

# **Cambium cnPilot Home & Small Business Wireless Router User Guide**

**System Release V4.3.1**

**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 3<sup>rd</sup> Party software products described in this document may include or describe copyrighted Cambium and other 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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 3<sup>rd</sup> 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**

Cambium and its supplier(s) specifically disclaim any express or implied warranty of fitness for any high risk activities or uses of its products including, but not limited to, the operation of nuclear facilities, aircraft navigation or aircraft communication systems, air traffic control, life support, or weapons systems ("High Risk Use"). Any High Risk is unauthorized, is made at your own risk and you shall be responsible for any and all losses, damage or claims arising out of any High Risk Use.

© 2017 Cambium Networks Limited. All Rights Reserved.

---

# Contents

---

- About This User Guide ..... 1**
  - Contacting Cambium Networks ..... 2
  - Purpose ..... 3
  - Cross references ..... 3
  - Feedback ..... 3
- Declaration of Conformity ..... 4
  - Part 15 FCC Rules ..... 4
  - Class B Digital Device or Peripheral ..... 4
  - GNU GPL Information ..... 4
- Warnings, cautions, and notes ..... 5
  - Warnings ..... 5
  - Cautions ..... 5
  - Notes ..... 5
- Chapter 1: Product description ..... 6**
  - cnPilot Home R200x/R201x ..... 7
  - cnPilot Home R200x LED Indicators and Interfaces ..... 8
  - cnPilot Home R201x LED Indicators and Interfaces ..... 10
  - Hardware Installation and Setup via cnMaestro ..... 11
  - Accessing and Configuring cnPilot Devices via cnMaestro ..... 12
    - Accessing cnMaestro and Beginning Setup/Configuration ..... 12
  - Accessing and Configuring cnPilot Devices via the local GUI (without cnMaestro) ..... 13
  - Voice Prompt ..... 15
- Chapter 2: Configuring Basic Settings ..... 19**
  - Two-Level Management ..... 20
    - Web Management Interface ..... 20
  - Web Management Interface Details ..... 22
    - Setting the Time Zone ..... 23
    - Configuring an Internet Connection ..... 24
    - Setting up Wireless Connections ..... 26
    - Configuring Session Initiation Protocol (SIP) ..... 29
    - Making a Call ..... 31
- Chapter 3: System planning ..... 33**
  - Login ..... 34
  - Status ..... 35
  - Network and Security ..... 38
    - WAN ..... 38
    - Multi WAN Setting ..... 45

LAN .....	52
Wireless.....	64
Wireless Security.....	77
SIP.....	79
FXS1 .....	81
FXS2 .....	97
Security .....	98
Application.....	101
Storage.....	103
Administration.....	106
Management.....	106
Firmware Upgrade .....	112
Provision .....	113
SNMP.....	115
TR-069.....	116
Diagnosis .....	137
Operating Mode .....	139
System Log .....	140
Logout .....	140
Reboot .....	140
<b>Chapter 4: IPv6 address configuration on WAN interface.....</b>	<b>141</b>
Introduction .....	141
Enabling IPv6.....	142
Configuring IPv6.....	142
Viewing WAN port status .....	145
IPv6 DHCP configuration for LAN/WLAN clients.....	145
LAN DHCPv6 .....	145
<b>Chapter 5: Managing device via cnMaestro .....</b>	<b>147</b>
Preparing the device .....	148
Login to cnMaestro .....	149
On Boarding of cnPilot R200/R201 .....	151
On Boarding using Serial Number .....	151
Onboarding using Cambium ID .....	152
Configuring the Devices .....	153
Basic Details.....	153
Set Device Location.....	153
Firmware Update.....	154
Configure Devices .....	154
Approving On Boarded devices.....	156
Unclaiming the Devices.....	157
<b>Chapter 6: Troubleshooting Guide.....</b>	<b>158</b>
Configuring PC to get IP Address automatically .....	159
Cannot connect to the Web GUI .....	159

Contents

Forgotten Password .....	160
Fast Bridge Setting.....	160
cnMaestro On Boarding troubleshooting .....	162
Quick Installation procedure for Router .....	164
<b>Glossary .....</b>	<b>I</b>

---

# Figures

---

Figure 1 Login Prompt – LAN Port.....	20
Figure 2 Login Prompt – WAN Port .....	21
Figure 3 Multi VLAN.....	45
Figure 4 Multi WAN network.....	46
Figure 5 Basic details .....	153
Figure 6 Select Location .....	154
Figure 7 Firmware update .....	154
Figure 8 Configure devices.....	155
Figure 9 Unclaiming the devices .....	157
Figure 10 LAN .....	159

---

# Tables

---

Table 1 Features at-a-glance .....	7
<b>Table 2</b> cnPilot Home R200x LED Indicators.....	8
<b>Table 3</b> cnPilot Home R200x Interfaces.....	9
Table 4 cnPilot Home R201x LED Indicators.....	10
Table 5 cnPilot Home R201x Interfaces.....	10
Table 6 Voice Menu Setting Options.....	15
Table 7 Web management interface .....	22
Table 8 Setting time zone.....	23
Table 9 Configuring an internet connection .....	24
Table 10 Wireless > Basic web page (user view) .....	26
Table 11 Wireless Security web page .....	28
Table 12 Configuring SIP via the Web Management Interface.....	29
Table 13 Registration status.....	30
Table 14 Login details.....	34
Table 15 Status Page.....	35
Table 16 Internet.....	38
Table 17 DHCP .....	39
Table 18 PPPoE.....	40
Table 19 Bridge Mode.....	42
Table 20 Connect name .....	44
Table 21 Internet.....	46
Table 22 Bridge Mode.....	48
Table 23 LAN port .....	52
Table 24 DHCP server settings.....	54
Table 25 DHCP server, DNS and Client Lease Time.....	55
Table 26 MAC clone .....	56
Table 27 VPN .....	57
Table 28 DMZ.....	57
Table 29 DDNS setting.....	58
Table 30 Port Forward.....	59
Table 31 Advance .....	60
Table 32 Port setting .....	61
Table 33 QoS .....	62
Table 34 Routing .....	63
Table 35 Basic.....	64
Table 36 Wireless security.....	67
Table 37 WiFi Security Setting.....	68
Table 38 WPA-PSK .....	69
Table 39 WPAPSKWPA2PSK.....	69

Table 40	Wireless Access Policy .....	70
Table 41	WMM .....	71
Table 42	WDS .....	72
Table 43	WPS.....	73
Table 44	Station info .....	74
Table 45	Advanced.....	75
Table 46	Wireless security.....	77
Table 47	SIP settings.....	79
Table 48	VoIP QoS.....	80
Table 49	SIP Account – Basic .....	81
Table 50	Audio configuration.....	82
Table 51	Supplementary service .....	83
Table 52	Advanced.....	84
Table 53	Volume settings .....	86
Table 54	Regional.....	87
Table 55	Features and call forward .....	88
Table 56	Miscellaneous .....	90
Table 57	Parameters and settings .....	91
Table 58	Adding one dial plan .....	92
Table 59	Dial Plan.....	92
Table 60	Blacklist.....	94
Table 61	Call log .....	95
Table 62	Filtering setting .....	98
Table 63	Content filtering .....	99
Table 64	UPnP .....	101
Table 65	IGMP .....	102
Table 66	MLD.....	102
Table 67	Disk Management.....	103
Table 68	FTP Setting .....	104
Table 69	Smb setting .....	105
Table 70	Save Config File .....	106
Table 71	Administrator settings.....	107
Table 72	NTP settings .....	108
Table 73	Daylight Saving Time .....	110
Table 74	System log Setting .....	110
Table 75	Factory Defaults Setting.....	111
Table 76	Factory Defaults .....	111
Table 77	Firmware upgrade .....	112
Table 78	Provision.....	113
Table 79	Firmware Upgrade.....	114
Table 80	SNMP .....	115
Table 81	TR069 .....	116
Table 82	Diagnosis .....	137



## Tables

Table 83 Operating mode .....	139
Table 84 System log.....	140
Table 85 Logout.....	140
Table 86 IPv6 Modes.....	141
Table 87 Enabling IPv6.....	142
Table 88 Configuring Statefull IPv6.....	143
Table 89 Configuring Stateless IPv6.....	144

---

# 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



This guide contains the following chapters:

- [Chapter 1: Product description](#)
- [Chapter 2: Configuring Basic Settings](#)
- [Chapter 3: System planning](#)
- [Chapter 5: Managing device via cnMaestro](#)
- [Chapter 6: Troubleshooting Guide](#)

## Contacting Cambium Networks

Support website:	<a href="http://www.cambiumnetworks.com/support">http://www.cambiumnetworks.com/support</a>
Main website:	<a href="http://www.cambiumnetworks.com">http://www.cambiumnetworks.com</a>
Sales enquiries:	<a href="mailto:solutions@cambiumnetworks.com">solutions@cambiumnetworks.com</a>
Support enquiries:	<a href="mailto:support@cambiumnetworks.com">support@cambiumnetworks.com</a>
Repair enquiries	<a href="mailto:rma@cambiumnetworks.com">rma@cambiumnetworks.com</a>
Telephone number list:	<a href="http://www.cambiumnetworks.com/contact">http://www.cambiumnetworks.com/contact</a>
Address:	Cambium Networks Limited, Linhay Business Park, Eastern Road, Ashburton, Devon, UK, TQ13 7UP

## Purpose

Cambium Networks Point-To-Point (PTP) documents are intended to instruct and assist personnel in the operation, installation and maintenance of the Cambium PTP equipment and ancillary devices. It is recommended that all personnel engaged in such activities be properly trained.

Cambium disclaims all liability whatsoever, implied or express, for any risk of damage, loss or reduction in system performance arising directly or indirectly out of the failure of the customer, or anyone acting on the customer's behalf, to abide by the instructions, system parameters, or recommendations made in this document.

## Cross references

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

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

## Feedback

We appreciate feedback from the users of our documents. This includes feedback on the structure, content, accuracy, or completeness of our documents. Send feedback to [support@cambiumnetworks.com](mailto:support@cambiumnetworks.com).

# Declaration of Conformity

---

## Part 15 FCC Rules

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

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

## Class B Digital Device or Peripheral

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



### Note

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

---

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

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

## 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. Important regulatory information.

# 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 could cause loss of life or physical injury. A warning has the following format:

**Warning**

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

---

## 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.

---

---

# Chapter 1: Product description

---

This chapter covers:

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

## cnPilot Home R200x/R201x

**Table 1** 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 <sup>1</sup>		2xFXS in RJ11 <sup>1</sup>		No
Cambium PoE (Power over Ethernet) Out	No	Yes <sup>2</sup>	No	Yes <sup>2</sup>	Yes <sup>2</sup>
Power Adapter	12V/2A	12V/3A	12V/2A	12V/3A	12V/3A
cnMaestro Managed	Yes	Yes	Yes	Yes	Yes

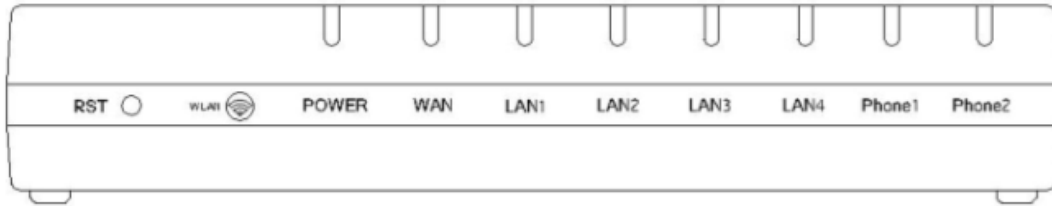
<sup>1</sup> A maximum of four devices may be connected to each FXS port.

