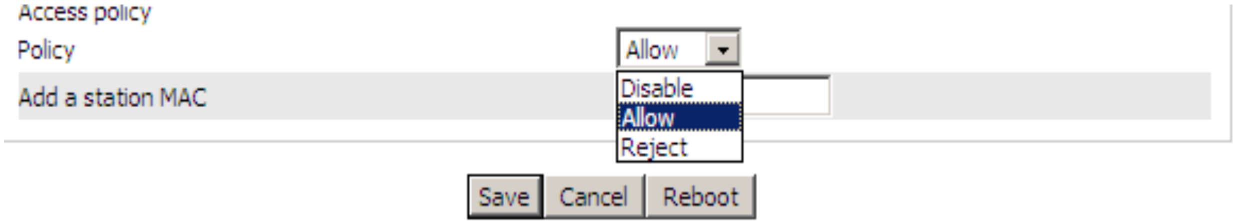
Key Renewal Interval: 3600 Second in Month (0 ~ 4194303)

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 40 Wireless Access Policy



Access policy

Policy: Allow

Add a station MAC

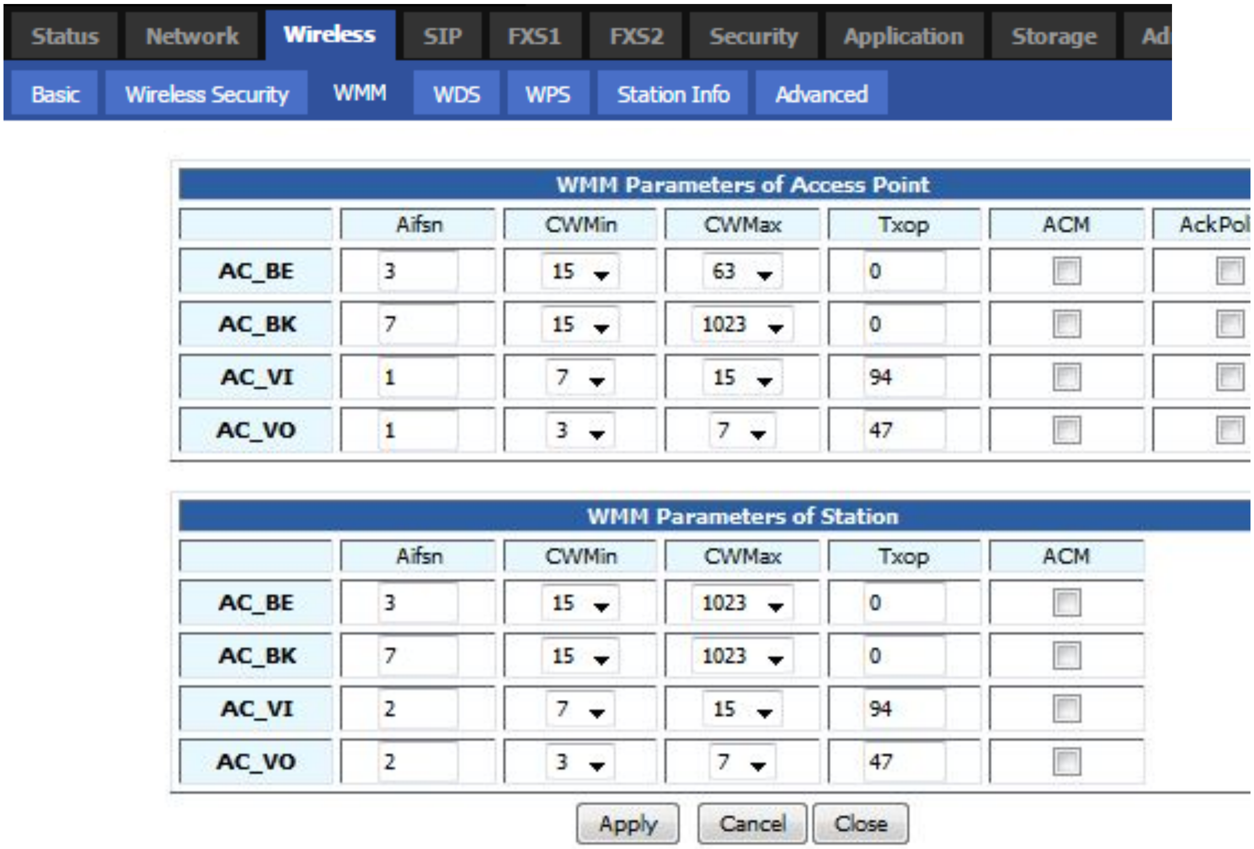
Field Name	Description
Access policy	Wireless access control is used to allow or prohibit the specified client to access to your wireless network based on the MAC address.
Policy	**Disable** : Prohibition: wireless access control policy. **Allow**: only allow the clients in the list to access. **Rejected**: block the clients in the list to access.
Add a station MAC	Enter the MAC address of the clients which you want to allow or prohibit

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.

WMM

Table 41 WMM



WMM Parameters of Access Point

	Aifsn	CWMin	CWMax	Txop	ACM	AckPol
AC_BE	3	15	63	0	□	□
AC_BK	7	15	1023	0	□	□
AC_VI	1	7	15	94	□	□
AC_VO	1	3	7	47	□	□

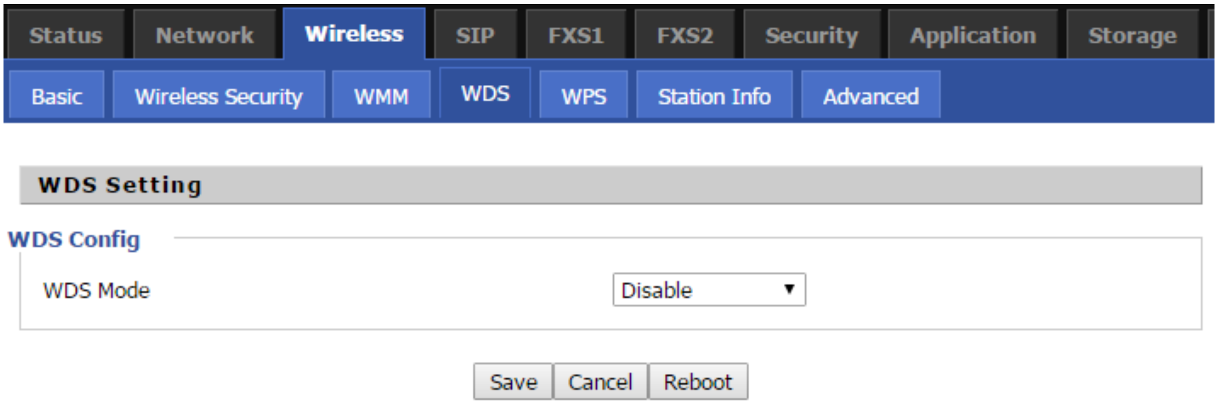
WMM Parameters of Station

	Aifsn	CWMin	CWMax	Txop	ACM
AC_BE	3	15	1023	0	□
AC_BK	7	15	1023	0	□
AC_VI	2	7	15	94	□
AC_VO	2	3	7	47	□

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 42 WDS



WDS Setting

WDS Config

WDS Mode: Disable

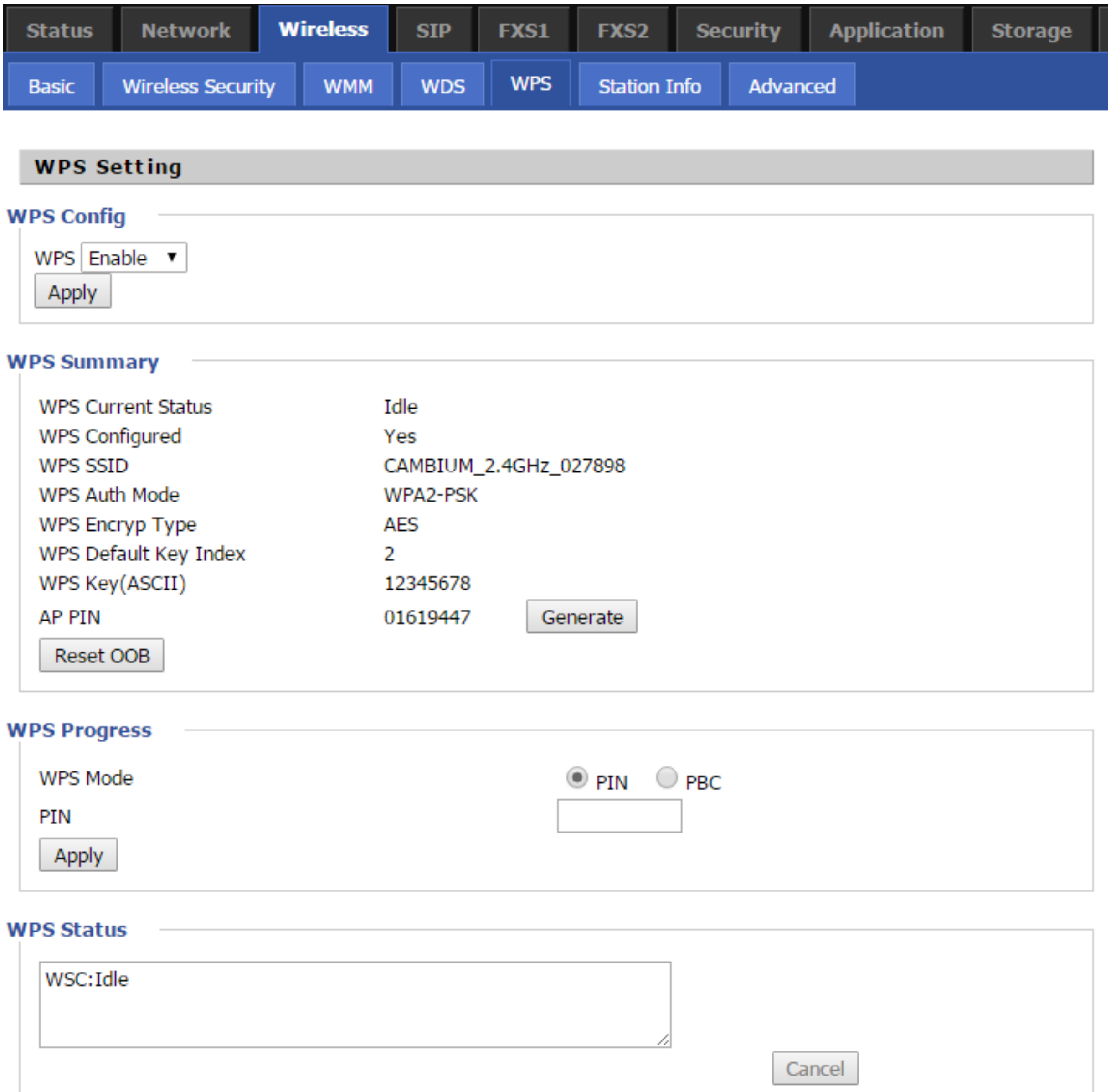
Description
WDS stands for Wireless Distribution System, enabling WDS access points to be interconnected to expand a wireless network.

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 43 WPS



WPS Setting

WPS Config

WPS: Enable

WPS Summary

WPS Current Status	Idle
WPS Configured	Yes
WPS SSID	CAMBIUM_2.4GHz_027898
WPS Auth Mode	WPA2-PSK
WPS Encryp Type	AES
WPS Default Key Index	2
WPS Key(ASCII)	12345678
AP PIN	01619447

WPS Progress

WPS Mode: ● PIN ○ PBC

PIN:

WPS Status

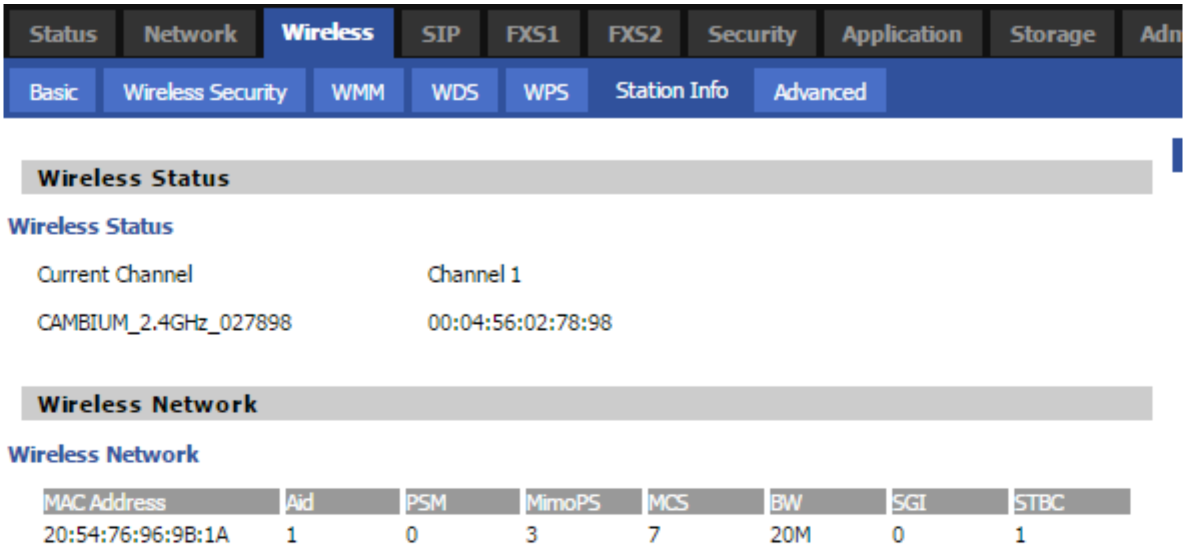
WSC:Idle

Field Name	Description
WPS Setting	Enable/Disable WPS function
WPS Summary	Display the current status of WPS, including current state, SSSID name, authentication methods, encryption type and the PIN code of this AP.
Generate	Generate a new PIN code
Reset OOB	CnPilot Home R200x uses default security policy to allow other non-WPS users to access and apply.
WPS Mode	• ***PIN***: *Enter the PIN code of the wireless device which accesses to this LAN in the following option, and press apply. Then CnPilot Home R200x begins to send signals, turn on the PIN accessing method on the clients,*

	and then it can access the wireless AP automatically. • ***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.*
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 44 Station info