<sup>2</sup> One PMP or ePMP device at a time may be powered by the Power-over-Ethernet (PoE) port.



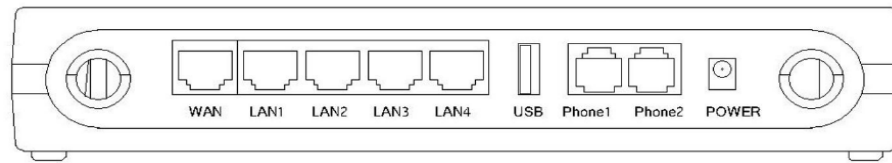
## cnPilot Home R200x LED Indicators and Interfaces

**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 100 Mbps
	Off	The port is disconnected
	Blinking (Green)	Transmitting data
WAN	On (Green)	Port is connected with 100 Mbps
	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

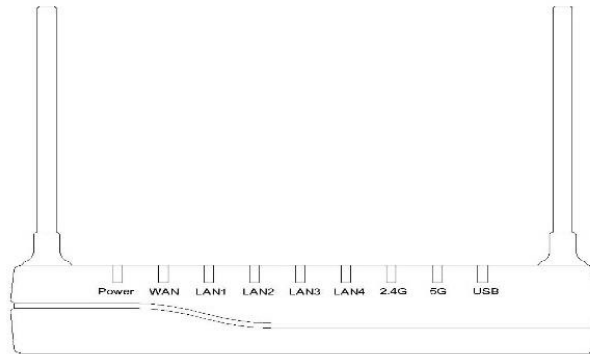
**Table 3** cnPilot Home R200x Interfaces

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	On (Green)	Wireless access point is ready
	Blinking (Green)	The port is passing data
	On (Green)	The port is connected at 100 Mbps
WAN	Off	The port is disconnected
	Blinking (Green)	The data is transmitting
	On (Green)	The port is connected at 100 Mbps
LAN 1/2/3/4	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

Follow the below links to configure and manage cnPilot devices:

- [Login to cnMaestro](#) on page 149
- [On Boarding of cnPilot R200/R201](#) on page 151
- [Configuring the Devices](#) on page 153
- [Approving On Boarded devices](#) on page 156
- [Unclaiming the Devices](#) on page 157

# 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 2 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
<p>1 WAN Port Connection Type</p>	<ol style="list-style-type: none"> <li>1. Pick up phone and press "****" to start IVR</li> <li>2. Choose "1", and cnPilot Home R200x/R201x reports the current WAN port connection type</li> <li>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.</li> <li>4. Prompt "Please enter password", user needs to input password and press "#" key if user wants to configuration WAN port connection type.</li> <li>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 ..."</li> <li>6. To quit, enter "**"</li> </ol>
<p>2 WAN Port IP Address</p>	<ol style="list-style-type: none"> <li>1. Pick up phone and press "****" to start IVR</li> <li>2. Choose "2", and cnPilot Home R200x /R201x reports current WAN Port IP Address</li> <li>3. Input the new WAN port IP address and press "#" key:  Use "*" to replace ".", for example user can input 192*168*20*168 to set the new IP address 192.168.20.168</li> <li>4. Press # key to indicate that you have finished  Report "operation successful" if user operation is ok.</li> <li>5. To quit, enter "***".</li> </ol>



<p style="text-align: center;">3 WAN Port Subnet Mask</p>	<ol style="list-style-type: none"> <li>1. Pick up phone and press "****" to start IVR</li> <li>2. Choose "3", and cnPilot Home R200x /R201x reports current WAN port subnet mask</li> <li>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</li> <li>4. Press "#" key to indicate that you have finished Report "operation successful" if user operation is ok.</li> <li>5. To quit, enter "***".</li> </ol>
<p style="text-align: center;">4 Gateway</p>	<ol style="list-style-type: none"> <li>1. Pick up phone and press "****" to start IVR</li> <li>2. Choose "4", and cnPilot Home R200x/R201x reports current gateway</li> <li>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.</li> <li>4. Press "#" key to indicate that you have finished. Report "operation successful" if user operation is ok.</li> <li>5. To quit, press "***".</li> </ol>
<p style="text-align: center;">5 DNS</p>	<ol style="list-style-type: none"> <li>1. Pick up phone and press "****" to start IVR</li> <li>2. Choose "5", and cnPilot Home R200x /R201x reports current DNS</li> <li>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.</li> <li>4. Press "#" key to indicate that you have finished. Report "operation successful" if user operation is ok.</li> <li>5. If you want to quit, press "***".</li> </ol>
<p style="text-align: center;">6 Factory Reset</p>	<ol style="list-style-type: none"> <li>1. Pick up phone and press "****" to start IVR</li> <li>2. Choose "6", and cnPilot Home R200x /R201x reports "Factory Reset"</li> <li>3. Prompt "Please enter password", the method of inputting password is the same as operation 1.</li> <li>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.</li> <li>5. Press "7" reboot to make changes effective.</li> </ol>

7 Reboot	<ol style="list-style-type: none"> <li>1. Pick up phone and press "*****" to start IVR</li> <li>2. Choose "7", and cnPilot Home R200x/R201x reports "Reboot"</li> <li>3. Prompt "Please enter password", the method of inputting password is same as operation 1.</li> <li>4. cnPilot Home R200x/R201x reboots if password is right and operation is ok.</li> </ol>
8 WAN Port Login	<ol style="list-style-type: none"> <li>1. Pick up phone and press "*****" to start IVR</li> <li>2. Choose "8", and cnPilot Home R200x/R201x reports "WAN Port Login"</li> <li>3. Prompt "Please enter password", the method of inputting password is same as operation 1.</li> <li>4. If user wants to quit, press "*" .</li> </ol>
9 WEB Access Port	<ol style="list-style-type: none"> <li>1. Pick up phone and press "*****" to start IVR</li> <li>2. Choose "9", and cnPilot Home R200x /R201x reports " WEB Access Port"</li> <li>3. Prompt "Please enter password", the method of inputting password is same as operation 1. Report "operation successful" if user operation is ok.</li> <li>4. Report the current WEB Access Port</li> <li>5. Set the new WEB access port and press "#" key.</li> <li>6. Report "operation successful" if user operation is successful.</li> </ol>
0 Firmware Version	<ol style="list-style-type: none"> <li>1. Pick up phone and press "*****" to start IVR</li> <li>2. Choose "0" and CnPilot Home R200x/R201x reports the current Firmware version</li> </ol>

**Note**

1. While using Voice menu, press \* (star) to return to main menu.
2. If any changes made in the IP assignment mode, the router must be rebooted in order for the settings to take effect.
3. While entering an IP address or subnet mask, use "\*" (star) to enter "." (Dot) and use "#" (hash) key to finish entering IP address or subnet mask

*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

4. 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.
5. 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.
6. 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 [Chapter 6: 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

Cambium Networks

Username

Password

Login

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

**Note**

If you are unable to access the web configuration, please see [Chapter 6: Troubleshooting Guide](#) for more information.

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

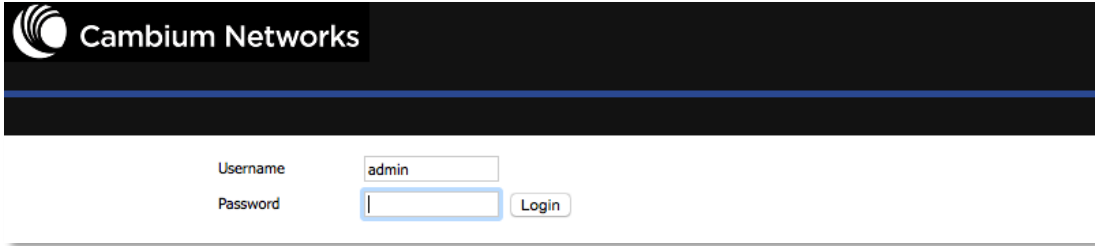
## Logging in from the WAN port

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



The screenshot shows the login interface for a Cambium Networks device. At the top, there is a dark header with the Cambium Networks logo and name. Below this, the login form is displayed on a white background. It includes a 'Username' field containing the text 'admin' and a 'Password' field which is empty. A 'Login' button is positioned to the right of the password field.

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



### Note

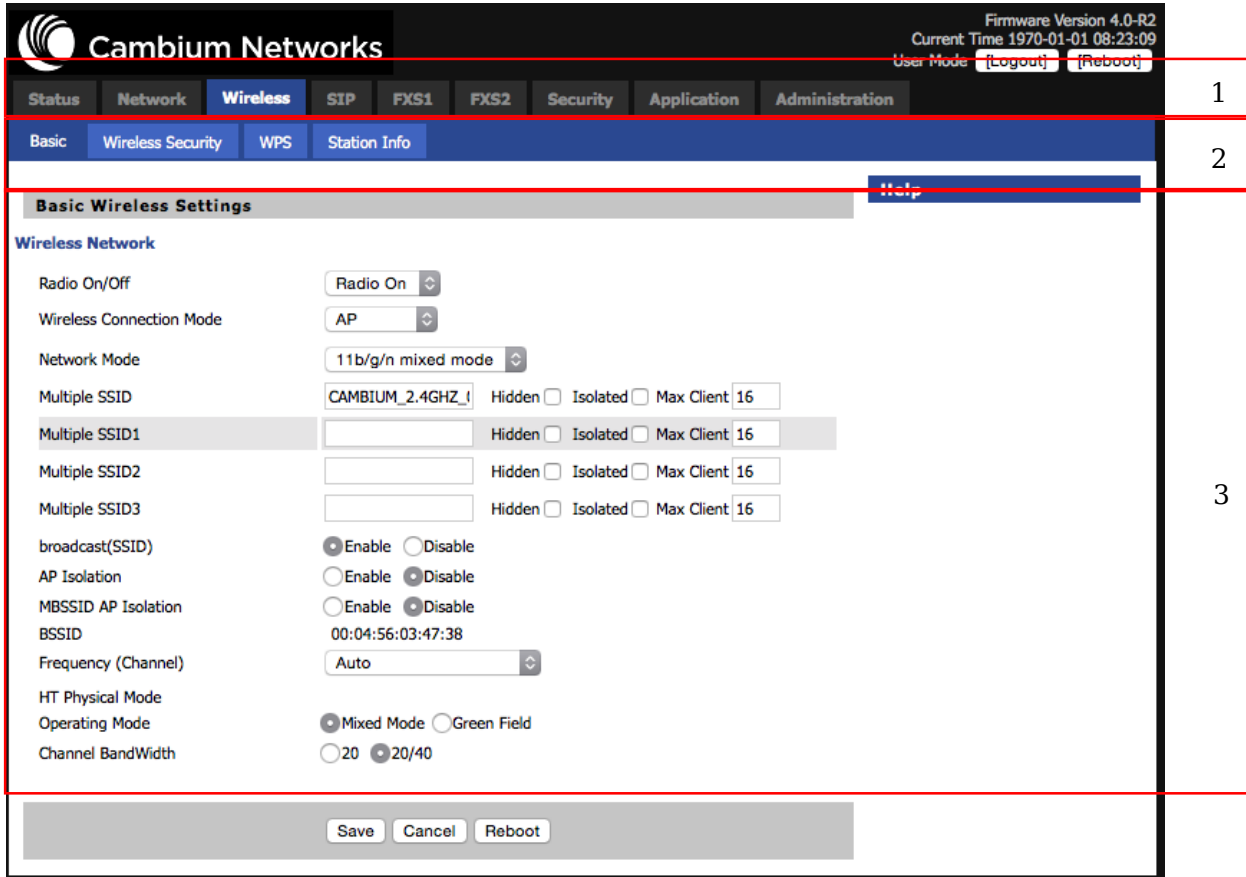
If you fail to access to the web configuration, see [Chapter 6: Troubleshooting Guide](#) for more information.

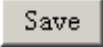
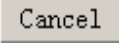
---

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

# Web Management Interface Details

**Table 7** Web management interface

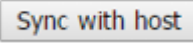


Field Name	Description
Top Navigation bar	Click an option in <b>Top Navigation</b> bar (area marked as "1"). Multiple options in the <b>Sub-navigation bar</b> are displayed
Sub-navigation bar	Click the <b>Sub-navigation bar</b> to choose a configuration page (area marked as "2")
Parameter configuration	This area displays the current parameters for configuration (e.g. area marked as "3")
	<p>1. Any time changes are made click "Save" to confirm and save the changes.</p> <p>2. On click of "Save" button, a red message will be displayed as shown below to notify a reboot.</p> <p><b>Please REBOOT to make the changes effective!</b></p>
	To cancel the changes.

## Setting the Time Zone

**Table 8** Setting time zone

Time/Date Setting	
<b>NTP Settings</b>	
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
<b>Daylight Saving Time</b>	
Daylight Saving Time	Disable

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



## Configuring an Internet Connection

From the Network > WAN page, WAN connections may be inserted or deleted. For more information on Internet Connection setting, see [Table 9](#) below.

**Table 9** Configuring an internet connection

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

### INTERNET

**WAN**

Connect Name:  Delete Connect

Service:

IP Protocol Version:

WAN IP Mode:

NAT Enable:

VLAN Mode:

VLAN ID:  (1-4094)

Static

IP Address:

Subnet Mask:

Default Gateway:

DNS Mode:

Primary DNS Address:

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 gotten from your ISP provider.

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

---

VLAN ID	 <b>Note</b> Multiple WAN connections may be created with the same VLAN ID
---------	--

---

DNS Mode	Select DNS mode, options are Auto and Manual: <ol style="list-style-type: none"><li>1. When DNS mode is Auto, the device under LAN port will automatically obtains the preferred DNS and alternate DNS.</li><li>2. When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS</li></ol>
----------	--

---

Primary DNS	Enter the preferred DNS address
Secondary DNS	Enter the secondary DNS address
<b>DHCP</b>	<b>(displayed when WAN IP Mode is set to DHCP)</b>
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)

Field Name	Description
Radio On/Off	Select "Radio Off" to disable wireless operation Select "Radio on" to enable wireless operation <i>Please note: "Save" required for this parameter change</i>
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)	<b>Enabled:</b> The device SSID is broadcast at regular intervals <b>Disabled:</b> The device SSID is not broadcast at regular intervals, disallowing wi-fi clients from automatically connecting to the cnPilot

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

## Encryption

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

**Table 11 Wireless Security web page**

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

---

**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	<p>Select an appropriate encryption mode to improve the security and privacy of your wireless data packets.</p> <p>Each encryption mode will launch an additional web page and ask you to offer additional configuration.</p> <p>For high security, the device can be configured for Security Mode as WPA2-PSK and WPA Algorithms as AES.</p>
WPA Algorithms	This parameter is used to select the encryption of wireless home gateway algorithms; options are TKIP, AES and TKIPAES.
Pass Phrase	Configure the WPA-PSK security password.
Key Renewal Interval	Set the key scheduled update cycle, default is 3600s.
<b>Access Policy</b>	
Policy	<p><b>Disable:</b> Access policy rules are not enforced</p> <p><b>Allow:</b> Only allow the clients in the station MAC list to access</p> <p><b>Rejected:</b> Block the clients in the station MAC list from registering</p>
Add a Station MAC	Enter the MAC address of the clients which you want to allow or reject

## Configuring Session Initiation Protocol (SIP)

### SIP Accounts

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

The screenshot shows the 'SIP Account' configuration page for 'FXS1'. The interface includes a navigation bar with tabs for 'Status', 'Network', 'Wireless', 'SIP', 'FXS1', 'FXS2', 'Security', 'Application', 'Storage', and 'A'. Below this is a sub-menu with 'SIP Account', 'Preferences', 'Dial Plan', 'Blacklist', and 'Call Log'. The main content area is titled 'Basic' and contains three sections: 'Basic Setup' with 'Line Enable' and 'Peer To Peer' both set to 'Disable'; 'Proxy and Registration' with fields for 'Proxy Server', 'Outbound Server', 'Backup Outbound Server', 'Proxy Port', 'Outbound Port', and 'Backup Outbound Port', all with '5060' entered; and 'Subscriber Information' with fields for 'Display Name', 'Account', 'Phone Number', and '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

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage
Basic	LAN Host	Syslog						
<b>Product Information</b>								
<b>Product Information</b>								
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							
<b>SIP Account Status</b>								
<b>SIP Account Status</b>								
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: System planning

---

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

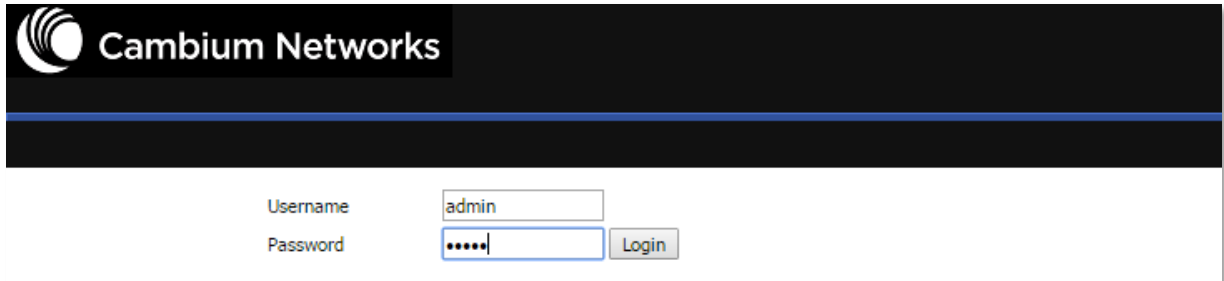
This chapter covers:

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

# Login

---

**Table 14** Login details



Cambium Networks

Username

Password

## Procedure

1. Connect the LAN port of the router to your PC via 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

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage
Basic	LAN Host	Syslog						

Product Information	
<b>Product Information</b>	
Product Name	cnPilot R.200P
Internet(WAN) MAC Address	00:04:56:04:27:89
PC(LAN) MAC Address	00:04:56:04:27:88
Hardware Version	V1.3
Loader Version	V3.07(Aug 20 2015 17:38:07)
Firmware Version	4.3-R1(201601131522)
Device-Agent Version	2.13
Serial Number	400FRG088N4X

SIP Account Status	
<b>SIP Account Status</b>	
FXS 1 SIP Account Status	Disable
Primary Server	0.0.0.0
Backup Server	0.0.0.0
FXS 2 SIP Account Status	Disable
Primary Server	0.0.0.0
Backup Server	0.0.0.0

FXS Port Status	
<b>FXS Port Status</b>	
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	10.110.134.15 <input type="button" value="Renew"/>
Subnet Mask	255.255.255.0
Default Gateway	10.110.134.254
Primary DNS	10.110.12.30
Secondary DNS	10.110.12.31
WAN Port Status	100Mbps Full

### TR069\_VOICE\_INTERNET Vlan Status

Connection Type	DHCP
MAC Address	00:04:56:04:27:89
IP Address	10.110.134.15
Subnet Mask	255.255.255.0
Default Gateway	10.110.134.254
Primary DNS	10.110.12.30
Secondary DNS	10.110.12.31

### VPN Status

VPN Type	Disable
Initial Service IP	
Virtual IP Address	

### LAN Port Status

IP Address	192.168.11.1
Subnet Mask	255.255.255.0
LAN1	Link Down
LAN2	Link Down
LAN3	100Mbps Full
LAN4	Link Down

### Wireless Info

#### Wireless 2.4GHz

Radio On/Off	On
Network Mode	11b/g/n
Current Channel	1
Channel Bandwidth	40MHz

#### CAMBIUM\_2.4GHz\_042788

BSSID	00:04:56:04:27:88
Number of Device	0

#### SSID2

BSSID	00:04:56:04:27:89
Number of Device	0

#### SSID3

BSSID	00:04:56:04:27:8A
Number of Device	0

#### SSID4

BSSID	00:04:56:04:27:8B
Number of Device	0

### System Status

#### System Status

Current Time	2016-01-19 05:47:28
Elapsed Time	1 Min

### Description

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

# 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

Static	
IP Address	<input type="text" value="192.34.30.69"/>
Subnet Mask	<input type="text" value="255.255.255.248"/>
Default Gateway	<input type="text" value="192.34.30.65"/>
DNS Mode	<input type="text" value="Manual"/>
Primary DNS Address	<input type="text" value="66.185.0.68"/>
Secondary DNS Address	<input type="text"/>

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 <b>Auto</b> and <b>Manual</b> : <ol style="list-style-type: none"> <li>When DNS mode is <b>Auto</b>, the device under LAN port will automatically obtain the preferred DNS and alternate DNS.</li> <li>When DNS mode is <b>Manual</b>, the user manually configures the preferred DNS and alternate DNS information</li> </ol>
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

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage	
WAN	LAN	MAC Clone	VPN	DMZ	Port Forward	Advance	Port Setting	QoS	Rou

---

**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	<input type="text"/>	
Secondary DNS Address	<input type="text"/>	
DHCP		
DHCP Renew	Renew	
DHCP Vendor(Option 60)	Cambium CNS-NG	

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



## PPPoE

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

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

**Table 18** PPPoE

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage	
WAN	LAN	MAC Clone	VPN	DMZ	Port Forward	Advance	Port Setting	QoS	Rout

---

**INTERNET**

**WAN**

Connect Name:  Delete Connect

Service:

IP Protocol Version:

WAN IP Mode:

NAT Enable:

VLAN Mode:

VLAN ID:  (1-4094)

DNS Mode:

Primary DNS Address:

Secondary DNS Address:

PPPoE

PPPoE Account:

PPPoE Password:

Confirm Password:

Service Name:

Leave empty to autodetect

Operation Mode:

Keep Alive Redial Period(0-3600s):