Wireless Status

Wireless Status

Current Channel Channel 1

CAMBIUM_2.4GHz_027898 00:04:56:02:78:98

Wireless Network

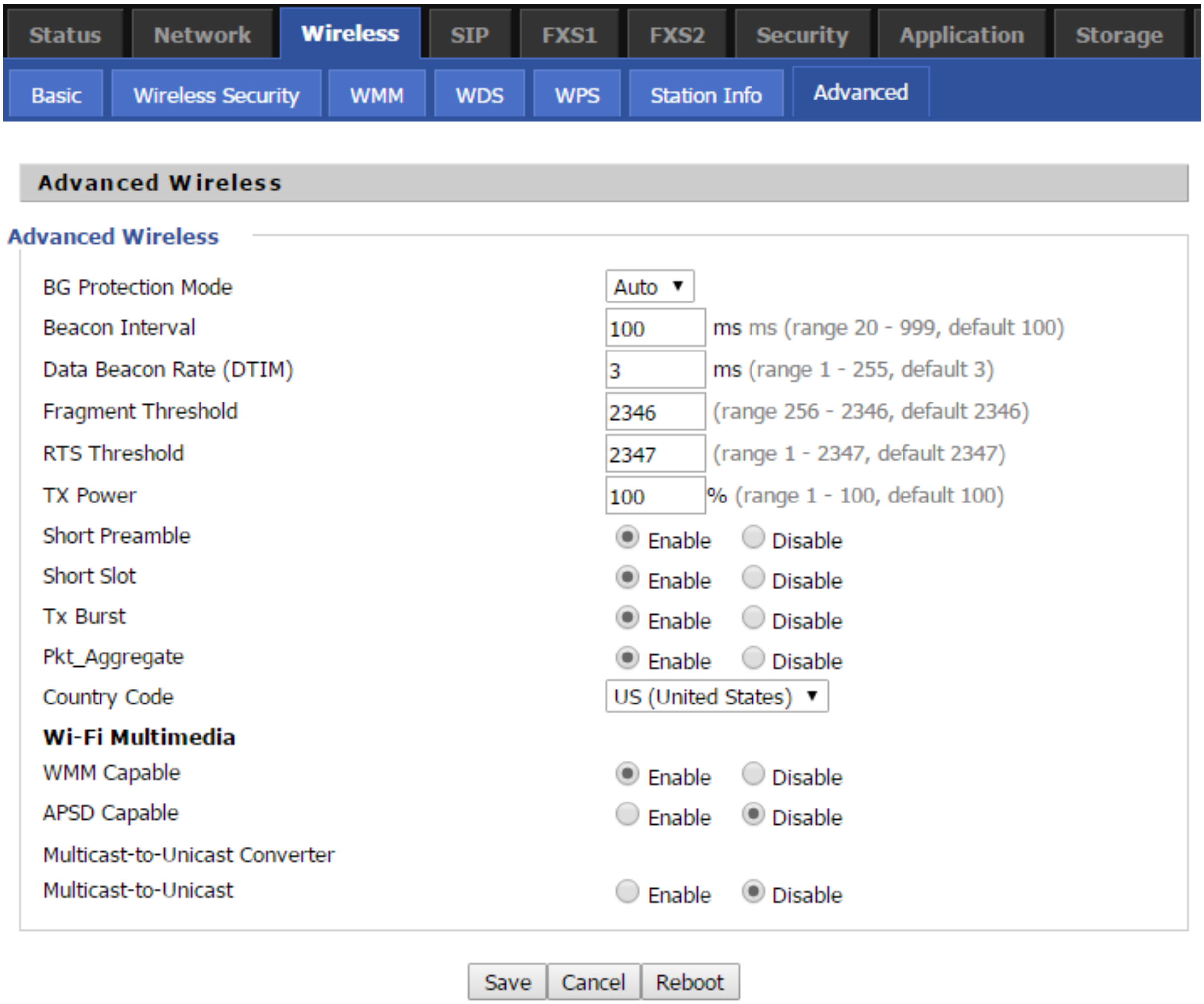
Wireless Network

MAC Address	Aid	PSM	MimoPS	MCS	BW	SGI	STBC
20:54:76:96:9B:1A	1	0	3	7	20M	0	1

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

Advanced

Table 45 Advanced



Advanced Wireless

Advanced Wireless

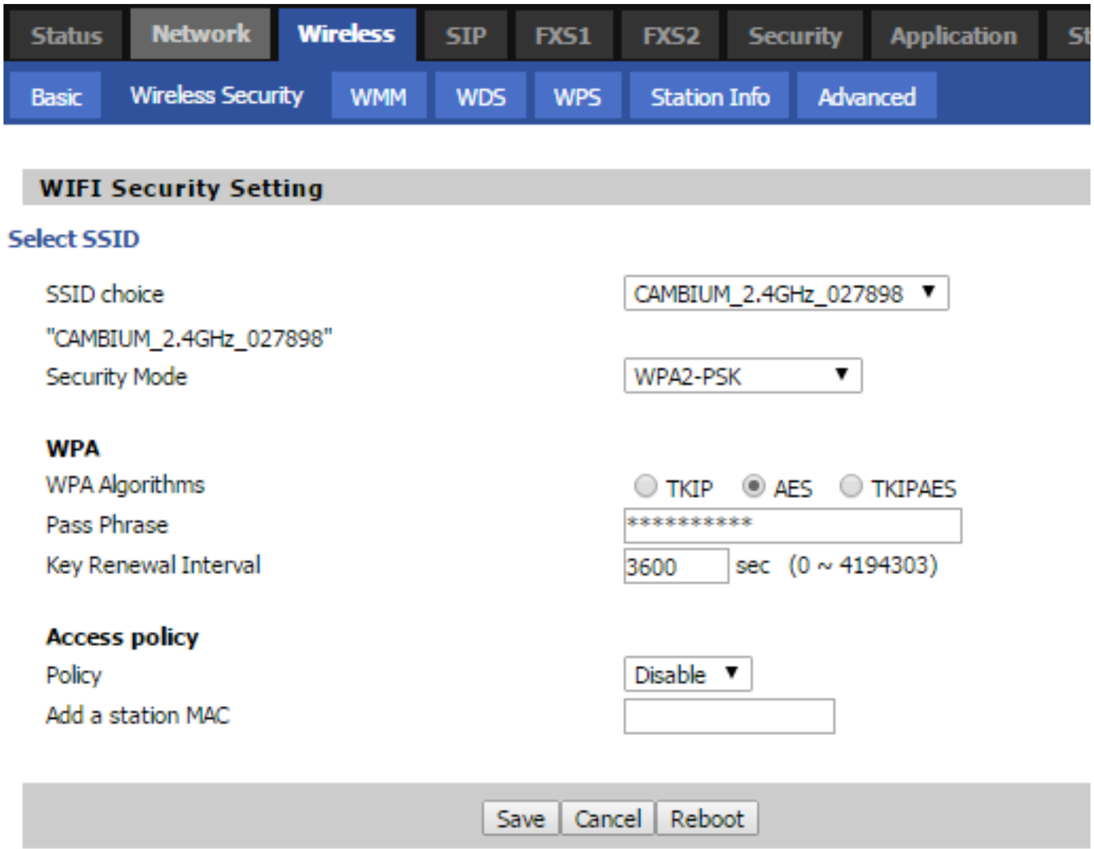
BG Protection Mode	Auto ▼
Beacon Interval	100 ms ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	3 ms (range 1 - 255, default 3)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	100 % (range 1 - 100, default 100)
Short Preamble	● Enable ○ Disable
Short Slot	● Enable ○ Disable
Tx Burst	● Enable ○ Disable
Pkt_Aggregate	● Enable ○ Disable
Country Code	US (United States) ▼
Wi-Fi Multimedia	
WMM Capable	● Enable ○ Disable
APSD Capable	○ Enable ● Disable
Multicast-to-Unicast Converter	
Multicast-to-Unicast	○ 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	Default is enable, CnPilot Home R200x system is not compatible with traditional IEEE802.11, the operation rate can be 1,2Mpbs
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.
IEEE802.11H support	Enable/Disable IEEE802.11H Support. By default, it is disabled.
Country Code	Select country code, options are CN, US, JP, FR, TW, IE, HK and NONE.
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 WMM Configuration, 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 Security

Table 46 Wireless security



WIFI Security Setting

Select SSID

SSID choice	CAMBIUM_2.4GHz_027898 ▼
"CAMBIUM_2.4GHz_027898"	
Security Mode	WPA2-PSK ▼
WPA	
WPA Algorithms	○ TKIP ● AES ○ TKIPAES
Pass Phrase	**********
Key Renewal Interval	3600 sec (0 ~ 4194303)
Access policy	
Policy	Disable ▼
Add a station MAC	

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.

For different encryption mode, the web interface will be different, user can configure the corresponding parameters under the mode you select. See section

STBC	Space-time Block Code **Enabled**: Multiple copies of signals are transmitted to increase the chance of successful delivery **Disabled**: STBC is not employed for signal transmission
Aggregation MSDU (A-	**Enabled**: Allows the device to aggregate multiple Ethernet frames

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

Wireless Security.

WMM

See *WMM.*

WDS

See *WDS.*

WPS

See *WPS*.

Station Info

See *Station Info*.

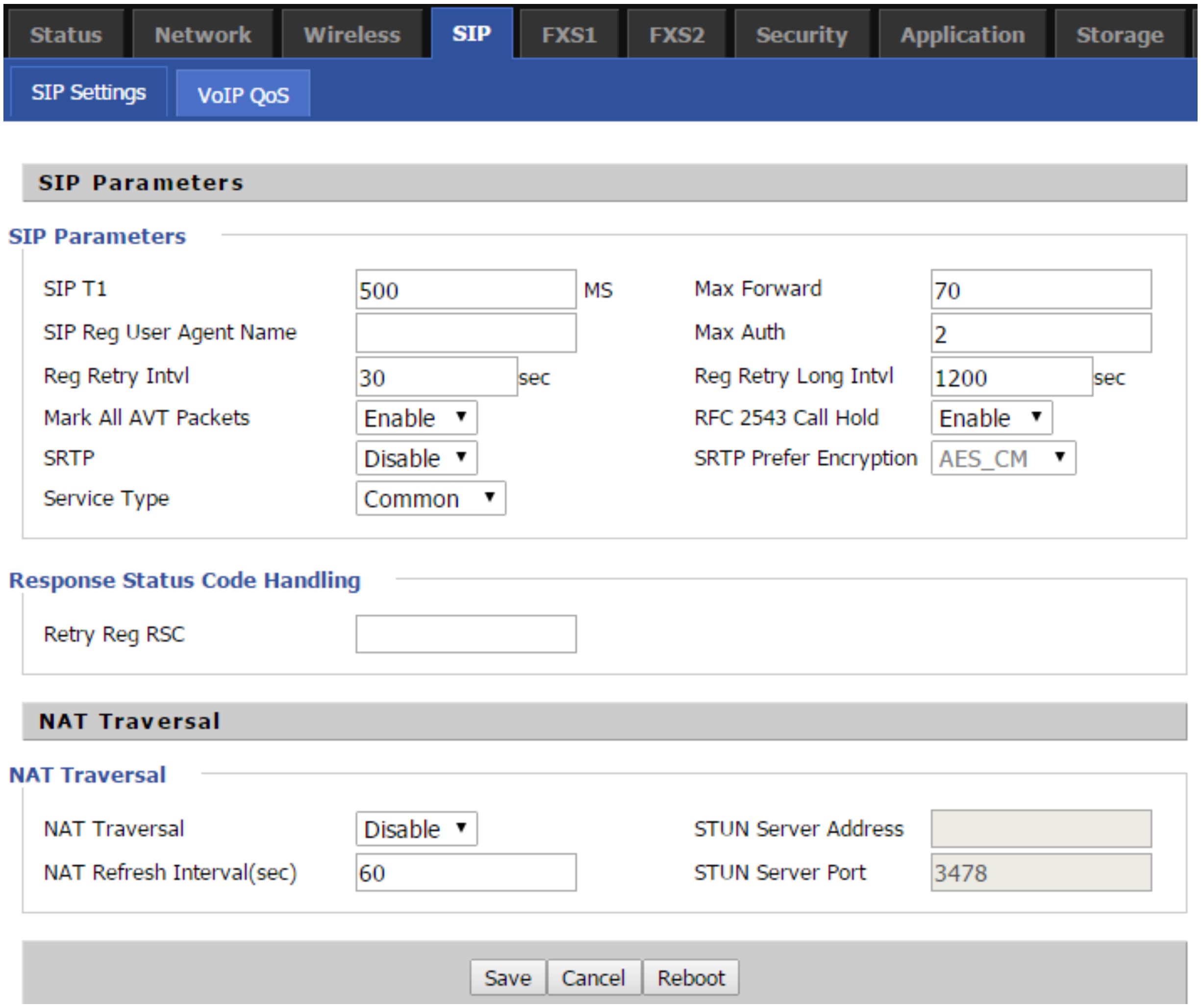
Advanced

See *Advanced*.

SIP

SIP Settings

Table 47 SIP settings



SIP Parameters

SIP Parameters

SIP T1	500 MS	Max Forward	70
SIP Reg User Agent Name		Max Auth	2
Reg Retry Intvl	30 sec	Reg Retry Long Intvl	1200 sec
Mark All AVT Packets	Enable	RFC 2543 Call Hold	Enable
SRTP	Disable	SRTP Prefer Encryption	AES_CM
Service Type	Common		

Response Status Code Handling

Retry Reg RSC	

NAT Traversal

NAT Traversal

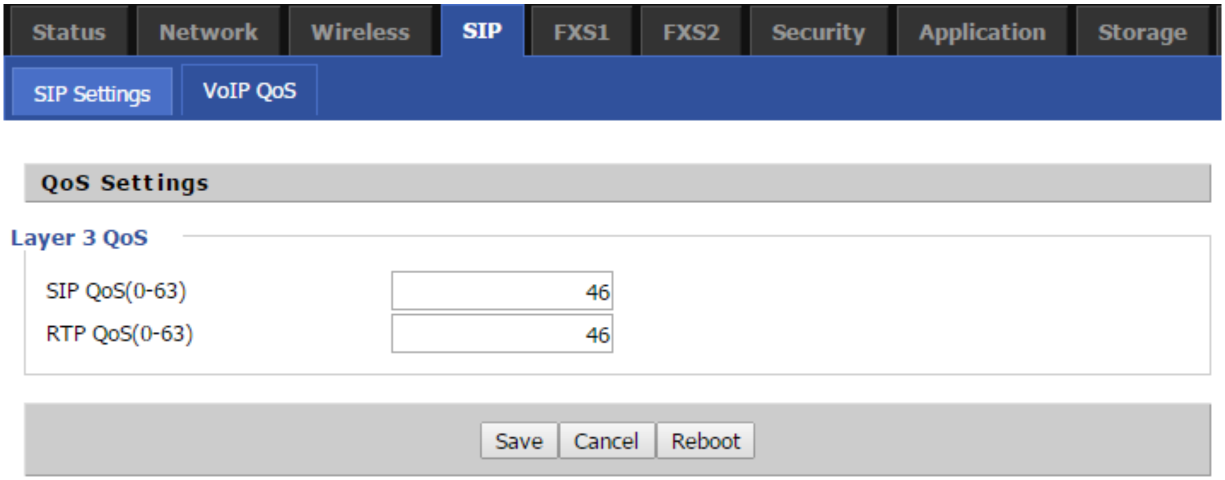
NAT Traversal	Disable	STUN Server Address	
NAT Refresh Interval(sec)	60	STUN Server Port	3478

Field Name	Description
SIP T1	The minimum scale of retransmission time
Max Forward	SIP contains Max Forward message header fields used to limit the requests for forwards.
SIP Reg User Agent Name	The agent name of SIP registered user
Max Auth	The maximum number of retransmissions
Mark All AVT Packets	Voice packet marking to enable this item will see the mark on the voice message when the call environment changed (such as press a key during

	the call)
RFC 2543 Call Hold	Enable the Connection Information field displays the address is 0.0.0.0 in the invite message of Hold. Disable the Connection Information field displays the device IP address in the invite message of Hold.
SRTP	Whether to enable the call packet encryption function
SRTP Prefer Encryption	The preferred encryption type of calling packet (the Message body of INVITE Message)
Service Type	Choose the server type
NAT Traversal	1. Enable/Disable NAT Traversal 2. cnPilot Home R200x/R201x 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 48 VoIP QoS



QoS Settings

Layer 3 QoS

SIP QoS(0-63) 46

RTP QoS(0-63) 46

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

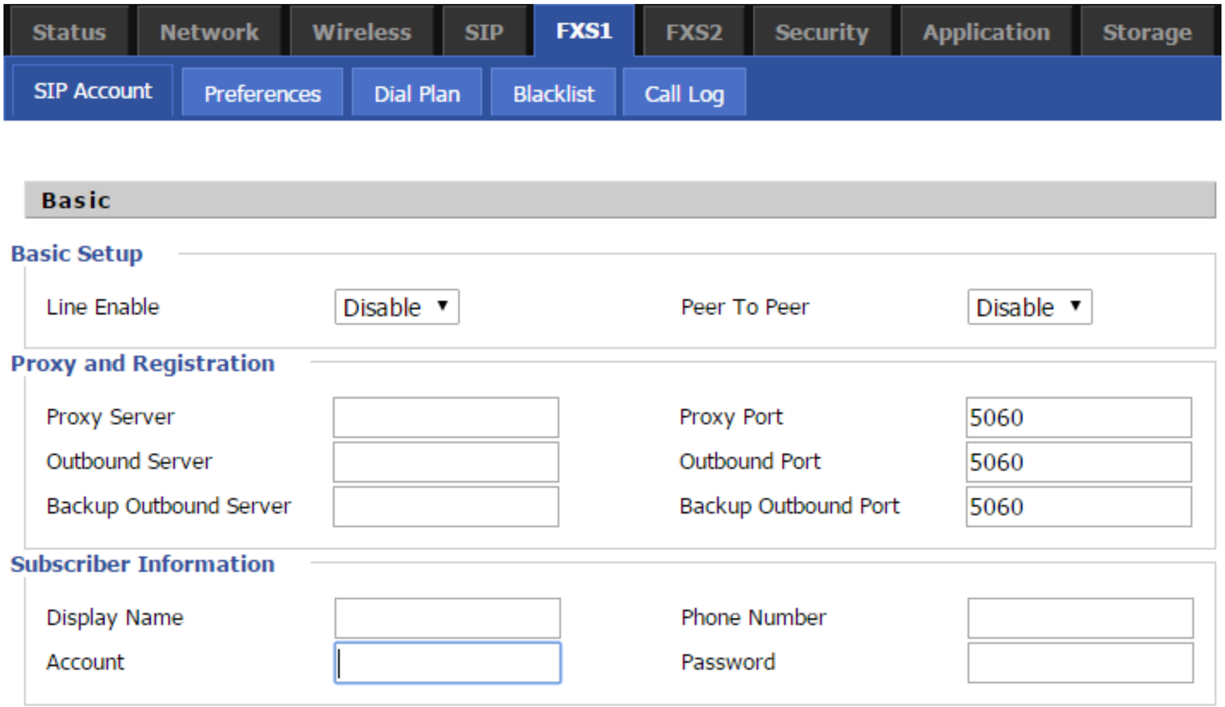
FXS1

SIP Account

Basic

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

Table 49 SIP Account – Basic



Basic

Basic Setup

Line Enable	Disable ▼	Peer To Peer	Disable ▼

Proxy and Registration

Proxy Server		Proxy Port	5060
Outbound Server		Outbound Port	5060
Backup Outbound Server		Backup Outbound Port	5060

Subscriber Information

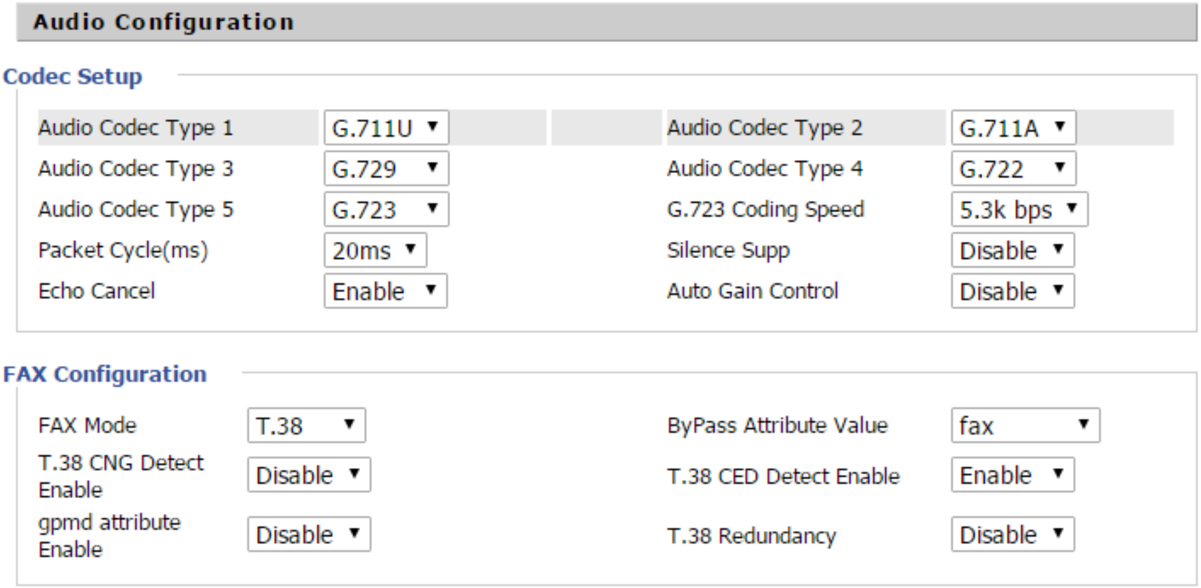
Display Name		Phone Number	
Account		Password	

Field Name	Description
Line Enable	Enable/Disable the line.
Peer To Peer	Enable/Disable PEER to PEER. If enabled, SIP-1 will not send register request to SIP server; but in Status/ SIP Account Status webpage, Status is Registered; lines 1 can dial out, but the external line number cannot dialed line1.
Proxy Server	The IP address or the domain of SIP Server
Outbound Server	The IP address or the domain of Outbound Server
Backup Outbound 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 50 Audio configuration



Audio Configuration

Codec Setup

Audio Codec Type 1	G.711U	Audio Codec Type 2	G.711A
Audio Codec Type 3	G.729	Audio Codec Type 4	G.722
Audio Codec Type 5	G.723	G.723 Coding Speed	5.3k bps
Packet Cycle(ms)	20ms	Silence Supp	Disable
Echo Cancel	Enable	Auto Gain Control	Disable

FAX Configuration

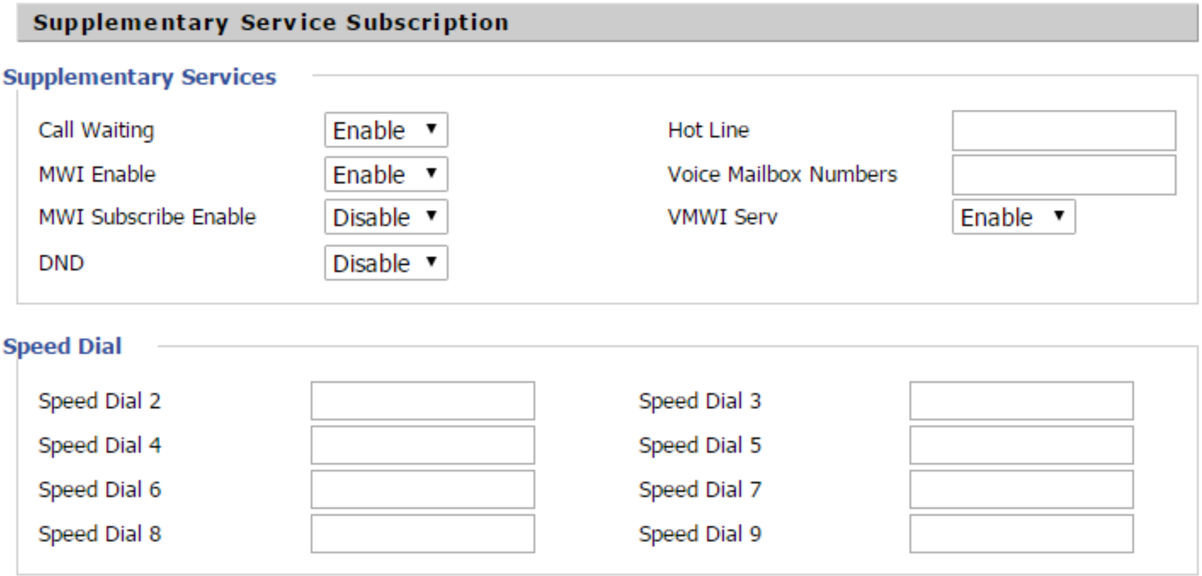
FAX Mode	T.38	ByPass Attribute Value	fax
T.38 CNG Detect Enable	Disable	T.38 CED Detect Enable	Enable
gpmd attribute Enable	Disable	T.38 Redundancy	Disable

Field Name	Description
Audio Codec Type1	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type2	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type3	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type4	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
Audio Codec Type5	Choose the audio codec type from G.711U, G.711A, G.722, G.729, G.723
G.723 Coding Speed	Choose the speed of G.723 from 5.3kbps and 6.3kbps
Packet Cycle	The RTP packet cycle time, default is 20ms

Silence Supp	Enable/Disable silence support.
Echo Cancel	Enable/Disable echo cancel. By default, it is enabled.
Auto Gain Control	Enable/Disable auto gain.
T.38 Enable	Enable/Disable T.38
T.38 Redundancy	Enable/Disable T.38 Redundancy
T.38 CNG Detect Enable	Enable/Disable T.38 CNG Detect
gpmd attribute Enable	Enable/Disable gpmd attribute.

Supplementary Service Subscription

Table 51 Supplementary service



Supplementary Service Subscription

Supplementary Services

Call Waiting: Enable ▼
MWI Enable: Enable ▼
MWI Subscribe Enable: Disable ▼
DND: Disable ▼
Hot Line:
Voice Mailbox Numbers:
VMWI Serv: Enable ▼

Speed Dial

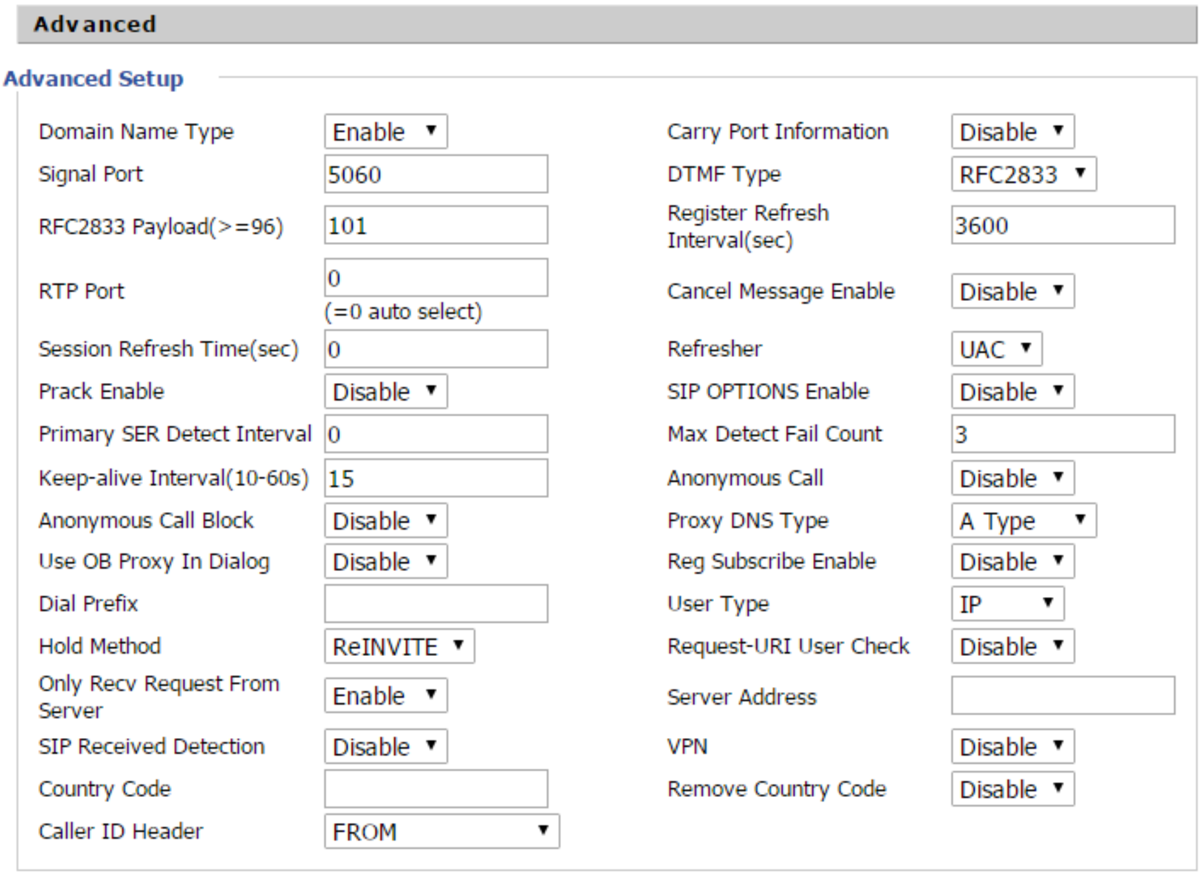
Speed Dial 2:
Speed Dial 3:
Speed Dial 4:
Speed Dial 5:
Speed Dial 6:
Speed Dial 7:
Speed Dial 8:
Speed Dial 9:

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 52 Advanced



Advanced

Advanced Setup

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

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.
RFC2833 Payload(>=96)	User can use the default setting.
Register Refresh	The interval between two normal Register messages. You can use the

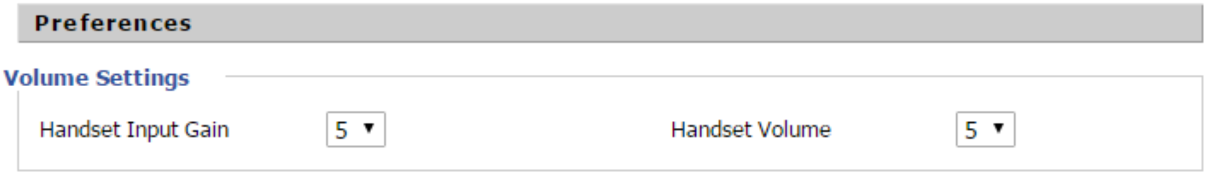
Interval	default setting.
RTP Port	Set the port to send RTP. The device will select one idle port for RTP if you set “0”; otherwise use the value which user sets.
Cancel Message Enable	When you set enable, an unregistered message will be sent before registration, while you set disable, unregistered message 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 53 Volume settings



Preferences

Volume Settings

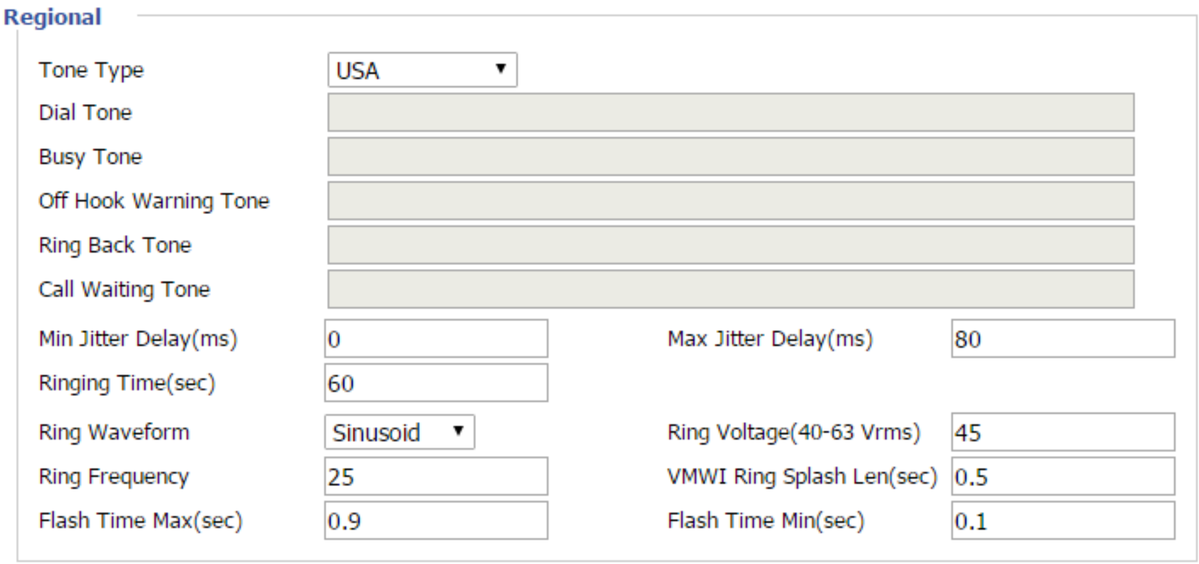
Handset Input Gain: 5

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 54 Regional



Regional

Tone Type: USA

Dial Tone:

Busy Tone:

Off Hook Warning Tone:

Ring Back Tone:

Call Waiting Tone:

Min Jitter Delay(ms): 0

Max Jitter Delay(ms): 80

Ringing Time(sec): 60

Ring Waveform: Sinusoid

Ring Voltage(40-63 Vrms): 45

Ring Frequency: 25

VMWI Ring Splash Len(sec): 0.5

Flash Time Max(sec): 0.9

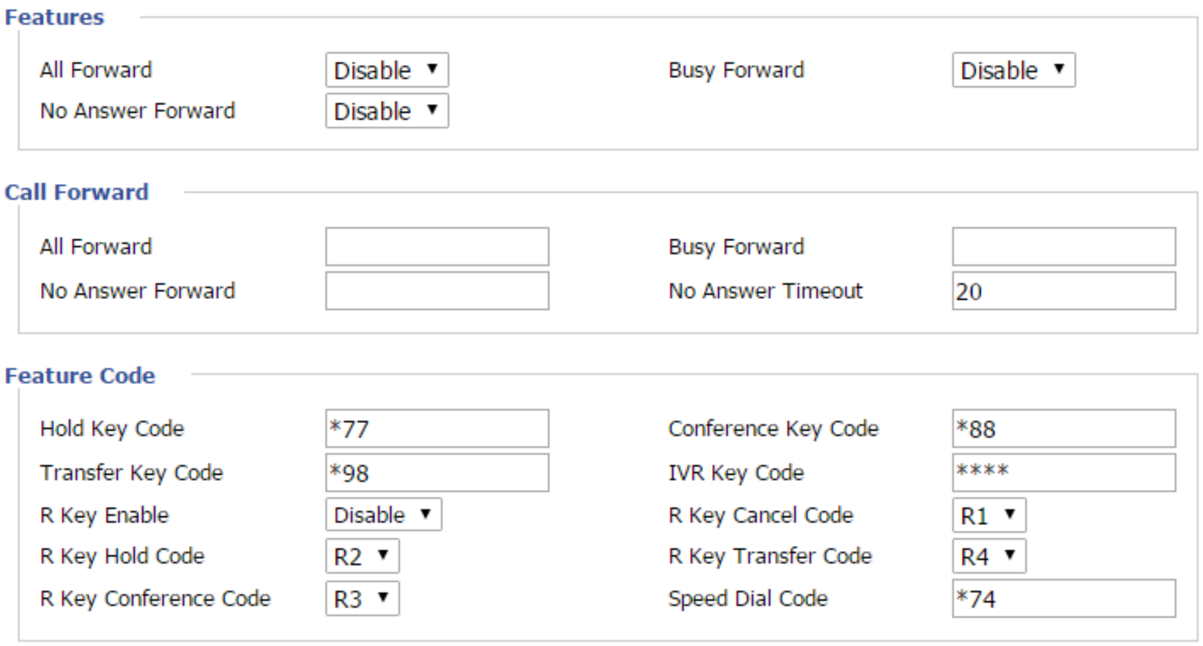
Flash Time Min(sec): 0.1

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	Off Hook warning tone

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 CnPilot Home R200x 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 55 Features and call forward



Features

All Forward: Disable ▼
Busy Forward: Disable ▼
No Answer Forward: Disable ▼

Call Forward

All Forward:
Busy Forward:
No Answer Forward:
No Answer Timeout: 20

Feature Code

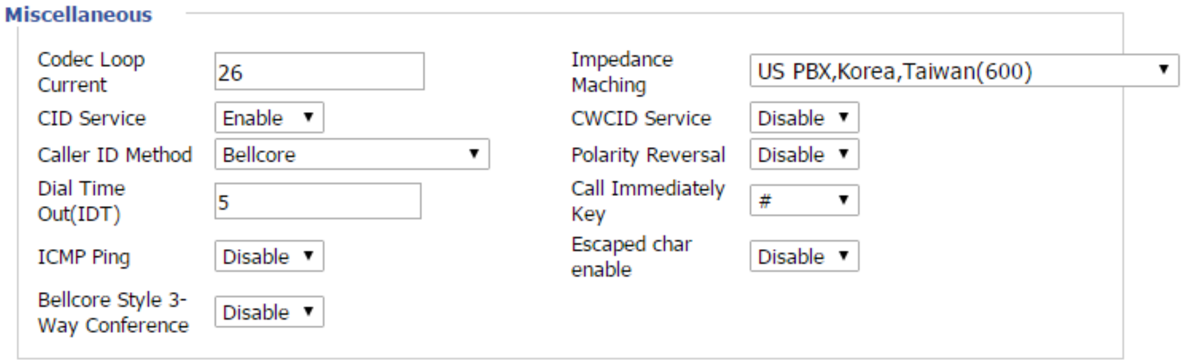
Hold Key Code: *77
Conference Key Code: *88
Transfer Key Code: *98
IVR Key Code: ****
R Key Enable: Disable ▼
R Key Cancel Code: R1 ▼
R Key Hold Code: R2 ▼
R Key Transfer Code: R4 ▼
R Key Conference Code: R3 ▼
Speed Dial Code: *74