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

Confirm Password	Enter your PPPoE password again
Service Name	Enter a service name for PPPoE authentication. If it is left empty, the service name is auto detected.
Operation Mode	<p>Select the mode of operation, options are <b>Keep Alive</b>, <b>On Demand</b> and <b>Manual</b>:</p> <ul style="list-style-type: none"> <li>When the mode is <b>Keep Alive</b>, the user sets the 'keep alive redial period' values range from 0 to 3600s, the default setting is 5 minutes;</li> <li>When the mode is <b>On Demand</b>, the user sets the 'on demand idle time' value in the range of 0-60 minutes, the default setting is 5 minutes;</li> </ul> <div style="text-align: right;"> <p>Operation Mode <input type="text" value="On Demand"/></p> <p>On Demand Idle Time(0-60m) <input type="text" value="5"/></p> </div> <ul style="list-style-type: none"> <li>When the mode is <b>Manual</b>, there are no additional settings to configure</li> </ul>
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	
<b>WAN</b>	
Connect Name	1_TR069_VOICE_INTERNET_R_VID_ <span>Delete Connect</span>
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 <input checked="" type="checkbox"/> Port_1 <input checked="" type="checkbox"/> Port_2 <input checked="" type="checkbox"/> Port_3 <input checked="" type="checkbox"/> Port_4 <input checked="" type="checkbox"/> Wireless(SSID1) <input checked="" type="checkbox"/> Wireless(SSID2) <input checked="" type="checkbox"/> Wireless(SSID3) <input checked="" type="checkbox"/> 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
<b>Bridge Type</b>	
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
<b>DHCP Service Type</b>	
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.
<b>VLAN Mode</b>	
Disable	The WAN interface is untagged. LAN is untagged.
Enable	The WAN interface is tagged. LAN is untagged.
Trunk	Only valid in bridge mode. All ports, including WAN and LAN, belong to this VLAN Id and all ports are tagged with this VLAN id. Tagged packets can pass through WAN and LAN.
VLAN ID	Set the VLAN ID.
	<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p><b>Note</b></p> <p>Multiple WAN connections may be created with the same VLAN ID</p> </div> </div>
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)

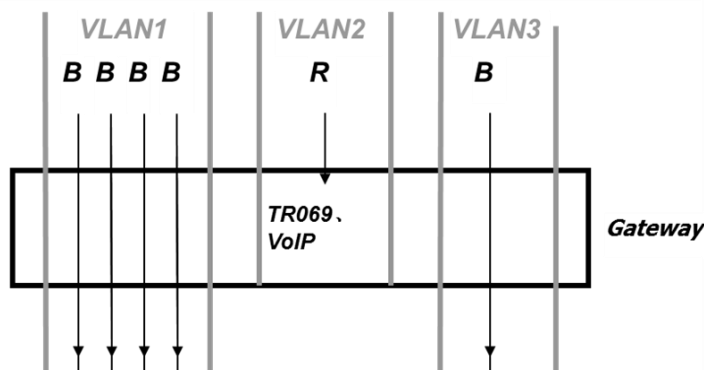
2\_INTERNET\_B\_VID\_(Second Interface, Service is INTERNET, Bridge Mode, VLAN is disabled)

## 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.

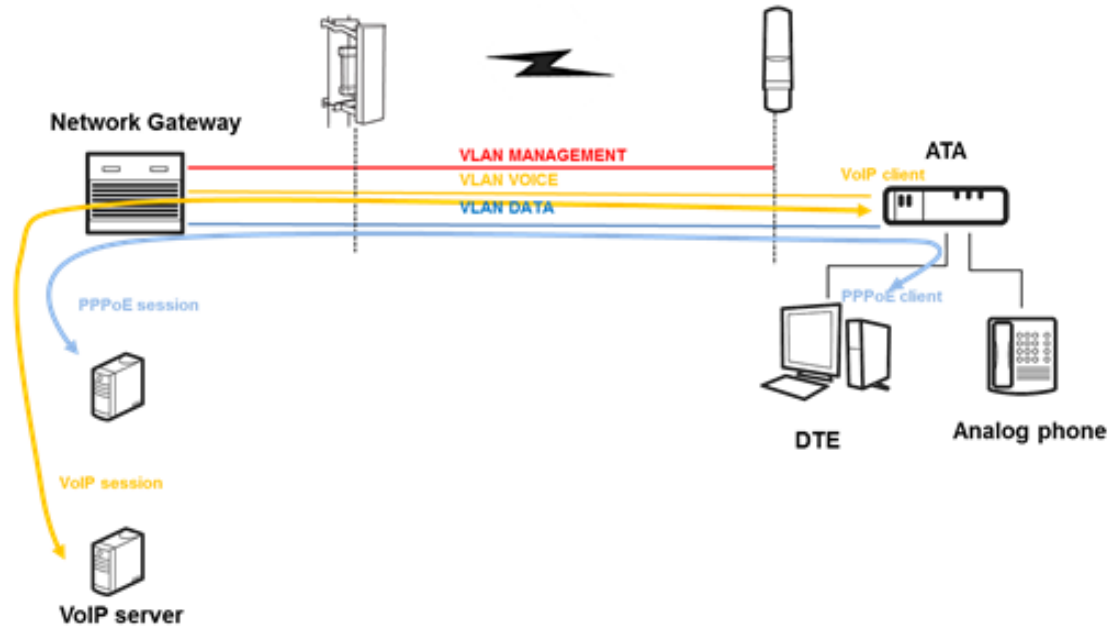
**Figure 3** Multi VLAN



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.
- Multiple WAN link (i.e. Connect Name) can be configured with same VLAN ID.

**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	
<b>WAN</b>	
Connect Name	1_TR069_VOICE_INTERNET_R_VID_ <span style="float: right;">Delete Connect</span>
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	<input type="text"/>
Secondary DNS Address	<input type="text"/>

Content	Define	Comment
<b>No</b>	1 to 99	WAN Connection identifier
<b>Service</b>	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
<b>NAT Mode</b>	B	Bridge
	R	Router
<b>VLAN ID</b>	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	
<b>WAN</b>	
Connect Name	1_TR069_VOICE_INTERNET_R_VID_ <span>Delete Connect</span>
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 <input checked="" type="checkbox"/> Port_1 <input checked="" type="checkbox"/> Port_2 <input checked="" type="checkbox"/> Port_3 <input checked="" type="checkbox"/> Port_4 <input checked="" type="checkbox"/> Wireless(SSID1) <input checked="" type="checkbox"/> Wireless(SSID2) <input checked="" type="checkbox"/> Wireless(SSID3) <input checked="" type="checkbox"/> 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 !	
<span>Save</span> <span>Cancel</span> <span>Reboot</span>	

Field Name	Description
<b>Bridge Type</b>	
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.
<b>DHCP Service Type</b>	
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.

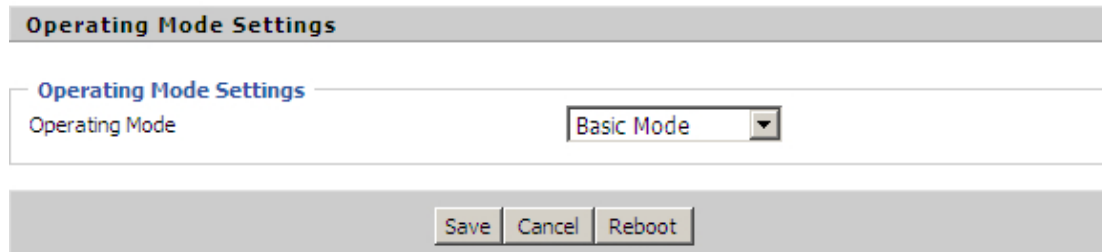
---

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**.

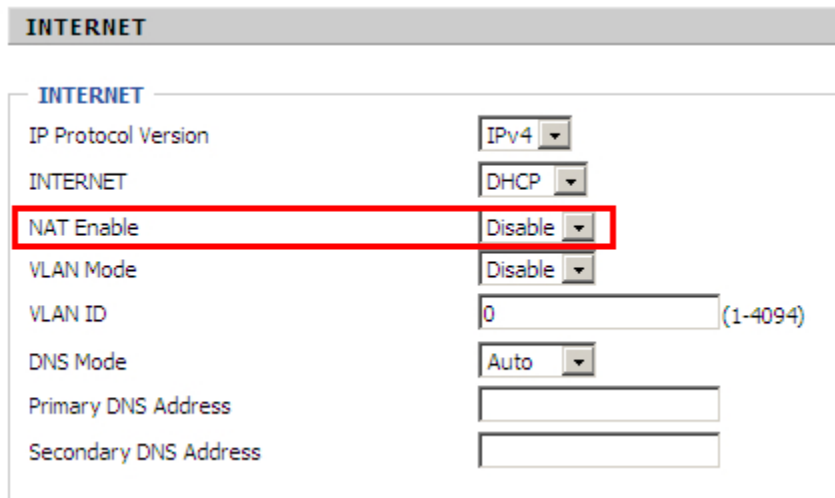


**Operating Mode Settings**

**Operating Mode Settings**

Operating Mode

- 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

INTERNET

**NAT Enable**

VLAN Mode

VLAN ID  (1-4094)

DNS Mode

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.

<b>TR069_VOICE_INTERNET Vlan Status</b>	
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	

<b>Other Vlan Status</b>	
Connection Type	Bridge
MAC Address	
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	

<b>VPN Status</b>	
VPN Type	Disable
Initial Service IP	
Virtual IP Address	

<b>PC Port Status</b>	
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

Status	<b>Network</b>	Wireless	SIP	FXS1	FXS2	Security	Application	Storage	
WAN	LAN	MAC Clone	VPN	DMZ	Port Forward	Advance	Port Setting	QoS	Routing

**PC Port(LAN)**

PC Port(LAN)

Local IP Address:

Local Subnet Mask:

Local DHCP Server:

DHCP Start Address:

DHCP End Address:

DNS Mode:

Primary DNS:

Secondary DNS:

Client Lease Time(0-86400s):

DHCP Static Allotment

NO.	MAC	IP Address
1	<input type="text"/>	<input type="text"/>
2	<input type="text"/>	<input type="text"/>
3	<input type="text"/>	<input type="text"/>

DNS Proxy:

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: <ol style="list-style-type: none"><li>1. When DNS mode is Auto, the device under LAN port will automatically obtains the preferred DNS and alternate DNS.</li><li>2. When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS.</li></ol>
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)	
<b>PC Port(LAN)</b>	
Local IP Address	<input type="text" value="192.168.11.1"/>
Local Subnet Mask	<input type="text" value="255.255.255.0"/>
Local DHCP Server	<input type="text" value="Enable"/>
DHCP Start Address	<input type="text" value="192.168.11.2"/>
DHCP End Address	<input type="text" value="192.168.11.254"/>
DNS Mode	<input type="text" value="Auto"/>

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

**Table 25** DHCP server, DNS and Client Lease Time

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

Field Name	Description
Primary DNS	Specify the Primary DNS address provided by your ISP. If your ISP does not provide it, the 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

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage	
WAN	LAN	MAC Clone	VPN	DMZ	Port Forward	Advance	Port Setting	QoS	Routing

**MAC Address Clone**

MAC Address Clone  Disable ▾

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

## VPN

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

**Table 27** VPN

Status	<b>Network</b>	Wireless	SIP	FXS1	FXS2	Security	Application	Storage	
WAN	LAN	MAC Clone	VPN	DMZ	Port Forward	Advance	Port Setting	QoS	Routing