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

Miscellaneous

Table 56 Miscellaneous



Miscellaneous

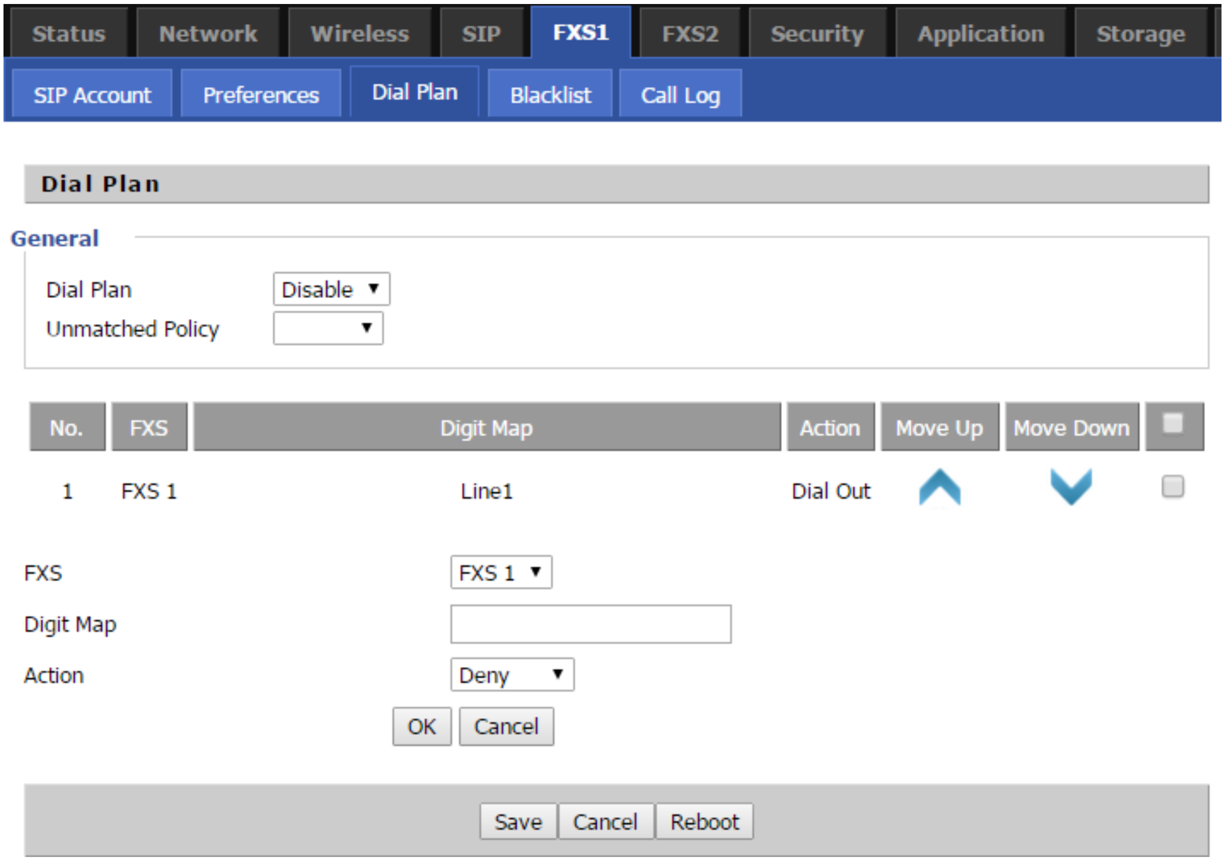
Codec Loop Current	26	Impedance Maching	US PBX,Korea,Taiwan(600)
CID Service	Enable	CWCID Service	Disable
Caller ID Method	Bellcore	Polarity Reversal	Disable
Dial Time Out(IDT)	5	Call Immediately Key	#
ICMP Ping	Disable	Escaped char enable	Disable
Bellcore Style 3-Way Conference	Disable		

Field Name	Description
Codec Loop Current	Set off-hook loop current, default is 26
Impedance Maching	Set impedance matching, default is US PBX,Korea,Taiwan(600).
CID service	Enable/Disable displaying caller ID; If enable, caller ID is displayed when there is an incoming call or it won't be displayed. Default is 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 cnPilot Home will sound dial out tone when cnPilot Home 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 #

Dial Plan

Parameters and Settings

Table 57 Parameters and settings



Dial Plan

General

Dial Plan: Disable

Unmatched Policy:

No.	FXS	Digit Map	Action	Move Up	Move Down	□
1	FXS 1	Line1	Dial Out	⌃	⌄	□

FXS: FXS 1

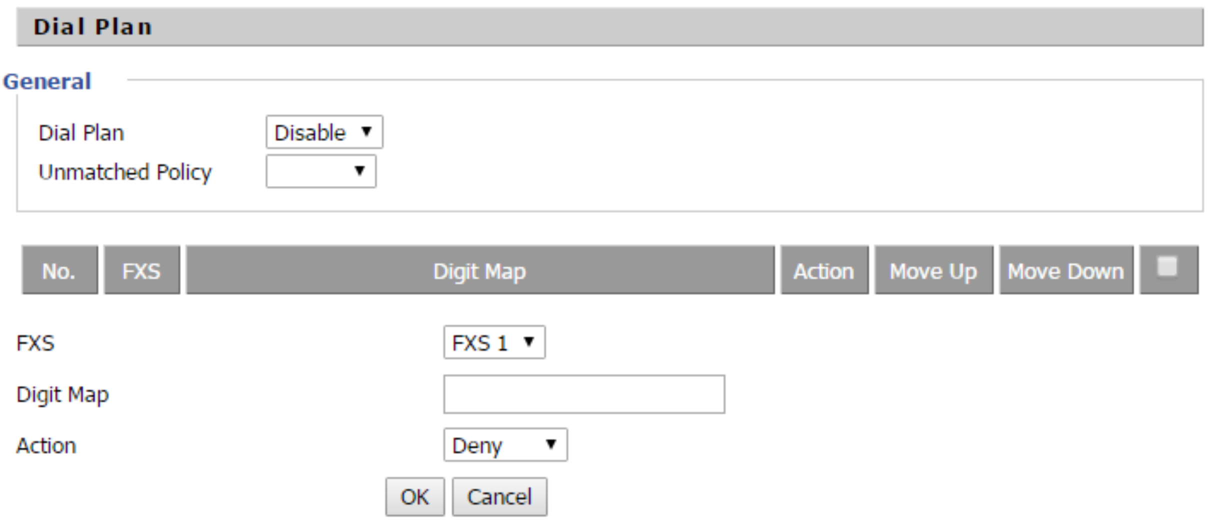
Digit Map:

Action: Deny

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 CnPilot Home will reject the matched number, while Dial Out means CnPilot Home 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 58 Adding one dial plan



Dial Plan: Disable

Unmatched Policy:

FXS: FXS 1

Digit Map:

Action: Deny

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 59 Dial Plan

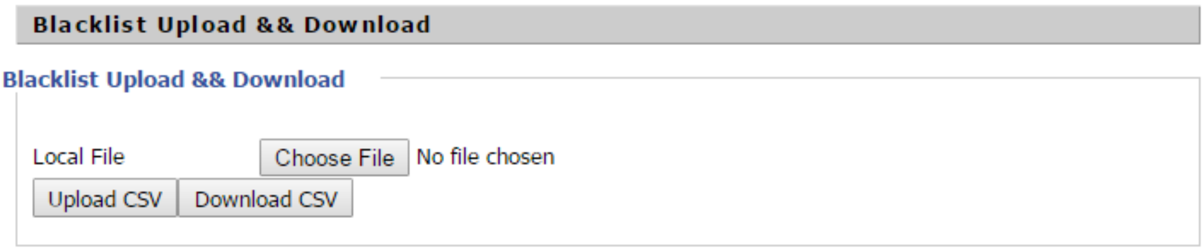
No.	String	Description
1	0 1 2 3 4 5 6 7 8 9 * #	Allowed characters
2	x	Lowercase letter x stands for one legal character
3	[sequence]	To match one character form sequence. For example: *1.* [0-9]: match one digit form 0 to 9 *2.* [23-5*]: match one character from 2 or 3 or 4 or 5 or *
4	x.	Match to x^0, x^1, x^2, x3...... x^n For example: “01.”:can match ”0”, “01”, “011”, ”0111”, ……..,”01111…”
5	<dialed:substituted>	Replace dialed with substituted.

		For example： <8:1650>123456：input is “85551212”, output is“16505551212”
6	x,y	Make outside dial tone after dialing “x”, stop until dialing character “y” For example： “9,1xxxxxxxxxx”:the device reports dial tone after inputting “9”, stops tone until inputting “1” “9,8,010x”: make outside dial tone after inputting “9”, stop tone until inputting “0”
7	T	Set the delayed time. For example: “<9:111>T2”: The device will dial out the matched number “111” after 2 seconds.

Blacklist

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

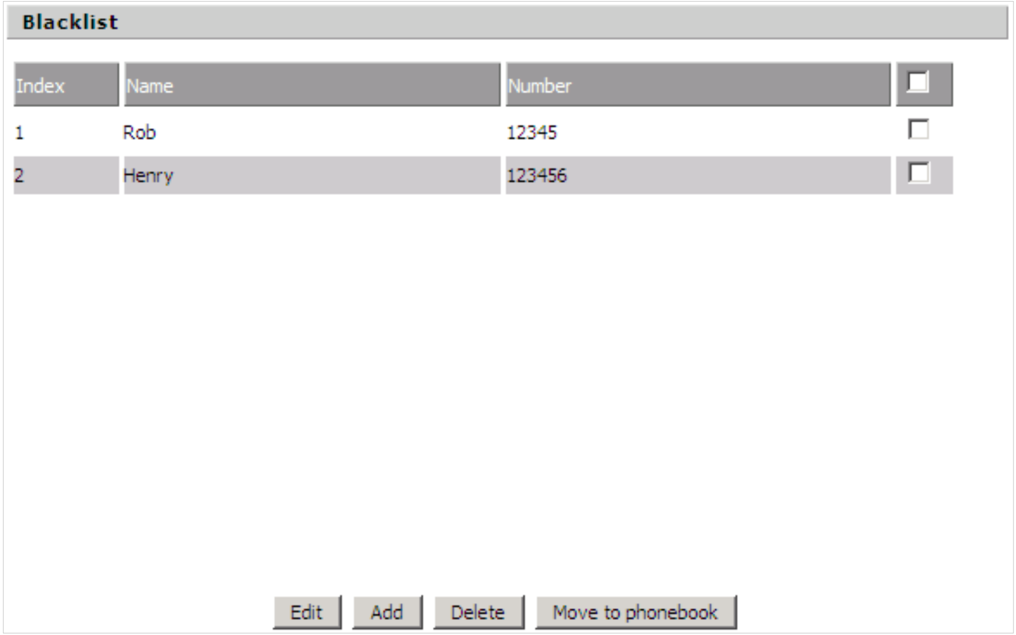
Table 60 Blacklist



Blacklist Upload && Download

Blacklist Upload && Download

Local File: No file chosen



Blacklist

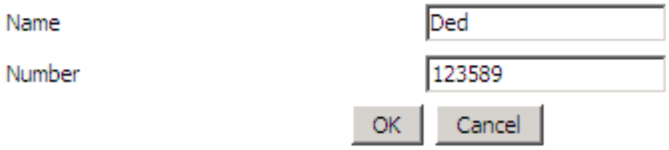
Index	Name	Number	□
1	Rob	12345	□
2	Henry	123456	□

Description

Click 浏览… to select the blacklist file and click upload CSV to upload it to CnPilot Home; 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.

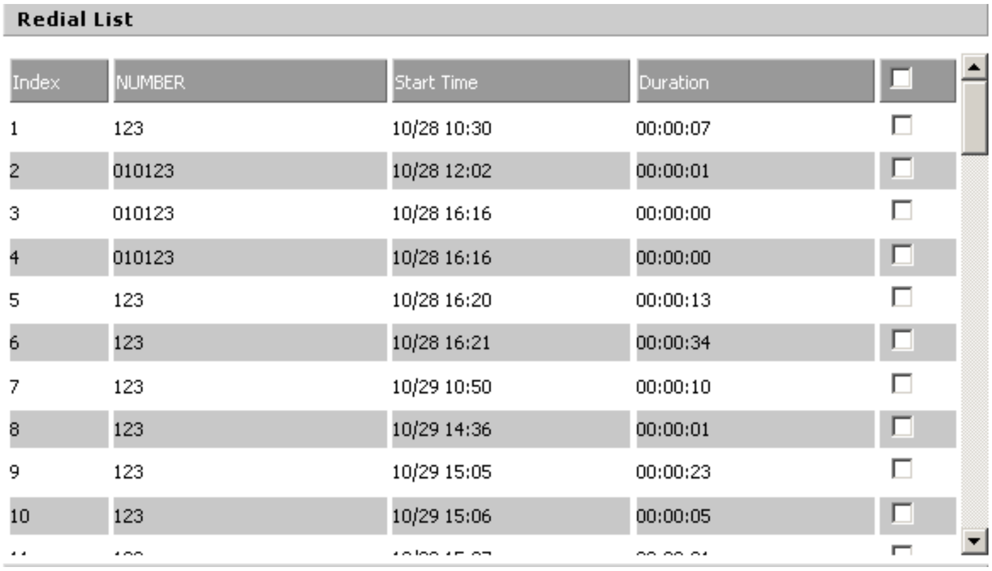


Name	Ded
Number	123589

Call Log

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

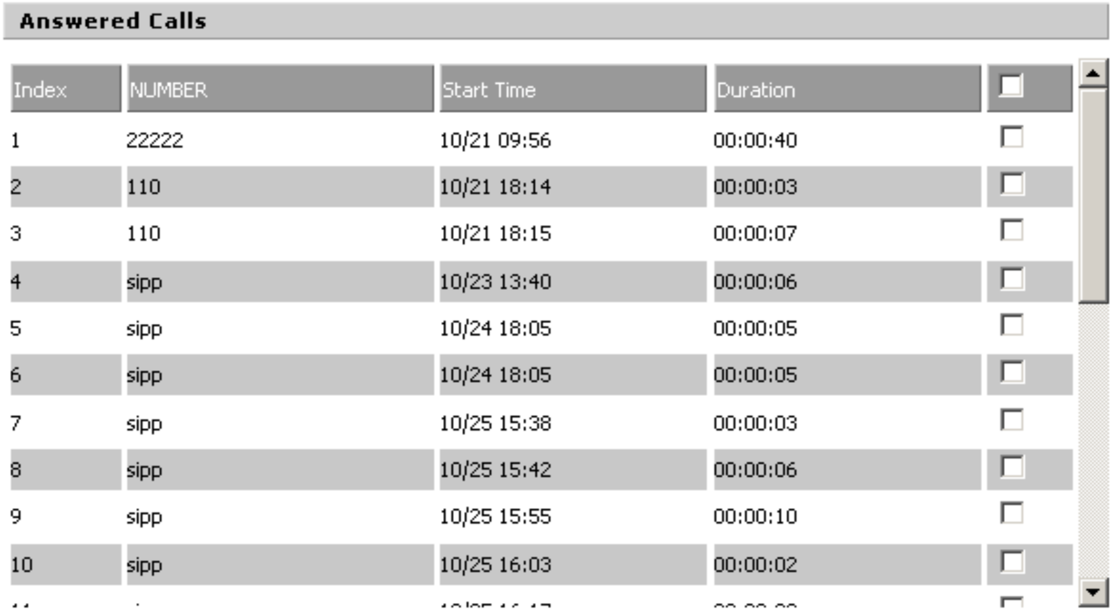
Table 61 Call log



Redial List

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

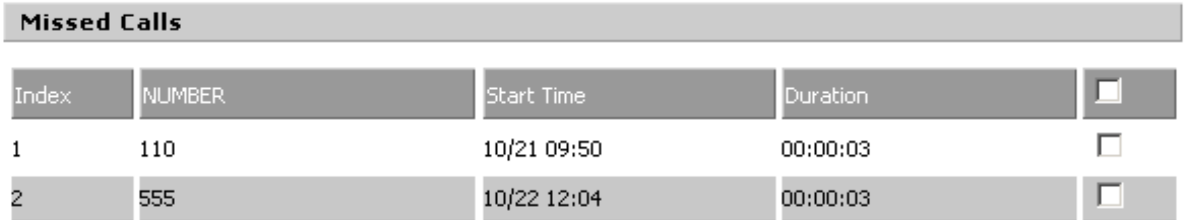
Redial List



Answered Calls

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

Answered Calls



Missed Calls

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

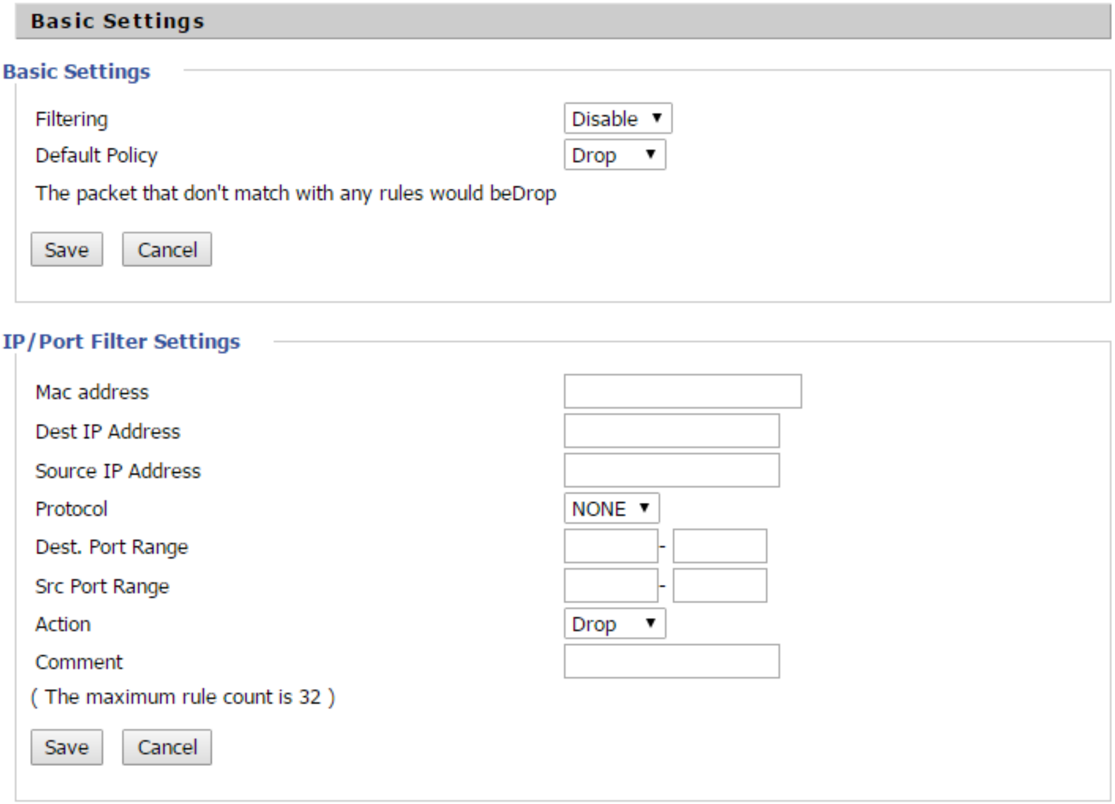
FXS2

The settings of FXS2 are the same as FXS1. See FXS1 on page 3-47.