**VPN Settings**

**Administration**

VPN Enable

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

Status	<b>Network</b>	Wireless	SIP	FXS1	FXS2	Security	Application	Storage	
WAN	LAN	MAC Clone	VPN	DMZ	Port Forward	Advance	Port Setting	QoS	Routing

**Demilitarized Zone (DMZ)**

**DMZ Setting**

DMZ Enable

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

The screenshot shows a web-based configuration interface. At the top, there is a navigation bar with tabs for 'Status', 'Network', 'Wireless', 'SIP', 'FXS1', 'FXS2', 'Security', 'Application', 'Storage', and 'Ad'. Below this, a secondary menu has tabs for 'WAN', 'LAN', 'VPN', 'Port Forward', 'DMZ', 'DDNS', 'QoS', 'MAC Clone', 'Port Setting', and 'Routing'. The 'DDNS' tab is selected, and the page title is 'DDNS Setting'. The main content area contains the following fields:

- Dynamic DNS Provider:** A dropdown menu currently showing 'None'.
- Account:** A text input field.
- Password:** A text input field.
- DDNS URL:** A text input field.
- Status:** A label indicating '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

Status Network Wireless SIP FXS1 FXS2 Security Application Storage Administration

WAN LAN MAC Clone VPN DMZ Port Forward Advance Port Setting QoS Routing

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

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage	
WAN	LAN	MAC Clone	VPN	DMZ	Port Forward	Advance	Port Setting	QoS	Route

Most Nat connections(512-8192)	4096
Mss Mode	<input type="radio"/> Manual <input checked="" type="radio"/> Auto
Mss Value(1260-1460)	1260
AntiDos-P	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP conflict detection	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
IP Conflict Detecting Interval(0-3600)	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

Status	<b>Network</b>	Wireless	SIP	FXS1	FXS2	Security	Application	Storage	
WAN	LAN	MAC Clone	VPN	DMZ	Port Forward	Advance	Port Setting	QoS	Routin

**Port Setting**

**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

WAN	LAN	VPN	Port Forward	DMZ	QoS	MAC Clone	Port Setting	Routing	Advance						
<b>QoS setting</b>															
<b>QoS setting</b>															
QoS Enable		Disable ▾													
Upstream		<input type="text"/> (0-102400)kbit/s													
Downstream		<input type="text"/> (0-102400)kbit/s													
					Save		Cancel								
Condition										Action					
Name	Src.IP Address	Dst.IP Address	Protocol	Src.Port Range	Dst.Port Range	Physical Port	DSCP	802.1p	VLAN ID	Remark DSCP	Remark 802.1p	Remark VLAN_ID	Priority	Drop	Rate Limit
										Delete Selected		Add			

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



### Note

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

# Routing

**Table 34** Routing

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

**Static Routing Settings**

**Add a routing rule**

Destination

Host/Net

Gateway

Interface

Comment

**Current Routing table in the system**

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

**Help**

You may add or remove 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

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage	Administration
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced			

**Basic Wireless Settings**
Help

**Wireless Network**

Radio On/Off:

Wireless Connection Mode:

Network Mode:

Multiple SSID: CAMBIUM\_2.4GHZ\_1 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):

HT Physical Mode:  Mixed Mode  Green Field

Operating Mode:  20  20/40

Channel BandWidth:  Long  Short

Guard Interval:  Long  Short

Reverse Direction Grant(RDG):  Disable  Enable

STBC:  Disable  Enable

Aggregation MSDU(A-MSDU):  Disable  Enable

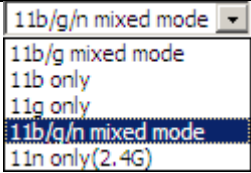
Auto Block ACK:  Disable  Enable

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

	
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	<ol style="list-style-type: none"> <li>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</li> <li>2. Green Field: high throughput can be achieved, but it will affect backward compatibility, and security of the system</li> </ol>
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)	<p><b>Enabled:</b> 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)</p> <p><b>Disabled:</b> Devices on the WLAN must make a request for transmit when communicating with another device on the network</p>
STBC	Space-time Block Code

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

# Wireless Security

**Table 36** Wireless security

Status
Network
Wireless
SIP
FXS1
FXS2
Security
Application
Storage
Ad

Basic
Wireless Security
WMM
WDS
WPS
Station Info
Advanced

**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 privacy of your wireless data packets. Each encryption mode will bring out different web page and ask you to offer additional configuration.

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

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

**Table 37 WiFi Security Setting**

Status	Network	<b>Wireless</b>	SIP	FXS1	FXS2	Security	Application	Storage
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		

**WiFi Security Setting**

Select SSID

SSID choice: CAMBIUM\_2.4GHz\_027898 ▼  
 "CAMBIUM\_2.4GHz\_027898"

Security Mode: WPA2-PSK ▼

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

The screenshot shows a configuration window for 'Access policy'. The 'Policy' dropdown menu is open, displaying four options: 'Allow', 'Disable', 'Allow' (which is highlighted with a blue selection bar), and 'Reject'. Below the dropdown menu, there are three buttons: 'Save', 'Cancel', and 'Reboot'. The background of the window is light gray, and the text is in a standard sans-serif font.

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

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

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

### Description

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



## WDS

Table 42 WDS

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

**WDS Setting**

**WDS Config**

WDS Mode

**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

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

**WPS Setting**

WPS Config

WPS  ▾

---

**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 <input type="button" value="Generate"/>

---

**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	<ul style="list-style-type: none"> <li><b>CnPilot</b> Home R200x uses default security policy to allow other non-WPS users to access and apply.</li> </ul>

- 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

The screenshot shows a web-based configuration interface for a wireless device. The top navigation bar includes tabs for Status, Network, **Wireless**, SIP, FXS1, FXS2, Security, Application, Storage, and Adm. Under the Wireless tab, there are sub-tabs for Basic, Wireless Security, WMM, WDS, WPS, **Station Info**, and Advanced. The Station Info page is displayed, showing the following information:

**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

Status	Network	<b>Wireless</b>	SIP	FXS1	FXS2	Security	Application	Storage
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced		

**Advanced Wireless**

**Advanced Wireless**

BG Protection Mode Auto ▾

Beacon Interval 100 ms (range 20 - 999, default 100)

Data Beacon Rate (DTIM) 3 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

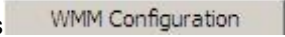
APSD Capable  Enable  Disable

Multicast-to-Unicast Converter

Multicast-to-Unicast  Enable  Disable

Save Cancel Reboot

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 1,2Mbps
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.
<b>Wi-Fi Multimedia (WMM)</b>	
WMM Capable	Enable/Disable WMM.
APSD Capable	Enable/Disable APSD. Once it is enabled, it may affect wireless performance, but can play a role in energy-saving power
WMM Parameters	Press  , the webpage will jump to the configuration page of Wi-Fi multimedia.
Multicast-to-Unicast Converter	Enable/Disable Multicast-to-Unicast. By default, it is Disabled.

# Wireless Security

**Table 46** Wireless security

Status	Network	<b>Wireless</b>	SIP	FXS1	FXS2	Security	Application	Storage	Ad
Basic	Wireless Security	WMM	WDS	WPS	Station Info	Advanced			

**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 [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

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage
SIP Settings		VoIP QoS						
<b>SIP Parameters</b>								
<b>SIP Parameters</b>								
SIP T1	<input type="text" value="500"/>	MS	Max Forward	<input type="text" value="70"/>				
SIP Reg User Agent Name	<input type="text"/>		Max Auth	<input type="text" value="2"/>				
Reg Retry Intvl	<input type="text" value="30"/>	sec	Reg Retry Long Intvl	<input type="text" value="1200"/>	sec			
Mark All AVT Packets	<input type="text" value="Enable"/>		RFC 2543 Call Hold	<input type="text" value="Enable"/>				
S RTP	<input type="text" value="Disable"/>		S RTP Prefer Encryption	<input type="text" value="AES_CM"/>				
Service Type	<input type="text" value="Common"/>							
<b>Response Status Code Handling</b>								
Retry Reg RSC	<input type="text"/>							
<b>NAT Traversal</b>								
<b>NAT Traversal</b>								
NAT Traversal	<input type="text" value="Disable"/>		STUN Server Address	<input type="text"/>				
NAT Refresh Interval(sec)	<input type="text" value="60"/>		STUN Server Port	<input type="text" value="3478"/>				
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Reboot"/>								

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	<ol style="list-style-type: none"> <li>1. Enable/Disable NAT Traversal</li> <li>2. cnPilot Home R200x/R201x supports STUN Traversal; if user wants to traverse NAT/Firewall, select the STUN.</li> </ol>
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

The screenshot displays the configuration page for VoIP QoS. The top navigation bar includes tabs for Status, Network, Wireless, SIP (selected), FXS1, FXS2, Security, Application, and Storage. Below this, there are sub-tabs for SIP Settings and VoIP QoS. The main content area is titled 'QoS Settings' and contains a section for 'Layer 3 QoS'. This section has two rows: 'SIP QoS(0-63)' with a value of 46, and 'RTP QoS(0-63)' with a value of 46. At the bottom of the configuration area, there are three buttons: 'Save', 'Cancel', and 'Reboot'.

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

Status	Network	Wireless	SIP	<b>FXS1</b>	FXS2	Security	Application	Storage
<div style="background-color: #4a7ebb; color: white; padding: 2px;"> <span style="background-color: white; color: #4a7ebb; padding: 2px;">SIP Account</span> <span style="background-color: white; color: #4a7ebb; padding: 2px;">Preferences</span> <span style="background-color: white; color: #4a7ebb; padding: 2px;">Dial Plan</span> <span style="background-color: white; color: #4a7ebb; padding: 2px;">Blacklist</span> <span style="background-color: white; color: #4a7ebb; padding: 2px;">Call Log</span> </div>								
<b>Basic</b>								
<b>Basic Setup</b> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 45%;">           Line Enable <input type="text" value="Disable"/> </div> <div style="width: 45%;">           Peer To Peer <input type="text" value="Disable"/> </div> </div>								
<b>Proxy and Registration</b> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 45%;">           Proxy Server <input type="text"/> </div> <div style="width: 45%;">           Proxy Port <input type="text" value="5060"/> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 45%;">           Outbound Server <input type="text"/> </div> <div style="width: 45%;">           Outbound Port <input type="text" value="5060"/> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 45%;">           Backup Outbound Server <input type="text"/> </div> <div style="width: 45%;">           Backup Outbound Port <input type="text" value="5060"/> </div> </div>								
<b>Subscriber Information</b> <div style="display: flex; justify-content: space-between; margin-top: 10px;"> <div style="width: 45%;">           Display Name <input type="text"/> </div> <div style="width: 45%;">           Phone Number <input type="text"/> </div> </div> <div style="display: flex; justify-content: space-between; margin-top: 5px;"> <div style="width: 45%;">           Account <input type="text"/> </div> <div style="width: 45%;">           Password <input type="text"/> </div> </div>								
Field Name	Description							
Line Enable	Enable/Disable the line.							
Peer To Peer	Enable/Disable PEER to PEER. If enabled, SIP-1 will not send register request to SIP server; but in Status/SIP Account Status webpage, Status is Registered; lines 1 can dial out, but the external line number cannot 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 ▼
gpmid 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	<input type="text" value="Enable"/>	Hot Line	<input type="text"/>
MWI Enable	<input type="text" value="Enable"/>	Voice Mailbox Numbers	<input type="text"/>
MWI Subscribe Enable	<input type="text" value="Disable"/>	VMWI Serv	<input type="text" value="Enable"/>
DND	<input type="text" value="Disable"/>		

**Speed Dial**

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

Field Name	Description
Call Waiting	Enable/Disable Call Waiting
Hot Line	Fill in the hotline number. Pickup handset or press hands-free or headset button, the device will dial out the hotline number automatically.
MWI Enable	Enable/Disable MWI (message waiting indicate). If the user needs to user voice mail, please enable this feature.
MWI Subscribe Enable	Enable/Disable MWI Subscribe

Voice Mailbox Numbers	Fill in the voice mailbox phone number, Asterisk platform, for example, its default voice mail is *97
VMWI Serv	Enable/Disable VMWI service.
DND	Enable/Disable DND (do not disturb). If enable, any phone call cannot arrive at the device; default is disable.
Speed Dial	Enter the speed dial phone numbers. Dial *74 to active speed dial function. Then press the speed dial numbers, for example, press 2, phone dials 075526099365 directly.