Security

Filtering Setting

Table 62 Filtering setting



Basic Settings

Basic Settings

Filtering	Disable ▼
Default Policy	Drop ▼

The packet that don't match with any rules would beDrop

IP/Port Filter Settings

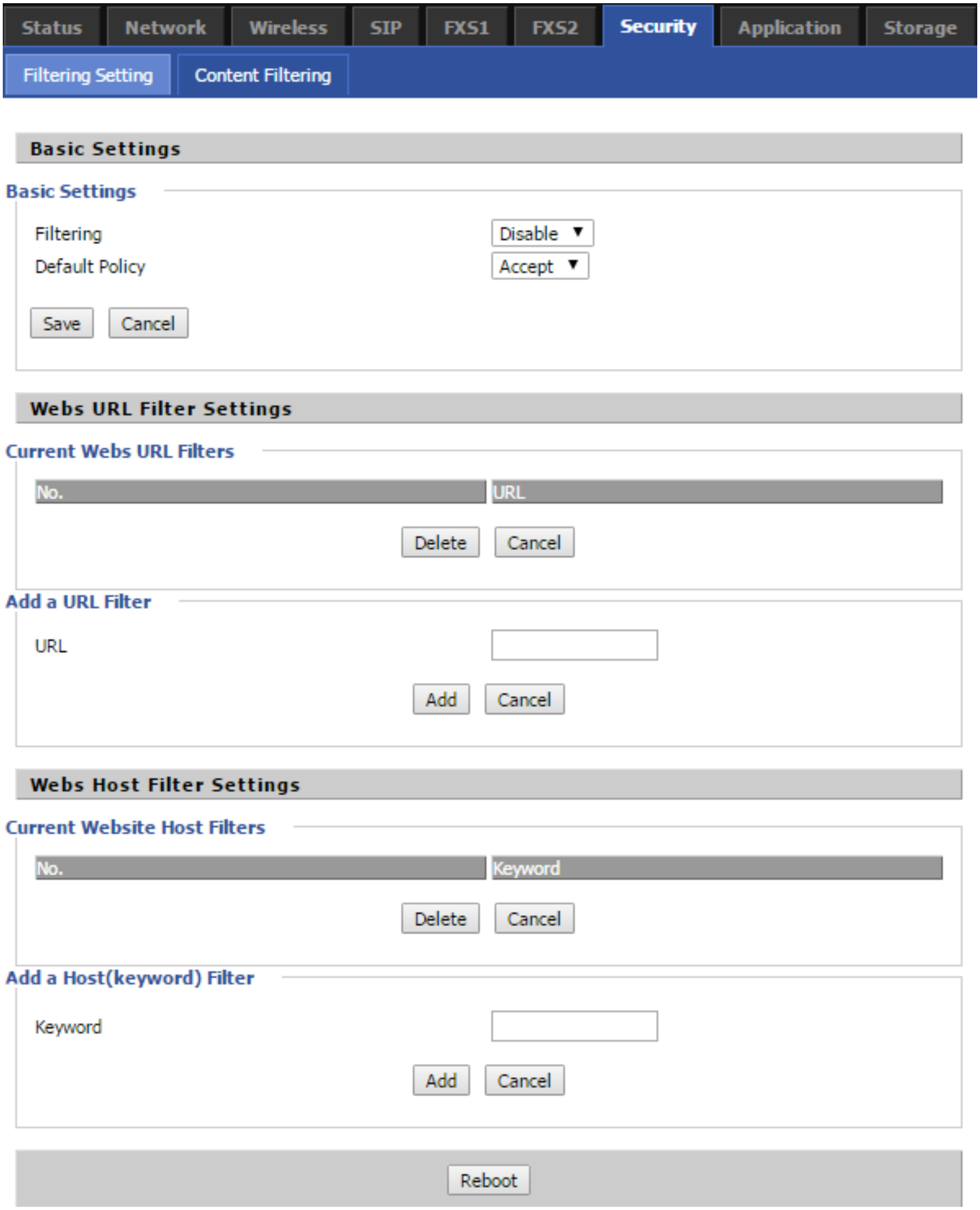
Mac address	
Dest IP Address	
Source IP Address	
Protocol	NONE ▼
Dest. Port Range	-
Src Port Range	-
Action	Drop ▼
Comment	

(The maximum rule count is 32)

Field Name	Description
Filtering	Enable/Disable filter function
Default Policy	Choose to drop or accept filtered MAC addresses
Mac address	Add the Mac address filtering
Dest IP address	Destination IP address
Source IP address	Source IP address
Protocol	Select a protocol name, support for TCP, UDP and TCP/UDP
Dest. Port Range	Destination port ranges
Src Port Range	Source port range
Action	You can choose to receive or give up; this should be consistent with the default policy.
Comment	Add callout
Delete	Delete selected item

Content Filtering

Table 63 Content filtering



Field Name	Description
Filtering	Enable/Disable content Filtering

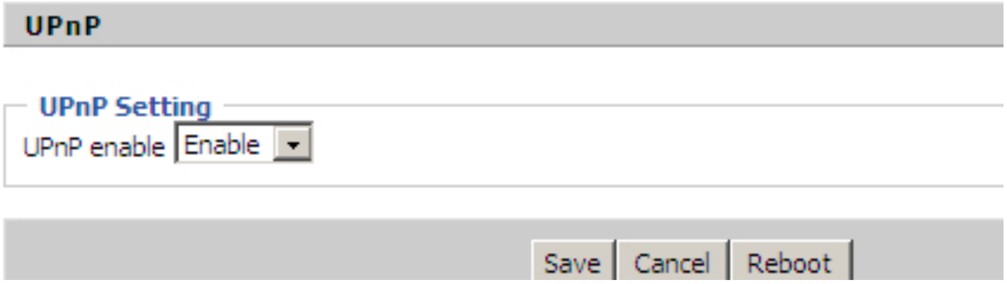
Default Policy	The default policy is to accept or to prohibit filtering rules
Current Webs URL Filters	List the URL filtering rules that already existed (blacklist)
Delete/Cancel	You can choose to delete or cancel the existing filter rules
Add a URL Filter	Add URL filtering rules
Add/Cancel	Click adds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

Application

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 64 UPnP



UPnP

UPnP Setting

UPnP enable: Enable

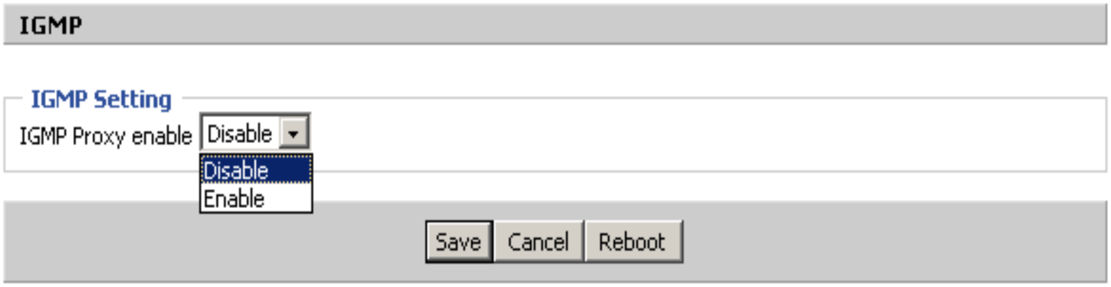
Field Name	Description
UPnP enable	Enable/Disable UPnP function.

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 65 IGMP



IGMP

IGMP Setting

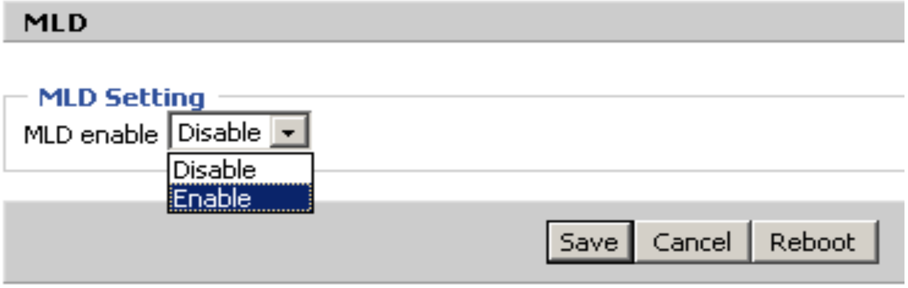
IGMP Proxy enable: Disable

Field Name	Description

IGMP Proxy enable	Enable/Disable IGMP function.

MLD

Table 66 MLD



MLD enable Disable

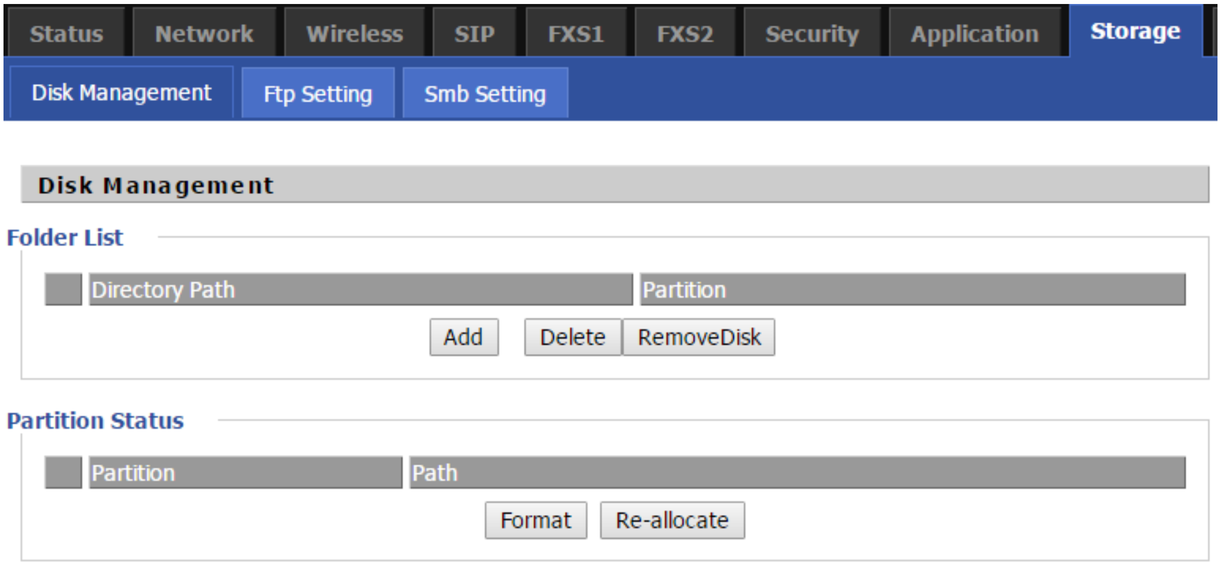
Field Name	Description
MLD enable	Enable/Disable MLD function (Multicast Listener Discovery)

Storage

Disk Management

This page is used to manage the USB storage device.

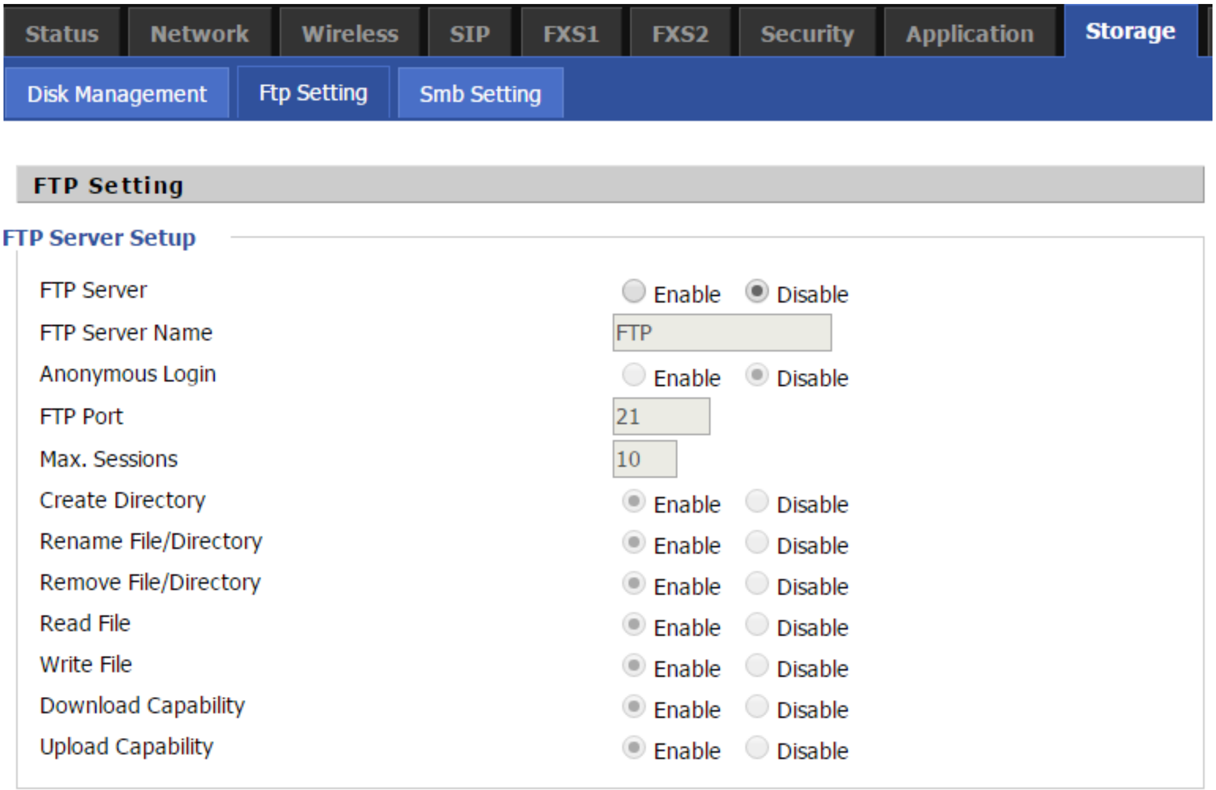
Table 67 Disk Management



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 68 FTP Setting



FTP Setting

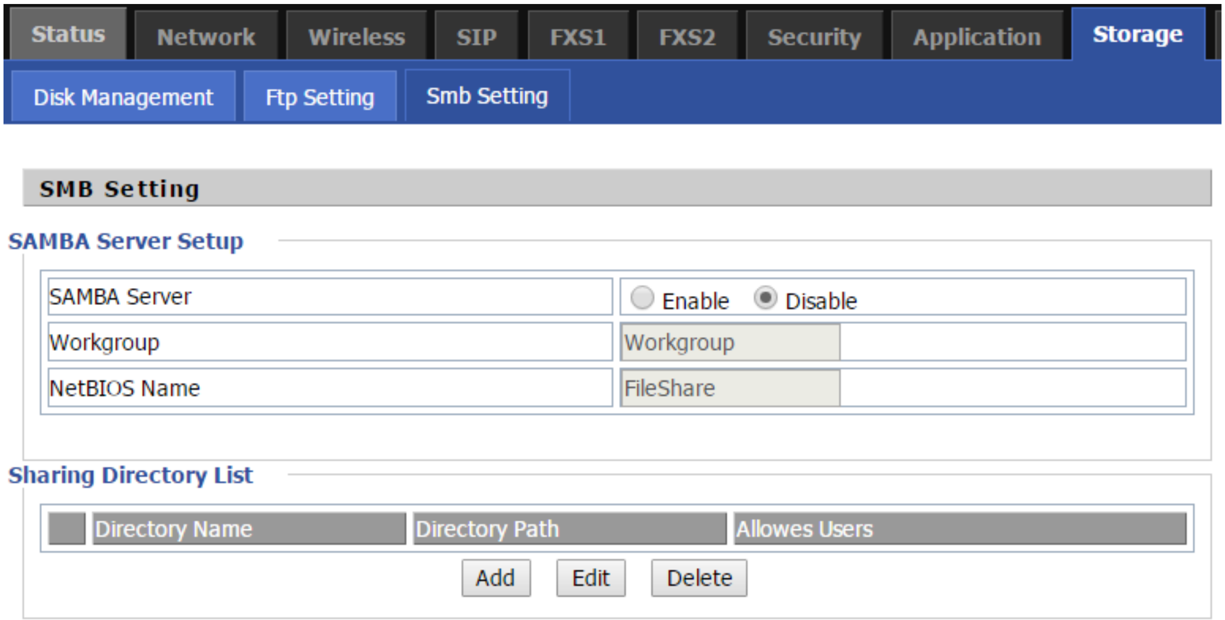
FTP Server Setup

FTP Server	○ Enable ● Disable
FTP Server Name	FTP
Anonymous Login	○ Enable ● Disable
FTP Port	21
Max. Sessions	10
Create Directory	● Enable ○ Disable
Rename File/Directory	● Enable ○ Disable
Remove File/Directory	● Enable ○ Disable
Read File	● Enable ○ Disable
Write File	● Enable ○ Disable
Download Capability	● Enable ○ Disable
Upload Capability	● Enable ○ Disable