## Advanced

**Table 52** Advanced

**Advanced**

**Advanced Setup**

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

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 Interval	The interval between two normal Register messages. You can use the default setting.
RTP Port	Set the port to send RTP. The device will select one idle port for RTP if you set "0"; otherwise use the value which user sets.
Cancel Message Enable	When you set enable, an unregistered message will be sent before registration, while you set disable, unregistered message will not be sent before registration. You should set the option for different Proxy.
Session Refresh Time(sec)	Time interval between two sessions, you can use the default settings.
Refresher	Choose refresher from UAC and UAS.
Prack Enable	Enable/Disable prack.
SIP OPTIONS Enable	When you set enable, the device will send SIP-OPTION to the server, instead of sending periodic Hello message. The sending interval is Keep-alive interval.
Primary SER Detect Interval	Test interval of the primary server, the default value is 0, it represents disable.
Max Detect Fail Count	Interval of detection of the primary server fail; the default value is 3, it means that if detect 3 times fail; the device will no longer detect the primary server.
Keep-alive Interval(10-60s)	The interval that the device will send an empty packet to proxy.
Anonymous Call	Enable/Disable anonymous call.
Anonymous Call Block	Enable/Disable anonymous call block.
Proxy DNS Type	Set the DNS server type, choose from A type and DNS SRV.
Use OB Proxy In Dialog	If or not use OB Proxy In Dialog.
Reg Subscribe Enable	If enable, subscribing will be sent after registration message, if not enable, do not send subscription.

Dial Prefix	The number will be added before your telephone number when making calls.
User Type	Choose the User Type from IP and Phone.
Hold Method	Choose the Hold Method from ReINVITE and INFO.
Request-URI User Check	Enable/Disable the user request URI check.
Only Recv request from server	Enable/Disable the only receive request from server.
Server Address	The IP address of SIP server.
SIP Received Detection	Enable/Disable SIP Received Detection, if enable, use it to confirm the public network address of the device.

## Preferences

### Volume Settings

**Table 53** Volume settings

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.

**Preferences**

**Volume Settings**

Handset Input Gain  Handset Volume

## Regional

**Table 54 Regional**

**Regional**

Tone Type	USA ▼		
Dial Tone	<input type="text"/>		
Busy Tone	<input type="text"/>		
Off Hook Warning Tone	<input type="text"/>		
Ring Back Tone	<input type="text"/>		
Call Waiting Tone	<input type="text"/>		
Min Jitter Delay(ms)	<input type="text" value="0"/>	Max Jitter Delay(ms)	<input type="text" value="80"/>
Ringing Time(sec)	<input type="text" value="60"/>		
Ring Waveform	Sinusoid ▼	Ring Voltage(40-63 Vrms)	<input type="text" value="45"/>
Ring Frequency	<input type="text" value="25"/>	VMWI Ring Splash Len(sec)	<input type="text" value="0.5"/>
Flash Time Max(sec)	<input type="text" value="0.9"/>	Flash Time Min(sec)	<input type="text" value="0.1"/>

Field Name	Description
Tone Type	Choose tone type form China, US, Hong Kong and so on.
Dial Tone	Dial Tone
Busy Tone	Busy Tone
Off Hook Warning Tone	Off Hook warning tone
Ring Back Tone	Ring back tone
Call Waiting Tone	Call waiting tone
Min Jitter Delay	The Min value of home gateway's jitter delay, home gateway is an adaptive jitter mechanism.
Max Jitter Delay	The Max value of home gateway's jitter delay, home gateway is an adaptive jitter mechanism.
Ringing Time	How long 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	<input type="text" value="Disable"/>	Busy Forward	<input type="text" value="Disable"/>
No Answer Forward	<input type="text" value="Disable"/>		

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

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

Field Name	Description
Features	All Forward Enable/Disable forward all calls
	Busy Forward Enable/Disable busy forward.
	No Answer Forward Enable/Disable no answer forward.
Call Forward	All Forward Set the target phone number for all forward. The device will forward all calls to the phone number immediately when there is an incoming call.
	Busy Forward The phone number which the calls will be forwarded to when line is busy.
	No Answer Forward The phone number which the call will be forwarded to when there's no answer.
	No Answer Timeout The seconds to delay forwarding calls, if there is no answer at your phone.
Feature Code	Hold key code Call hold signatures, default is *77.
	Conference key 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	<input type="text" value="26"/>
CID Service	<input type="button" value="Enable"/>
Caller ID Method	<input type="button" value="Bellcore"/>
Dial Time Out(IDT)	<input type="text" value="5"/>
ICMP Ping	<input type="button" value="Disable"/>
Bellcore Style 3-Way Conference	<input type="button" value="Disable"/>
Impedance Maching	<input type="button" value="US PBX,Korea,Taiwan(600)"/>
CWCID Service	<input type="button" value="Disable"/>
Polarity Reversal	<input type="button" value="Disable"/>
Call Immediately Key	<input type="button" value="#"/>
Escaped char enable	<input type="button" value="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

Status	Network	Wireless	SIP	<b>FXS1</b>	FXS2	Security	Application	Storage
<div style="display: flex; justify-content: space-between;"> <span>SIP Account</span> <span>Preferences</span> <span><b>Dial Plan</b></span> <span>Blacklist</span> <span>Call Log</span> </div>								
<b>Dial Plan</b>								
<b>General</b>								
Dial Plan <input type="text" value="Disable"/>								
Unmatched Policy <input type="text"/>								
No.	FXS	Digit Map			Action	Move Up	Move Down	
1	FXS 1	Line1			Dial Out			<input type="checkbox"/>
FXS <input type="text" value="FXS 1"/>								
Digit Map <input type="text"/>								
Action <input type="text" value="Deny"/>								
<input type="button" value="OK"/> <input type="button" value="Cancel"/>								
<input type="button" value="Save"/> <input type="button" value="Cancel"/> <input type="button" value="Reboot"/>								

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					
<b>General</b>					
Dial Plan	Disable ▼				
Unmatched Policy	▼				
No.	FXS	Digit Map	Action	Move Up	Move Down
	FXS	FXS 1 ▼			
	Digit Map	<input type="text"/>			
	Action	Deny ▼			
<input type="button" value="OK"/> <input type="button" value="Cancel"/>					
Description					
Step 1. Enable Dial Plan					
Step 2. Click Add button, and the configuration table					
Step 3. Fill in the value of parameters.					
Step 4. Press OK button to end configuration.					

## Dial Plan Syntactic

**Table 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 $x^0, x^1, x^2, x^3, \dots, x^n$ For example: "01.":can match "0", "01", "011", "0111", ....., "01111..."

---

5	<dialcd:substituted>	Replace dialcd 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 : "9,1xxxxxxxxx":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			
<b>Blacklist Upload &amp;&amp; Download</b>			
Local File <input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload CSV"/> <input type="button" value="Download CSV"/>			
Blacklist			
Index	Name	Number	<input type="checkbox"/>
1	Rob	12345	<input type="checkbox"/>
2	Henry	123456	<input type="checkbox"/>
<input type="button" value="Edit"/> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="Move to phonebook"/>			
Description			
Click <input type="button" value="浏览..."/> to select the blacklist file and click <input type="button" value="upload CSV"/> to upload it to CnPilot Home; Click <input type="button" value="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

Number

---

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

### Redial List

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



---

**Answered Calls**

---

**Missed Calls**

Index	NUMBER	Start Time	Duration	<input type="checkbox"/>
1	110	10/21 09:50	00:00:03	<input type="checkbox"/>
2	555	10/22 12:04	00:00:03	<input type="checkbox"/>

---

**Missed Calls**

---

## FXS2

---

The settings of FXS2 are the same as FXS1. See [FXS1](#) on page 81.

# Security

## Filtering Setting

**Table 62** Filtering setting

Basic Settings	
Filtering	Disable ▾
Default Policy	Drop ▾
The packet that don't match with any rules would beDrop	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	
IP/Port Filter Settings	
Mac address	<input type="text"/>
Dest IP Address	<input type="text"/>
Source IP Address	<input type="text"/>
Protocol	NONE ▾
Dest. Port Range	<input type="text"/> - <input type="text"/>
Src Port Range	<input type="text"/> - <input type="text"/>
Action	Drop ▾
Comment	<input type="text"/>
( The maximum rule count is 32 )	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

# Content Filtering

**Table 63** Content filtering

Status	Network	Wireless	SIP	FXS1	FXS2	<b>Security</b>	Application	Storage
Filtering Setting		Content Filtering						

**Basic Settings**

**Basic Settings**

Filtering Disable ▼

Default Policy Accept ▼

**Webs URL Filter Settings**

**Current Webs URL Filters**

No.	URL

**Add a URL Filter**

URL

**Webs Host Filter Settings**

**Current Website Host Filters**

No.	Keyword

**Add a Host(keyword) Filter**

Keyword

<b>Field Name</b>	<b>Description</b>
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

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

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

**MLD****Table 66 MLD**

**MLD**

**MLD Setting**

MLD enable

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

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage								
<div style="display: flex; justify-content: space-between;"> <span>Disk Management</span> <span>Ftp Setting</span> <span>Smb Setting</span> </div>																
<div style="border: 1px solid #ccc; padding: 10px;"> <p><b>Disk Management</b></p> <p><b>Folder List</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 70%;">Directory Path</th> <th style="width: 30%;">Partition</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;"> <input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="RemoveDisk"/> </td> </tr> </tbody> </table> <p><b>Partition Status</b></p> <table border="1" style="width: 100%; border-collapse: collapse;"> <thead> <tr> <th style="width: 35%;">Partition</th> <th style="width: 65%;">Path</th> </tr> </thead> <tbody> <tr> <td colspan="2" style="text-align: center;"> <input type="button" value="Format"/> <input type="button" value="Re-allocate"/> </td> </tr> </tbody> </table> </div>									Directory Path	Partition	<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="RemoveDisk"/>		Partition	Path	<input type="button" value="Format"/> <input type="button" value="Re-allocate"/>	
Directory Path	Partition															
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="RemoveDisk"/>																
Partition	Path															
<input type="button" value="Format"/> <input type="button" value="Re-allocate"/>																
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