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 69 Smb setting



SMB Setting

SAMBA Server Setup

SAMBA Server	○ Enable ● Disable
Workgroup	Workgroup
NetBIOS Name	FileShare

Sharing Directory List

	Directory Name	Directory Path	Allowes Users

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

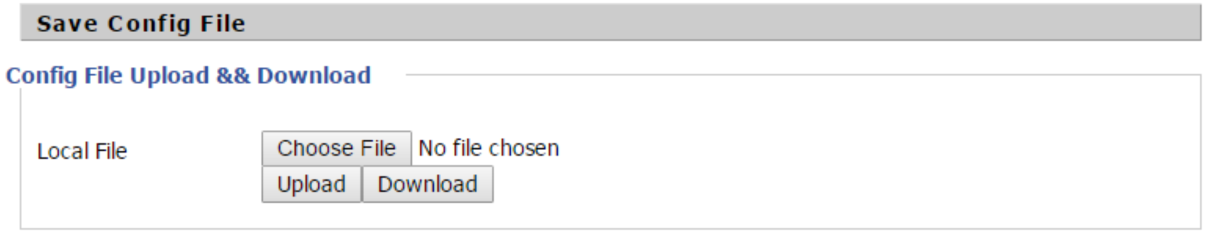
Administration

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

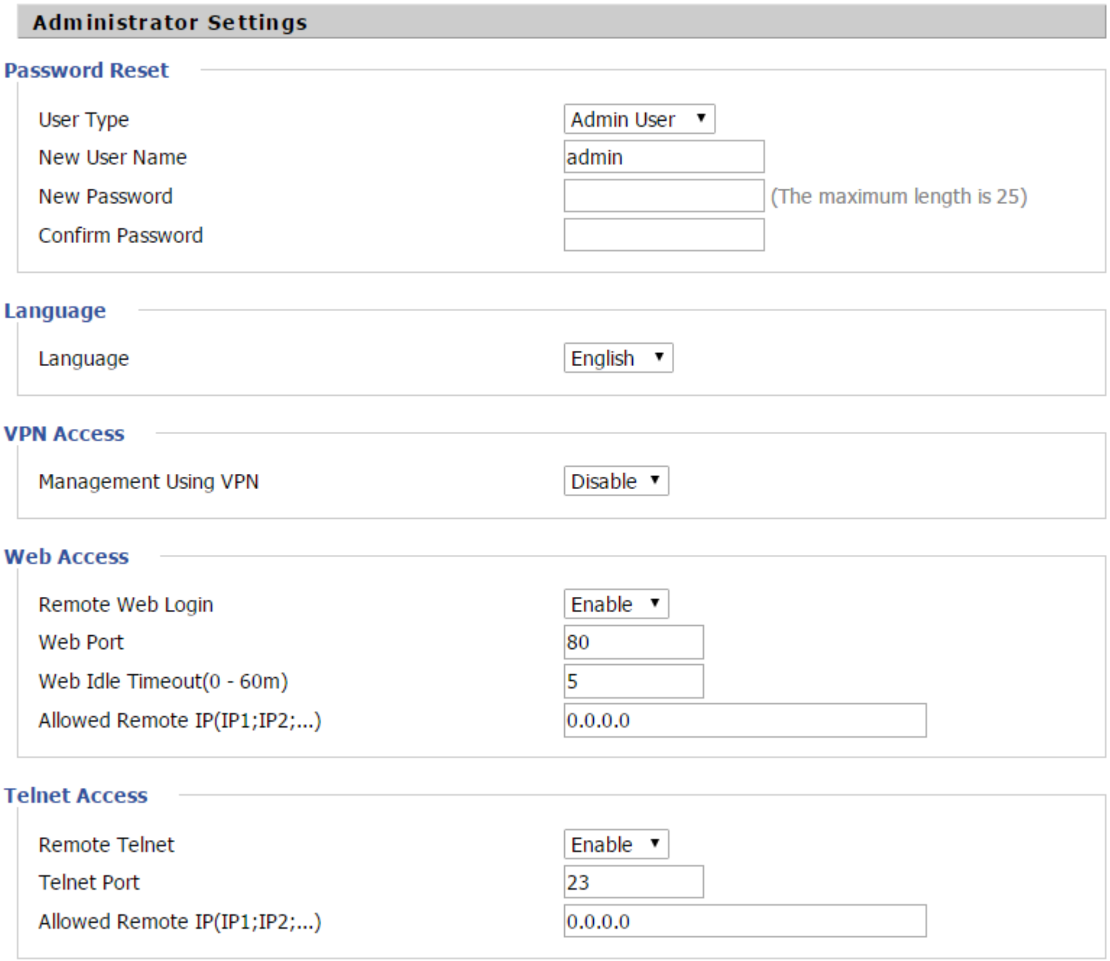
Table 70 Save Config File



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

Administrator settings

Table 71 Administrator settings



Administrator Settings

Password Reset

User Type: Admin User ▼
New User Name: admin
New Password: (The maximum length is 25)
Confirm Password:

Language

Language: English ▼

VPN Access

Management Using VPN: Disable ▼

Web Access

Remote Web Login: Enable ▼
Web Port: 80
Web Idle Timeout(0 - 60m): 5
Allowed Remote IP(IP1;IP2;...): 0.0.0.0

Telnet Access

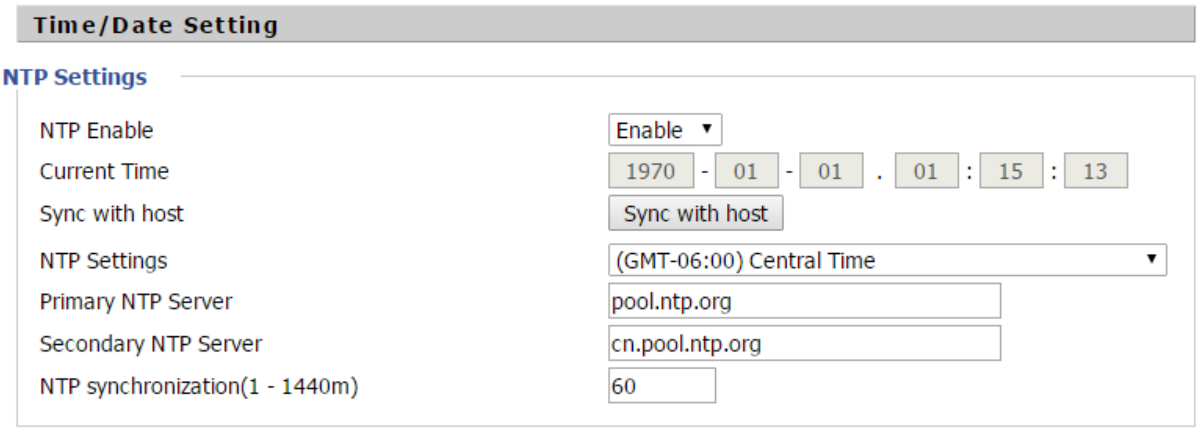
Remote Telnet: Enable ▼
Telnet Port: 23
Allowed Remote IP(IP1;IP2;...): 0.0.0.0

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.
Remote Telnet	Enable/Disable remote telnet login
Telnet Port	Set the port value which is used to telnet to the device.

NTP settings

Table 72 NTP settings



Time/Date Setting

NTP Settings

NTP Enable: Enable

Current Time: 1970 - 01 - 01 . 01 : 15 : 13

Sync with host: Sync with host

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

Primary NTP Server: pool.ntp.org

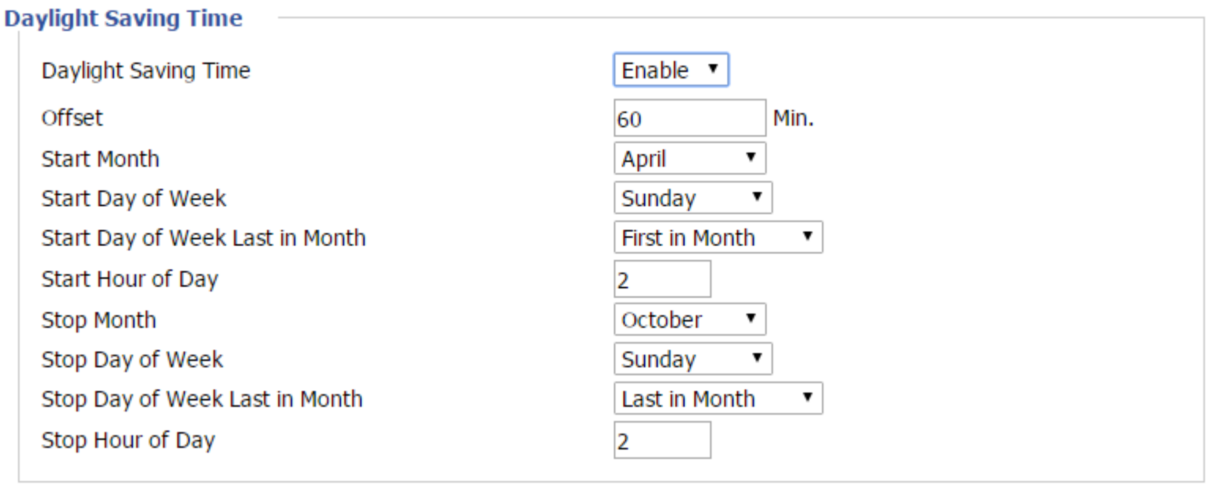
Secondary NTP Server: cn.pool.ntp.org

NTP synchronization(1 - 1440m): 60

Field Name	Description
NTP Enable	Enable/Disable NTP
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 73 Daylight Saving Time



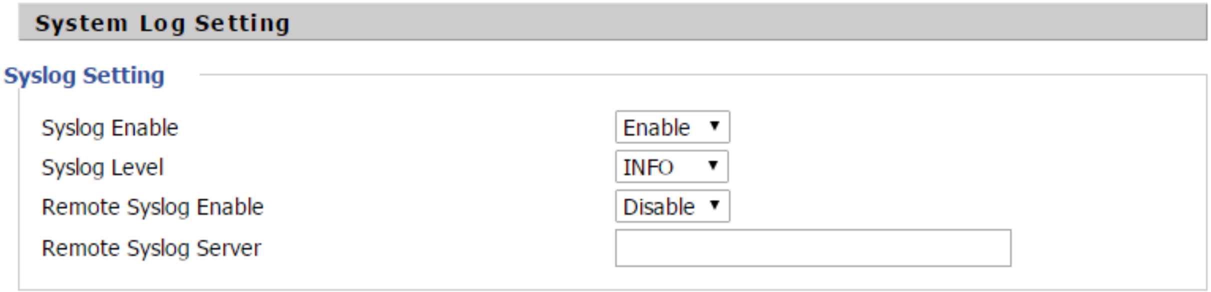
Daylight Saving Time

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 74 System log Setting



System Log Setting

Syslog Setting

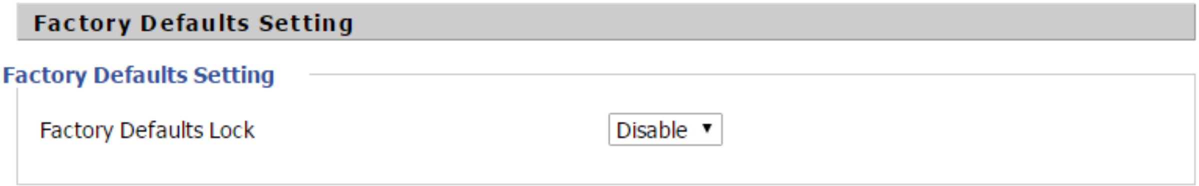
Syslog Enable	Enable ▾
Syslog Level	INFO ▾
Remote Syslog Enable	Disable ▾
Remote Syslog Server	

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
Syslog Level	Select the system log, there is INFO and Debug two grades, the Debug INFO can provide more information.

Factory Defaults Setting

Table 75 Factory Defaults Setting



Factory Defaults Setting

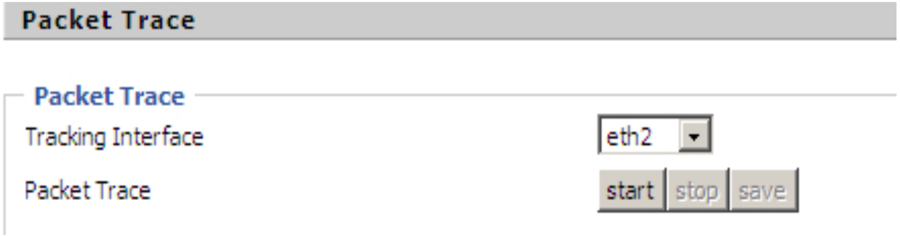
Factory Defaults Setting

Factory Defaults Lock: Disable ▾

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

Packet Trace

Table 76 Packet Trace



Packet Trace

Packet Trace

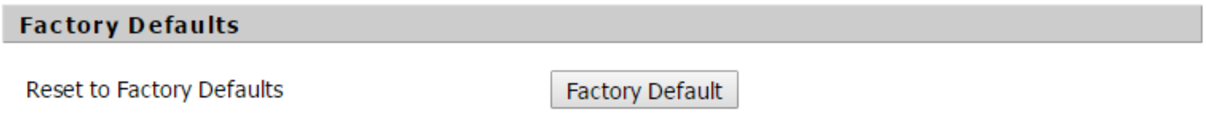
Tracking Interface: eth2 ▾

Packet Trace: start stop save

Description
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.