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	<b>Storage</b>
Disk Management		Ftp Setting		Smb Setting				

### FTP Setting

#### FTP Server Setup

FTP Server	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
FTP Server Name	<input type="text" value="FTP"/>
Anonymous Login	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
FTP Port	<input type="text" value="21"/>
Max. Sessions	<input type="text" value="10"/>
Create Directory	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Rename File/Directory	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Remove File/Directory	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Read File	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Write File	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Download Capability	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Upload Capability	<input checked="" type="radio"/> Enable <input type="radio"/> 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

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	<b>Storage</b>
Disk Management		Ftp Setting	Smb Setting					

**SMB Setting**

**SAMBA Server Setup**

SAMBA Server	<input type="radio"/> Enable <input checked="" type="radio"/> 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

Save Config File	
<b>Config File Upload &amp;&amp; Download</b>	
Local File	<input type="button" value="Choose File"/> No file chosen <input type="button" value="Upload"/> <input type="button" value="Download"/>


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	
<b>Password Reset</b>	
User Type	Admin User ▾
New User Name	admin
New Password	<input type="text"/> (The maximum length is 25)
Confirm Password	<input type="text"/>
<b>Language</b>	
Language	English ▾
<b>VPN Access</b>	
Management Using VPN	Disable ▾
<b>Web Access</b>	
Remote Web Login	Enable ▾
Web Port	80
Web Idle Timeout(0 - 60m)	5
Allowed Remote IP(IP1;IP2;...)	0.0.0.0
<b>Telnet Access</b>	
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
	 <b>Note</b> Telnet access is disabled by default.
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 ▼

Option 42 Disable ▼

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

Sync with host

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

Primary NTP Server

Secondary NTP Server

NTP synchronization(1 - 1440min)

**Daylight Saving Time**

Daylight Saving Time Disable ▼

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

---

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

---

## Daylight Saving Time

**Table 73** Daylight Saving Time

Daylight Saving Time	
Daylight Saving Time	Enable ▾
Offset	60 <input type="text"/> Min.
Start Month	April ▾
Start Day of Week	Sunday ▾
Start Day of Week Last in Month	First in Month ▾
Start Hour of Day	2 <input type="text"/>
Stop Month	October ▾
Stop Day of Week	Sunday ▾
Stop Day of Week Last in Month	Last in Month ▾
Stop Hour of Day	2 <input type="text"/>

### 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	<input type="text"/>

Field Name	Description
Syslog Enable	Enable/Disable syslog function
Syslog Level	Select the system log, there is INFO and Debug two grades, the Debug INFO can provide more information.

Remote Syslog Enable	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	
<p><b>Factory Defaults Setting</b></p> <p>Factory Defaults Lock <input type="button" value="Disable ▼"/></p>	
Description	
<p>When enabled, the device may not be reset to factory defaults until this parameter is reset to Disable.</p>	

## Factory Defaults

**Table 76** Factory Defaults

Factory Defaults	
Reset to Factory Defaults	<input type="button" value="Factory Default"/>
Description	
<p>Click Factory Default to restore the residential gateway to factory settings.</p>	



# Firmware Upgrade

**Table 77** Firmware upgrade

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage
Management	Firmware Upgrade	Certification	Provision	SNMP	TR069	Cambium Network Ma		
Operating Mode								

## Firmware Management

### Firmware Upgrade

Upgrade Types

Local Upgrade  No file chosen

### Description

1. Choose upgrade file type from Image File and Dial Rule
2. Press "Browse.." button to browser file
3. Press  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

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

**Table 78** Provision

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage
Management	Firmware Upgrade	Certification	Provision	SNMP	TR069	Cambium Network Ma		
Operating Mode								

### 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(sec)	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 79 Firmware Upgrade**

**Firmware Upgrade**

Upgrade Enable	Enable ▾
Upgrade Error Retry Delay(sec)	3600
Upgrade Rule	<input type="text"/>

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 80** SNMP

Management	Firmware Upgrade	Certification	Provision	SNMP	TR069	Cambium Network Ma
Operating Mode						

## SNMP Configuration

### SNMP Configuration

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

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

## TR-069

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

### Device Configuration using TR-069

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

**Table 81** TR069

Management	Firmware Upgrade	Certification	Provision	SNMP	TR069	Cambium Network Man
Operating Mode						

**TR069 Configuration**

**ACS**

TR069 Enable

CWMP

ACS URL

User Name

Password

Periodic Inform Enable

Periodic Inform Interval

**Connect Request**

User Name

Password

Field Name	Description
<b>ACS parameters</b>	
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
<b>Connect Request parameters</b>	
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.

## Friendly Platform Operation

### Login Friendly Platform

Enter the friendly server URL in the browser:

<http://testui.friendly-tech.com/CPEAdmin/>

Account and password are provided by the server:

**Account : flyingvoice password : flying11**

Enter TR069 server interface, As shown in Figure :

The screenshot shows the 'Update a CPE' page in the FriendlyTR69 Suite Management Console. The page includes a navigation menu on the left with options like 'List', 'Search', 'Device Info', 'Device Settings', 'Advanced View', 'Provision Manager', 'Software Manager', 'Device Monitoring', 'File Download', 'File Upload', 'Port Mapping', 'Device Diagnostics', 'Custom RPC', 'Device History', and 'Device Activity'. The main content area displays a table of devices with columns for Manufacturer, Model name, Serial, Created, Updated, Firmware, Pending tasks, and Status. The table contains 14 rows of device data.

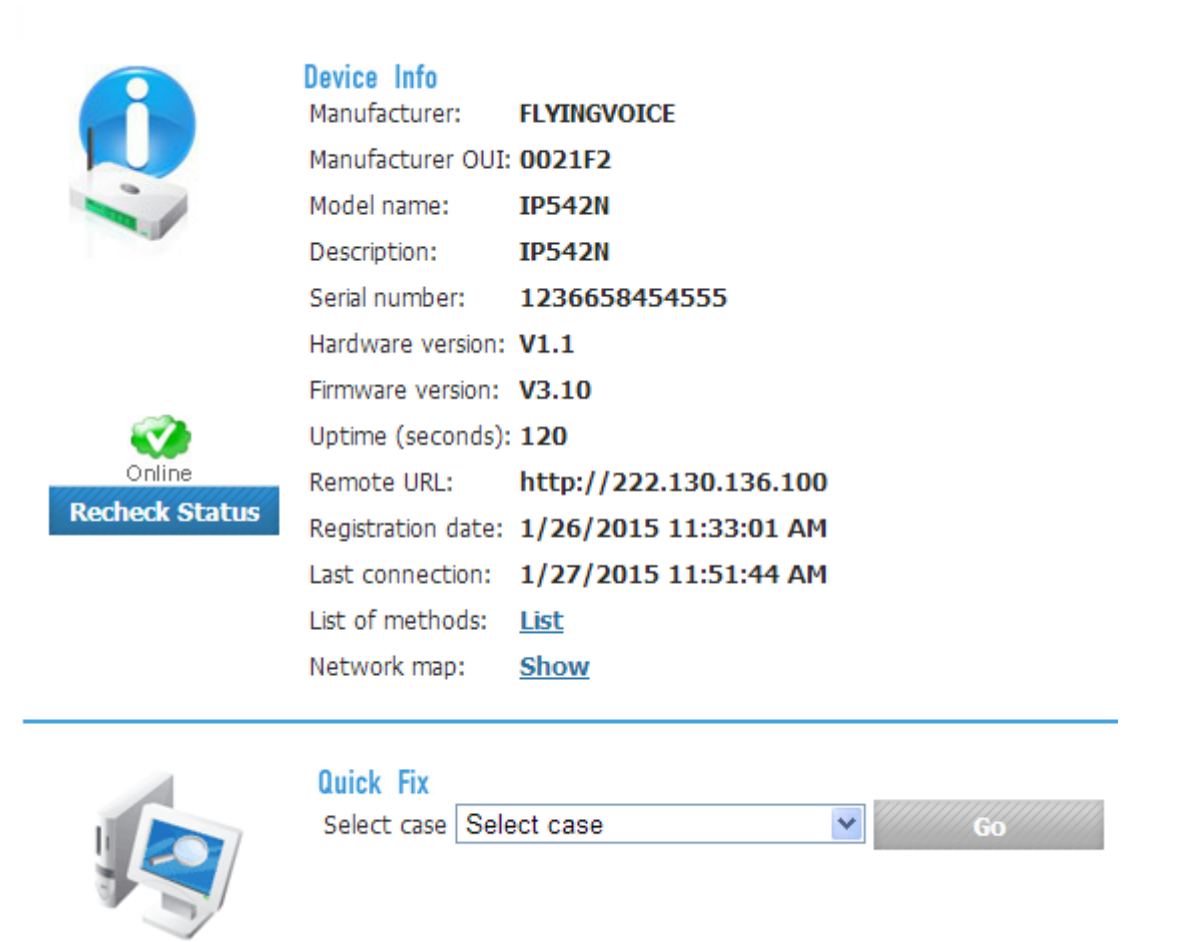
	Manufacturer	Model name	Serial	Created	Updated	Firmware	Pending tasks	Status
<input type="checkbox"/>	Dune HD	STB_SMP	0000-0000-2FAC-02AA-2600-E36E-80E9-7140	12/15/2014 2:15:34 PM	1/16/2015 8:19:15 AM	141209_1757_r10		1
<input type="checkbox"/>	Dune HD	STB_SMP	0000-0000-00E2-00AA-2600-13C5-4388-E226	12/30/2014 1:35:14 PM	1/16/2015 8:19:11 AM	141128_2027_r10		1
<input type="checkbox"/>	Yeastar	NeoGate-TA	02E907019011	12/29/2014 10:48:16 AM	1/16/2015 8:19:11 AM	40.19.99.10-beta01		1
<input type="checkbox"/>	Dune HD	STB_SMP	0000-0000-9626-02AA-2600-4939-97EB-D1C4	12/30/2014 1:32:11 PM	1/16/2015 8:18:59 AM	141209_1757_r10		1
<input type="checkbox"/>	Gemtek	Lte VoIP Gateway	GMH120726000105	12/3/2014 7:31:14 PM	1/16/2015 8:18:35 AM	01.01.02.010		1
<input type="checkbox"/>	Gemtek	Lte VoIP Gateway	GMH120726000158	12/3/2014 4:15:26 PM	1/16/2015 8:18:19 AM	01.01.02.010		1
<input type="checkbox"/>	HUAWEI	BM2022	0C4C39893587	12/9/2014 9:17:51 PM	1/16/2015 8:18:18 AM	V100R001C01SPC100		1
<input type="checkbox"/>	Arcadyan	PR711AAW	J250204772	12/5/2014 3:00:32 PM	1/16/2015 8:18:18 AM	ARCTFI_CCD100_R10.11		1
<input type="checkbox"/>	Comtrend	PG-9172	131162000017	9/25/2014 12:17:45 PM	1/16/2015 8:18:17 AM	COMTRD_9172_R1.1		1
<input type="checkbox"/>	Marvell	Product class	LCD913D1017770	1/15/2015 6:49:33 PM	1/16/2015 8:18:17 AM	NZ_CP_1.40.000		1
<input type="checkbox"/>	Arcadyan	PR711AAW	.....	12/20/2014 3:09:22 PM	1/16/2015 8:18:16 AM			1
<input type="checkbox"/>	Netopix, Inc.	3347-02	157982862944	12/24/2013 12:46:12 AM	1/16/2015 8:17:51 AM	7.8.1r2		1
<input type="checkbox"/>	Comtrend	PG-9171n	R7D9W1404001380	12/30/2014 1:35:19 PM	1/16/2015 8:17:43 AM	COMTRD_9171nW_R5.5		0

### Search Device

1. Click on the Search menu. Then select the Serial Number, and fill in the equipment S/N, then click Search.

The screenshot shows the 'Update a CPE' search interface. It includes a 'Search By' dropdown menu set to 'Default', a 'Serial Number' dropdown menu, and a search input field containing the serial number '1236658454555'. The 'Search match only' checkbox is checked. The 'Search' button is highlighted.