Factory Defaults

Table 77 Factory Defaults



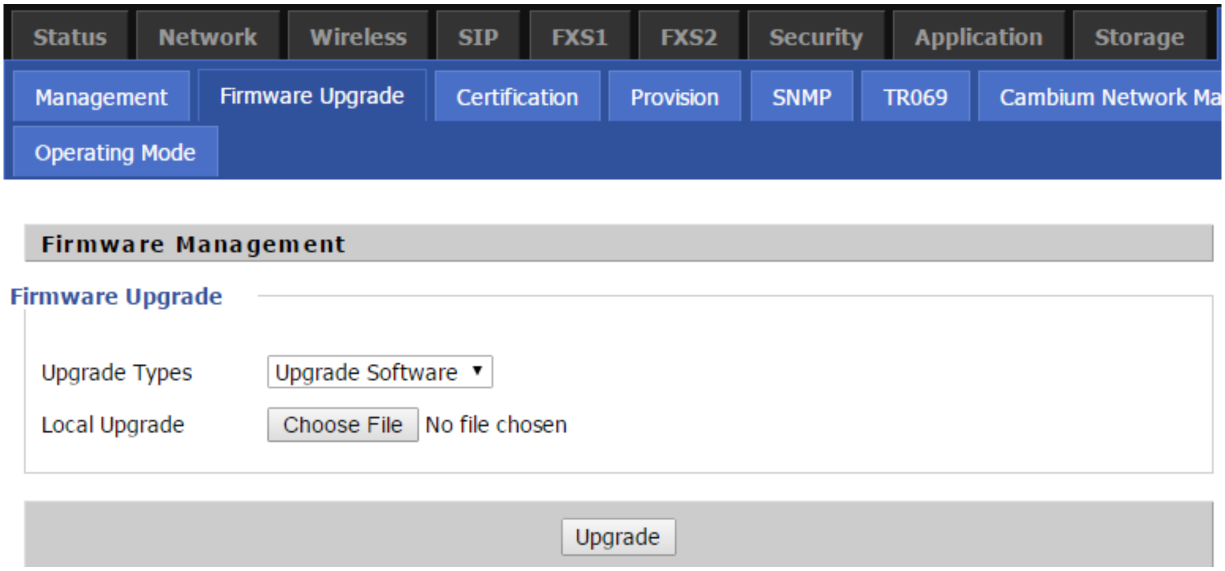
Factory Defaults

Reset to Factory Defaults

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

Firmware Upgrade

Table 78 Firmware upgrade



Firmware Management

Firmware Upgrade

Upgrade Types: Upgrade Software ▼

Local Upgrade: Choose File No file chosen

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

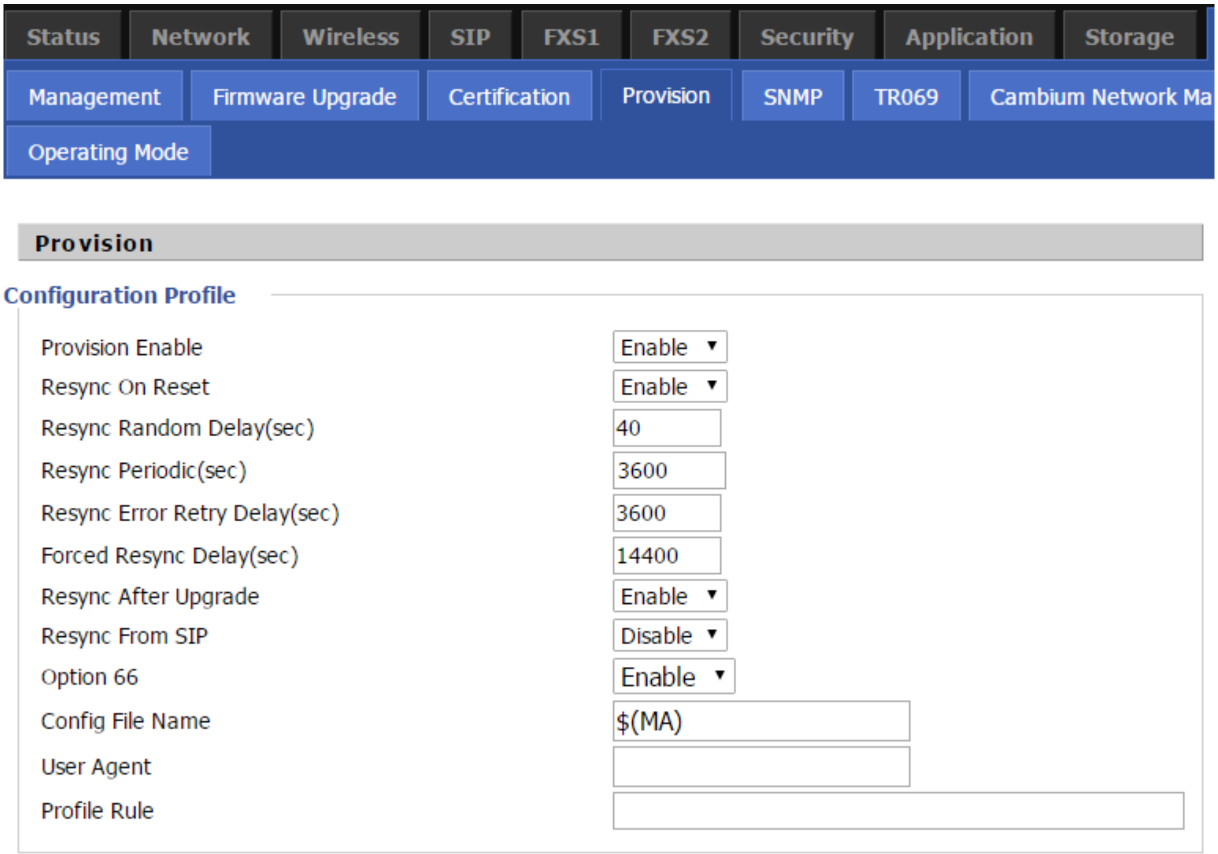
Provision

Provisioning allows CnPilot Home R200x/R201x 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(HTTPS provision will be supported soon)

User can upload a CA Certificate file and Client Certificate file and Private Key file in the Security page.

Table 79 Provision



Provision

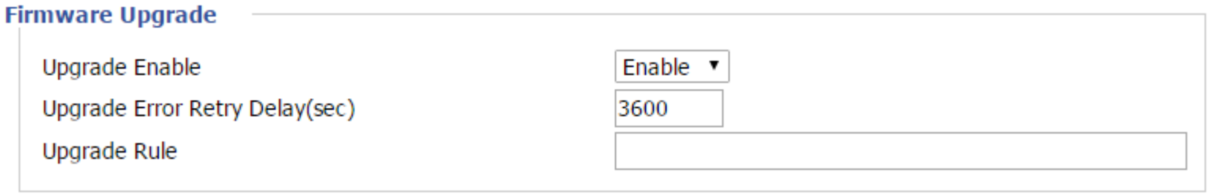
Configuration Profile

Provision Enable	Enable ▾
Resync On Reset	Enable ▾
Resync Random Delay(sec)	40
Resync Periodic(sec)	3600
Resync Error Retry Delay(sec)	3600
Forced Resync Delay(sec)	14400
Resync After Upgrade	Enable ▾
Resync From SIP	Disable ▾
Option 66	Enable ▾
Config File Name	$(MA)
User Agent	
Profile Rule	

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, CnPilot Home R200x will retry resync after the "Resync Error Retry Delay " time, default is 3600s.
Resync Error Retry Delay(rec)	Set the periodic time for resync, default is 3600s.
Forced Resync Delay(sec)	If it's time to resync, but CnPilot Home R200x is busy now, in this case, CnPilot Home R200x will wait for a period time, the longest is "Forced Resync Delay", default is 14400s, when the time over, CnPilot Home R200x 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 80 Firmware Upgrade



Firmware Upgrade

Upgrade Enable: Enable ▼

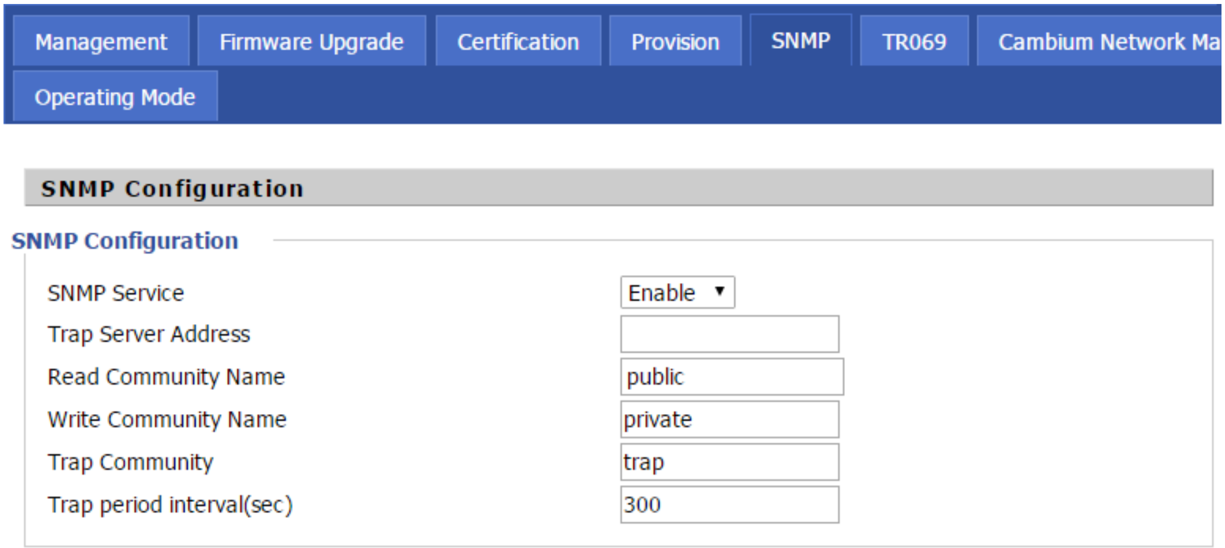
Upgrade Error Retry Delay(sec): 3600

Upgrade Rule:

Field Name	Description
Upgrade Enable	Enable firmware upgrade via provision or not.
Upgrade Error Retry Delay(sec)	If the last upgrade fails, CnPilot Home R200x will try upgrading again after "Upgrade Error Retry Delay" period, default is 3600s.
Upgrade Rule	URL of upgrade file

SNMP

Table 81 SNMP



SNMP Configuration

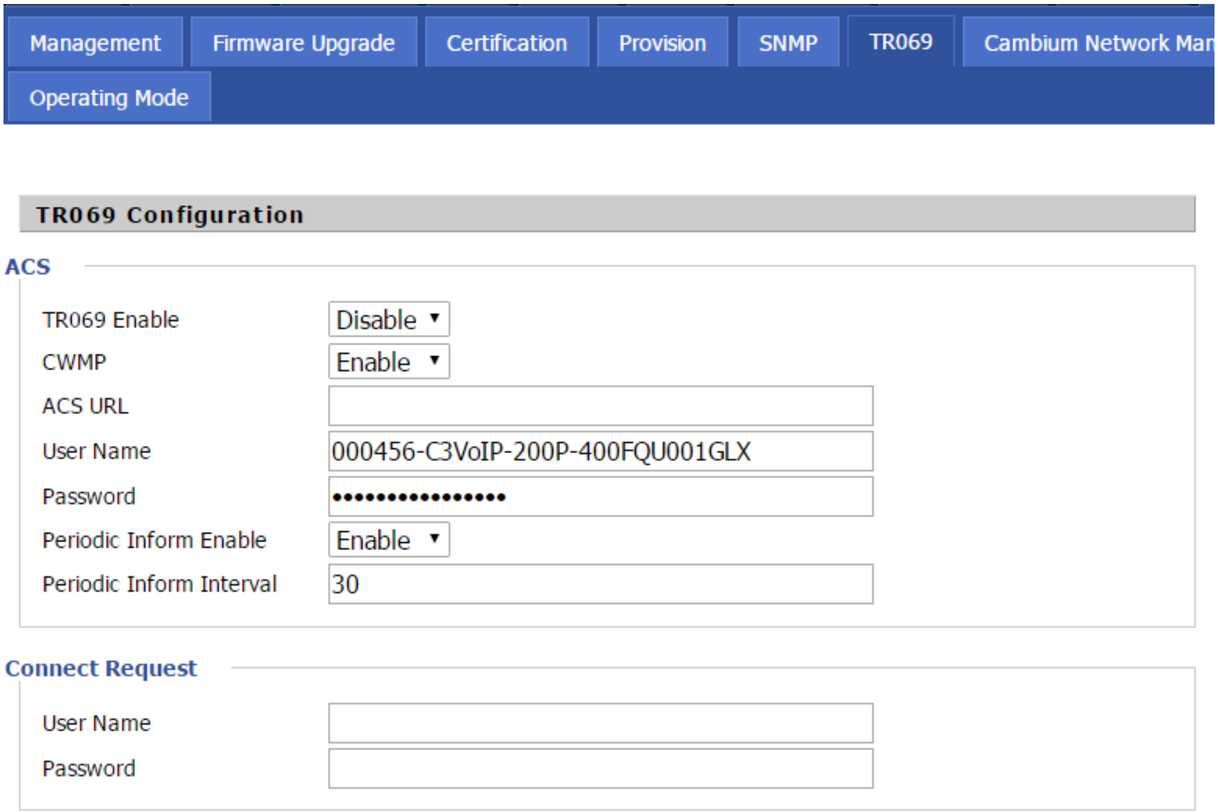
SNMP Configuration

SNMP Service	Enable ▼
Trap Server Address	
Read Community Name	public
Write Community Name	private
Trap Community	trap
Trap period interval(sec)	300

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

TR069

Table 82 TR069



TR069 Configuration

ACS

TR069 Enable	Disable ▾
CWMP	Enable ▾
ACS URL	
User Name	000456-C3VoIP-200P-400FQU001GLX
Password	••••••••••••••••
Periodic Inform Enable	Enable ▾
Periodic Inform Interval	30

Connect Request

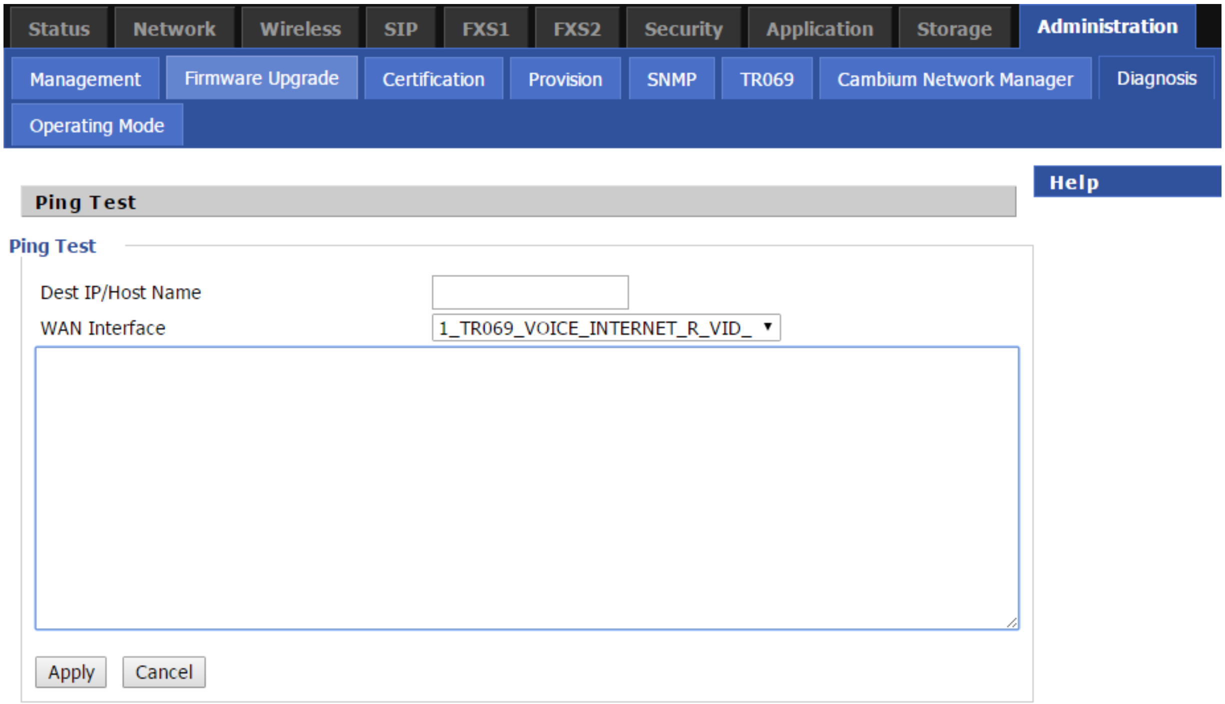
User Name	
Password	

Field Name	Description
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 43200s
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 ping test and traceroute test to diagnose the device's connection status.

Table 83 Diagnosis



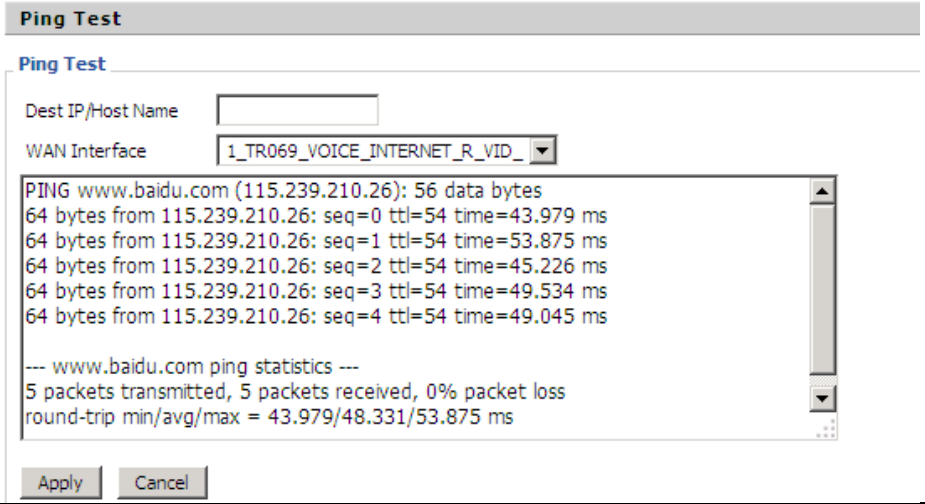
Ping Test

Ping Test

Dest IP/Host Name

WAN Interface: 1_TR069_VOICE_INTERNET_R_VID_

Description
1. 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: 1_TR069_VOICE_INTERNET_R_VID_

```
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
```

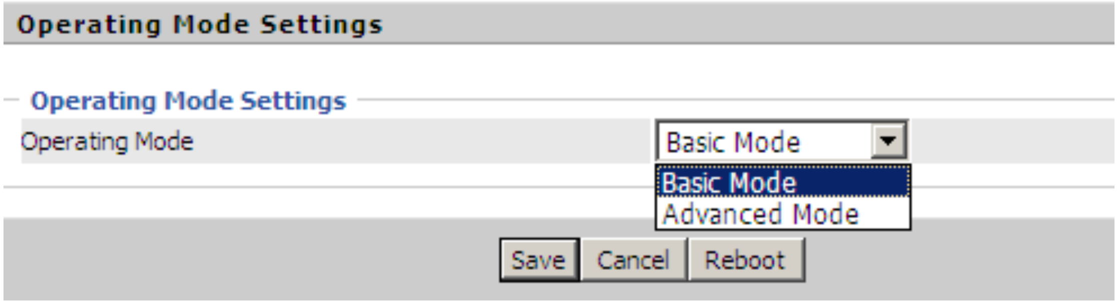
2. Traceroute Test

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

test.

Operating Mode

Table 84 Operating mode



Operating Mode Settings

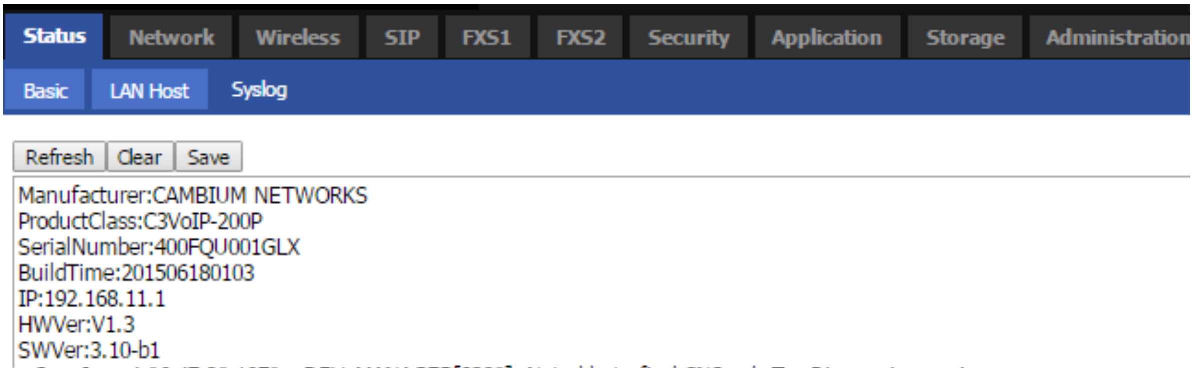
Operating Mode Settings

Operating Mode: Basic Mode

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

System Log

Table 85 System log

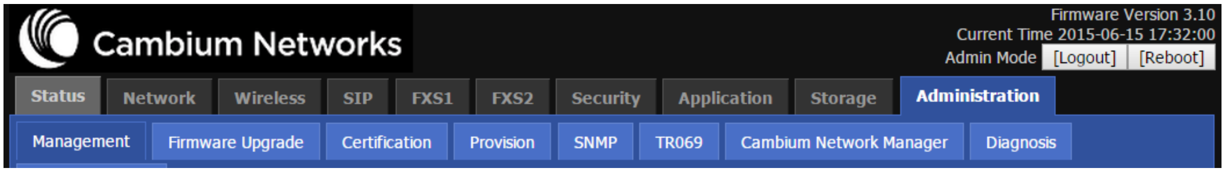


```
Manufacturer:CAMBIUM NETWORKS
ProductClass:C3VoIP-200P
SerialNumber:400FQU001GLX
BuildTime:201506180103
IP:192.168.11.1
HWVer:V1.3
SWVer:3.10-b1
```

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

Logout

Table 86 Logout



Firmware Version 3.10
Current Time 2015-06-15 17:32:00
Admin Mode

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

Reboot

Press the Reboot button to reboot CnPilot Home device.

Chapter 4: Troubleshooting Guide

This chapter covers:

Configuring PC to get IP Address automatically

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

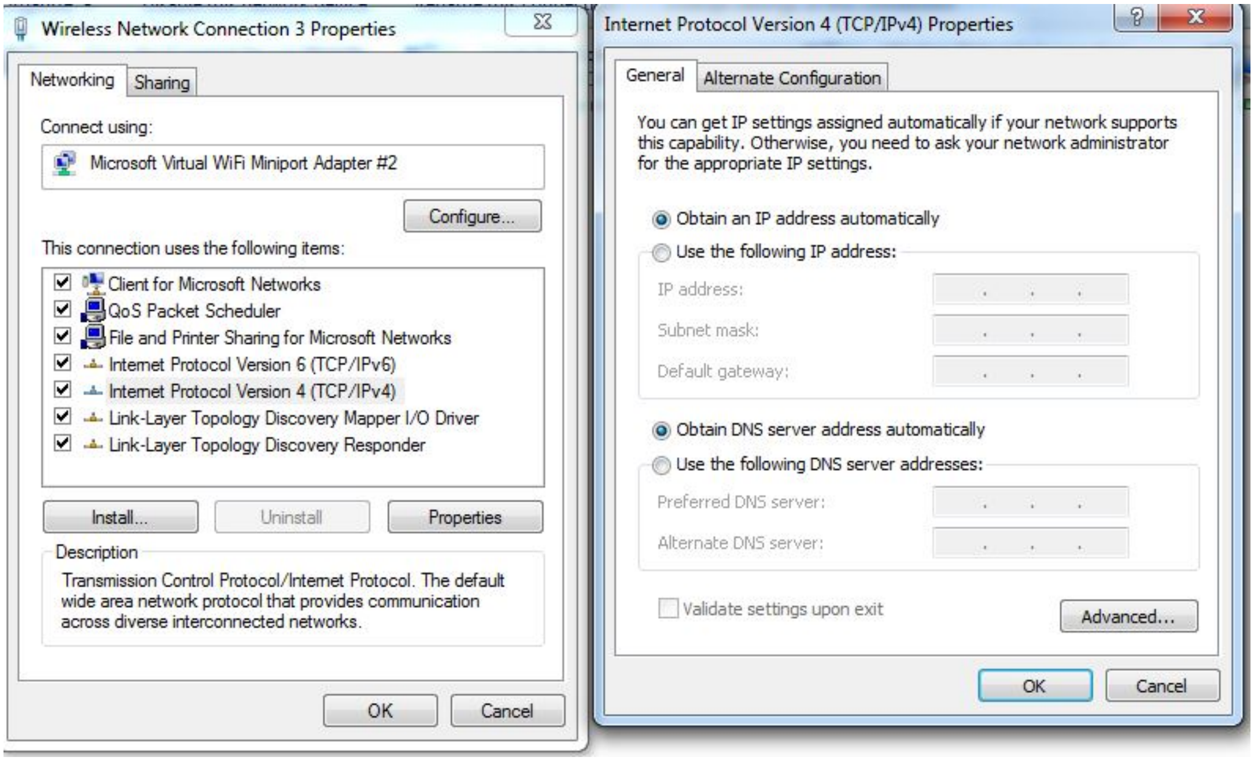
Step 1 : Click the “Start” button

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 5*.

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

Figure 5 *LAN*



Wireless Network Connection 3 Properties

Connect using:

Microsoft Virtual WiFi Miniport Adapter #2

This connection uses the following items:

- ☑ Client for Microsoft Networks
- ☑ QoS Packet Scheduler
- ☑ File and Printer Sharing for Microsoft Networks
- ☑ Internet Protocol Version 6 (TCP/IPv6)
- ☑ Internet Protocol Version 4 (TCP/IPv4)
- ☑ Link-Layer Topology Discovery Mapper I/O Driver
- ☑ Link-Layer Topology Discovery Responder

Description

Transmission Control Protocol/Internet Protocol. The default wide area network protocol that provides communication across diverse interconnected networks.

Internet Protocol Version 4 (TCP/IPv4) Properties

You can get IP settings assigned automatically if your network supports this capability. Otherwise, you need to ask your network administrator for the appropriate IP settings.

● Obtain an IP address automatically

○ Use the following IP address:

IP address: . . .

Subnet mask: . . .

Default gateway: . . .

● Obtain DNS server address automatically

○ Use the following DNS server addresses:

Preferred DNS server: . . .

Alternate DNS server: . . .

□ Validate settings upon exit

Cannot connect to the Web GUI

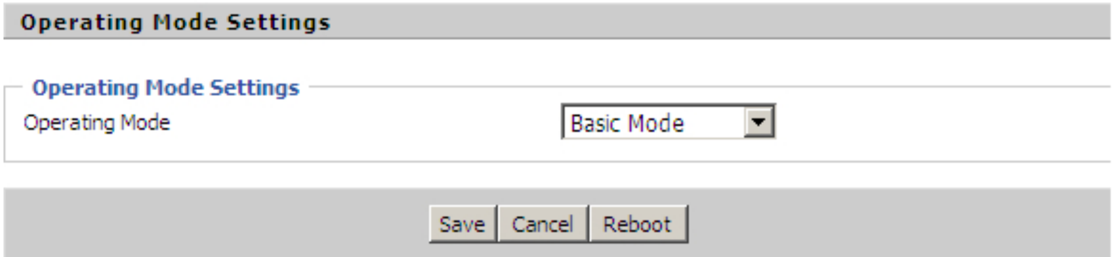
Solution:

- Check if the Ethernet cable is properly connected
- Check if the URL is correct. The format of URL is: http:// the IP address: 8080, 8080 must be added
- Check on any other browser apart from Internet explorer such as Firefox or Mozilla
- 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.

Fast Bridge Setting

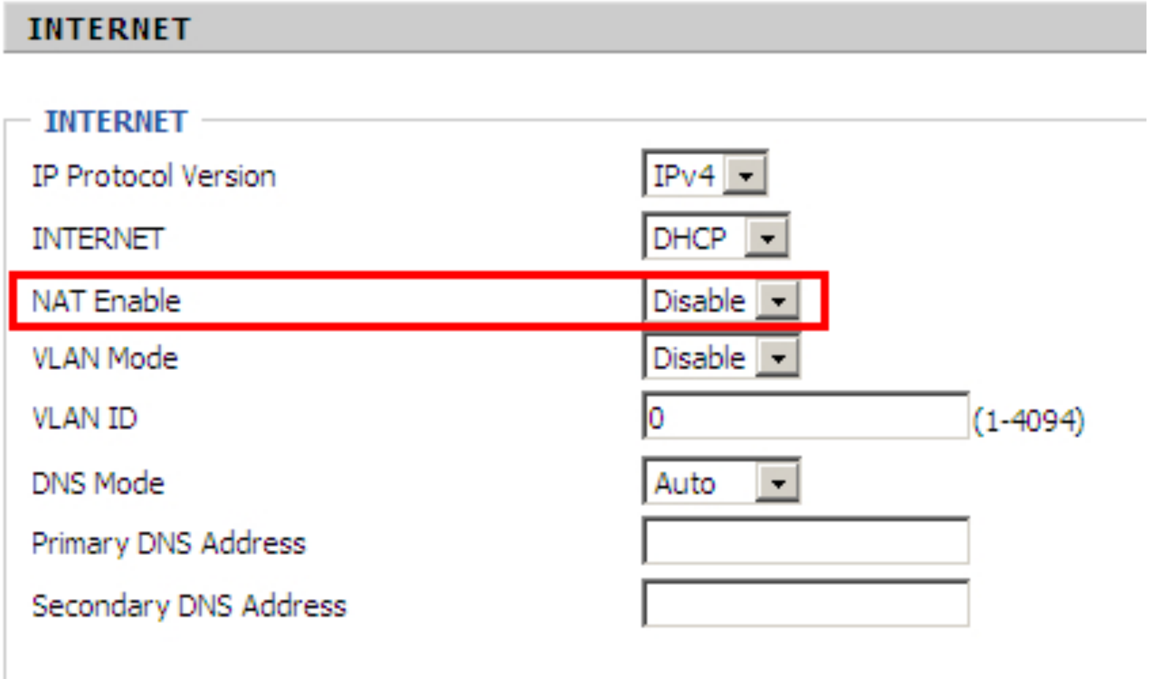


Operating Mode Settings

Operating Mode Settings

Operating Mode: Basic Mode

Description
Step 1: Login Web GUI of the device. Go to **Administration-=> Operating Mode**. Set Operating mode to Basic Mode. Save.



INTERNET

INTERNET

IP Protocol Version: IPv4

INTERNET: DHCP

NAT Enable: Disable

VLAN Mode: Disable

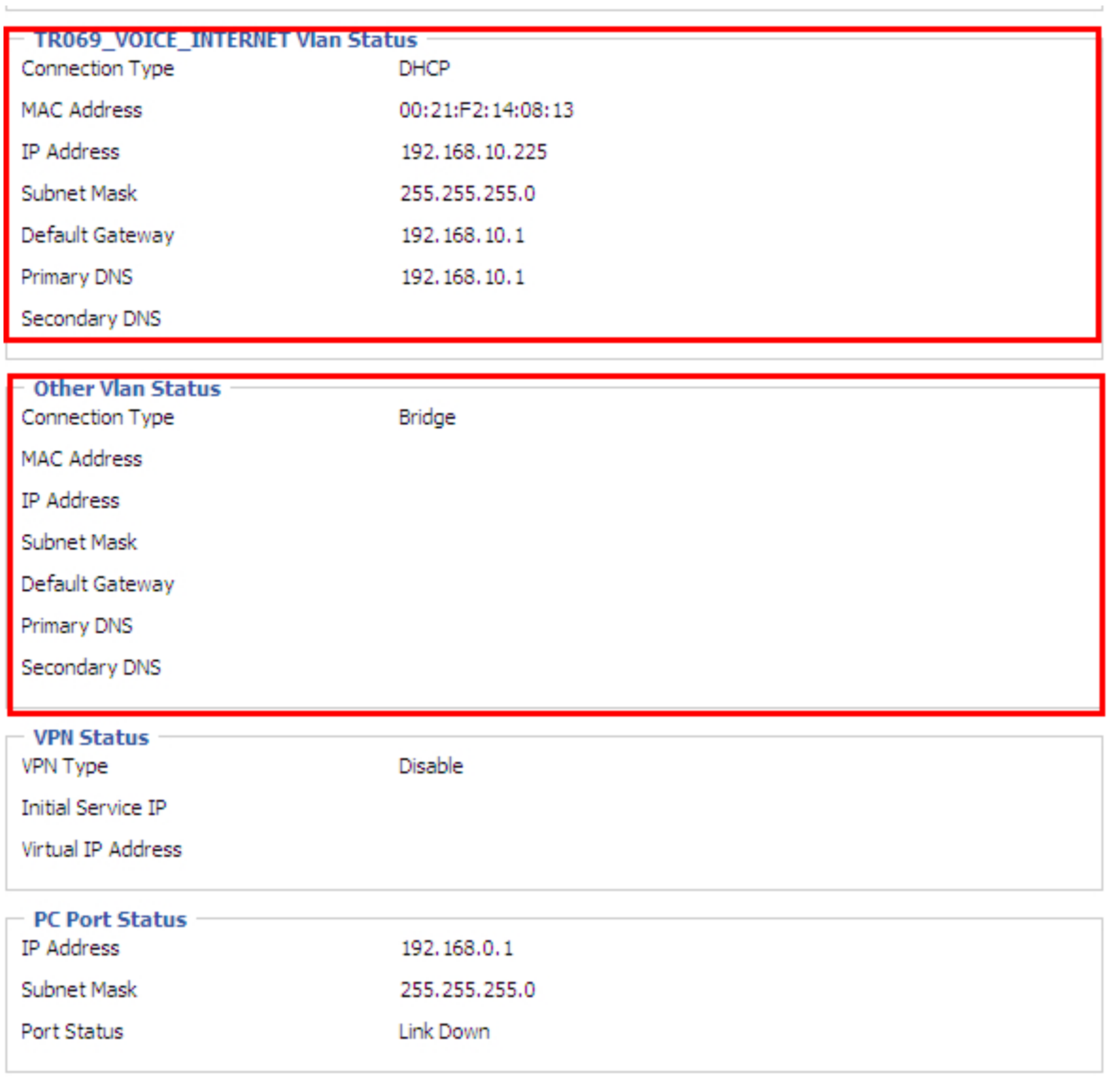
VLAN ID: 0 (1-4094)

DNS Mode: Auto

Primary DNS Address:

Secondary DNS Address:

Step 2: Open Network-> WAN, Change NAT Enable to Disable. Save and Reboot. Now the device works in Bridge mode.



TR069_VOICE_INTERNET Vlan Status

Connection Type	DHCP
MAC Address	00:21:F2:14:08:13
IP Address	192.168.10.225
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
Primary DNS	192.168.10.1
Secondary DNS	

Other Vlan Status

Connection Type	Bridge
MAC Address	
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	

VPN Status

VPN Type	Disable
Initial Service IP	
Virtual IP Address	

PC Port Status

IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Port Status	Link Down

Step 3: Login from WAN port. See example page Status->Basic.

Quick Installation procedure for Router

1. Power ON the wireless router using the power supply/PoE. POWER LED will glow after 5 seconds of powering ON and wait for 2 minutes to boot up device properly.
2. Insert the Ethernet cable to any LAN port on the RJ45 port labeled LAN1 to LAN4 and connect other end of the cable to Ethernet port of PC
3. LAN LED will turn ON after connecting the LAN cable
4. Configure the LAN interface of your PC to acquire the IP address using DHCP. The LAN interface of the PC will get an IP address from the 192.168.11.x/24 subnet
5. Connect to the wireless router by typing http://192.168.11.1 in web browser
6. Enter default username "admin" and password "admin"
7. Change the default password by going to Administration->Management->Password Reset option.
8. Go to Network tab and select INTERNET mode as DHCP/STATIC or PPPoE based on the internet service provided by the ISP. Most common mode of connection would be DHCP (Please refer your ISP's instruction).
9. Go to wireless tab and change the SSID name from default value to your choice of SSID. For selecting the security password for SSID go to Wireless ->Wireless Security and select the SSID from SSID drop down list and select the security type and password. It is recommended to change the wireless security password.
10. Connect the WAN port of the wireless router to the ISP device (eg. ADSL, Cable Modem). Notice that WAN LED will start glowing now.
11. Please save the configuration and reboot the device.
12. cnPilot Home R200P/R201P model has PoE out functionality on WAN port which can power up PMP450 or ePMP 1000 SMs (Subscriber Modules).
13. Again open http://192.168.11.1 and go to STATUS tab and see the "Network Status" for details of internet connectivity and statistics.
14. Now the connection is established for configured SSID and browsing internet.