- Click on the Device Info menu item, and you can see basic information about the test equipment. As shown in Figure : (Button on the bottom of the device can perform basic operations, such as reboot.)



**Device Info**

Manufacturer: **FLYINGVOICE**

Manufacturer OUI: **0021F2**

Model name: **IP542N**

Description: **IP542N**

Serial number: **1236658454555**

Hardware version: **V1.1**

Firmware version: **V3.10**

Uptime (seconds): **120**

Remote URL: **http://222.130.136.100**

Registration date: **1/26/2015 11:33:01 AM**

Last connection: **1/27/2015 11:51:44 AM**

List of methods: [List](#)

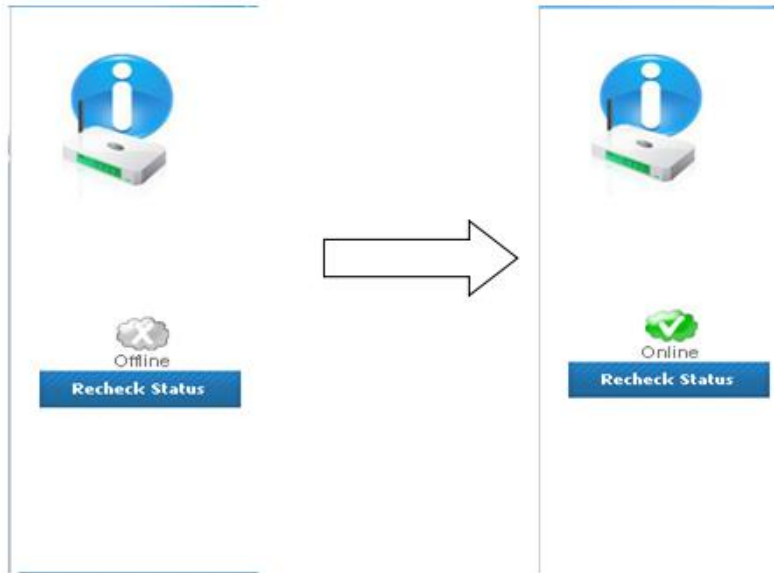
Network map: [Show](#)

---

**Quick Fix**

Select case

- If the device is properly connected server,offline will be online. That is a successful connection :



If you could not find the device in the list, please check if the device WEB page filled in correctly.

### Get Device Info

Click on the Advanced View menu button, you can do some node. As shown in Figure:

- [-] Device
- [-] DeviceInfo
- [-] GatewayInfo
- [-] LAN
- [-] ManagementServer
- [-] Services
- [-] VoiceService
- [-] VoiceService.1
- [-] Capabilities
- [-] VoiceProfile
- [-] VoiceProfile.1
- [-] Line
- [-] Line.1
- [-] Codec
- [-] Session
- [-] SIP
- [-] Stats
- [-] RTP
- [-] SIP
- [-] VoiceProfile.2
- [-] VoiceProfile.3
- [-] VoiceProfile.4
- [-] Time
- [-] UserInterface
- [-] X\_0021F2\_Syslog

Device.Services.VoiceService.1.VoiceProfile.1.Line.1.SIP

Parameter name	Parameter value	Notification	Access list	Polling
AuthPassword	*****	Off	ACS only	<input type="checkbox"/>
AuthUserName	555	Off	ACS only	<input type="checkbox"/>
URI		Off	ACS only	<input type="checkbox"/>

Edit
Get Current
Edit Tree
Save Parameters

#### 1. Get AuthUserName of line1

Click on the top menu options and parameter values can be obtained depending on the options in the form. For example, if you want to get AuthUserName of line1, VOIP need to select the menu, and click Options VoiceProfile.1 next sip, you can get the value in the right AuthUserName.



Information Management LAN **VoIP**

Services

- VoiceService
  - VoiceService.1
    - VoiceProfile
      - VoiceProfile.1
        - SIP
          - RTP
            - Line
              - Line.1
                - SIP**
                - Codec

Device.Services.VoiceService.1.VoiceProfile.1.Line.1.SIP

Parameter name	Parameter value
AuthUserName	555
AuthPassword	*****
URI	

## 4.4 Set Device Info

### 1. Set ProxyServer

The lower end of the button "Edit" can set new values for writable nodes. After clicking edit, fill in the new value directly in the box Parameter value field after the node name. For example, if set ProxyServer of Line1, the current value is followed:

Device

- DeviceInfo
- GatewayInfo
- LAN
- Stats
- ManagementServer
- Services
  - VoiceService
    - VoiceService.1
      - Capabilities
      - VoiceProfile
        - VoiceProfile.1
          - Line
            - Line.1
              - Codec
              - Session
              - SIP
              - Stats
              - RTP
              - SIP**
              - VoiceProfile.2
              - VoiceProfile.3
              - VoiceProfile.4
- Time
- UserInterface
  - X\_0021F2\_Syslog

Device.Services.VoiceService.1.VoiceProfile.1.Line.1.SIP

Parameter name	Parameter value
Organization	
OutboundProxy	
OutboundProxyPort	5060
ProxyServer	192.168.10.1
ProxyServerPort	5060
ProxyServerTransport	UDP
RegisterExpires	3600
RegistrarServer	192.168.10.1

Then click edit, and fill in the new ProxyServer.

OutboundProxyPort	<input type="text" value="5060"/>
ProxyServer	<input type="text" value="192.168.10.141"/>
ProxyServerPort	<input type="text" value="5060"/>

Click to send update after modification.

Parameter name	Parameter value
Organization	
OutboundProxy	
OutboundProxyPort	5060
ProxyServer	192.168.10.141
ProxyServerPort	5060
ProxyServerTransport	UDP
RegisterExpires	3600
RegistrarServer	192.168.10.1

### 4.5 Firmware Upgrade

Under is firmware upgrading operation on FreeACS.

#### 1. Equipment connection configure

Please REBOOT to make the changes effective!

**TR069 Configuration**

**ACS**

TR069 Enable:

CWMP:

ACS URL:

User Name:

Password:

Periodic Inform Enable:

Periodic Inform Interval:

**Connect Request**

User Name:

Password:

Buttons: Save, Cancel, Reboot

**Help**

**TR069 Configuration:**  
Allow the device to be managed by the ACS server which is set in the ACS URL.

If the connection is successful, you will see the following pages.

FreeACS Web admin@182.92.234.149 Permissions | Monitor | About | Help | Logout

Context navigation: IP542N Default user\_ip542n Select action:

**Unit dashboard**

Basic information

- Unit Type:** IP542N
- Profile:** Default
- Serial Number:** user\_ip542n
- Software Version:** V3.10(201501270031)
- Public IP address:** 114.253.252.235
- Behind Gateway/NAT:** No
- Supports TR-111:** No

Go to Unit configuration

Current status

- First Management:** 2015-01-27 18:13:58
- Last Management:** 2015-01-27 18:19:59
- Next Management:** 2015-01-28 16:30:06

History from Jan 26 2015 18:21 to Jan 27 2015 19:21

**Syslog status:** Errors have been logged (-0.2)

Go to Unit history

**Overall status:** 9.8

## 2. Upload new firmware

Choose File & Script enter the appropriate documentation, select the corresponding firmware, click button of upload file to upload new firmware.

FreeACS Web admin@182.92.234.149 Permissions | Monitor | About | Help | Logout global search

Context navigation: IP542N context search Select action:

**File configuration**

**Type:** SOFTWARE

**Name:** IP542N

**Description:** TEST

**Version:** V3.10(201501250034)

**Date:** 2015-01-27

**Target Name:** 123

**File:** 选择文件 IP542N\_16M...34\_Test.bin

Upload file

Uploaded firmware information will appear at the bottom.

Found 1 file(s)

File type: All Delete selected files

Name	Version	Type	Date	Owner	Export	Size	Delete
IP542N	V3.10(201501250034)	SOFTWARE	2015-01-27		Binary	6160480	<input type="checkbox"/>

### 3. Firmware Upgrade

Select firmware version, and then click upgrade.

The screenshot shows the FreeACS Web interface for unit IP542N. The 'Unit configuration' section is active, showing the 'Software' dropdown menu with the selected version 'V3.10(201501250034)'. The 'Unit Id' is 'user\_ip542n'. The 'Device GUI' is 'Not defined'. The 'Provisioning' section shows buttons for 'Provision', 'Read all', 'Reboot', and 'Reset'. The 'Freq/Spread' is set to 7 / 20, and the 'Interval' is 86400s +/- 17280s. The 'Last' update was on 2015-01-27 19:38:48 (53 seconds ago), and the 'Next' update is on 2015-01-29 00:12:50 (in 29 hours). The 'Parameters' section is also visible, showing a table with columns for Name, Flags, and Profile value.

### 3. Login web inspection equipment

If the upgrade is successful, you can check the firmware version number.

The screenshot shows the 'Unit dashboard' section of the FreeACS Web interface. The 'Basic information' section displays the following details:

<b>Unit Type:</b>	IP542N
<b>Profile:</b>	Default
<b>Serial Number:</b>	user_ip542n
<b>Software Version:</b>	V3.10(201501250034)
<b>Public IP address:</b>	123.114.35.79

Here you can see the firmware has been updated to the required firmware version.

## 5 TR-069 Profile

Under nodes base on TR098, TR104 and TR111.

```

{"InternetGatewayDevice", },
  {"DeviceSummary", },
  {"LANDeviceNumberOfEntries", },
  {"WANDeviceNumberOfEntries", },
  {"DeviceInfo", },
    {"Manufacturer", },
    {"ManufacturerOUI", },
    {"ModelName", },

```

```

    {"Description", },
    {"ProductClass", },
    {"SerialNumber", },
    {"HardwareVersion", },
    {"SoftwareVersion", },
    {"SpecVersion", },
    {"ProvisioningCode", },
    {"UpTime", },
    {"DeviceLog", },
{"", },

{"ManagementServer", },
    {"URL", },
    {"Username", },
    {"Password", },
    {"PeriodicInformEnable", },
    {"PeriodicInformInterval", },
    {"PeriodicInformTime", },
    {"ParameterKey", },
    {"ConnectionRequestURL", },
    {"ConnectionRequestUsername", },
    {"ConnectionRequestPassword", },
    {"UpgradesManaged", },
    {"UDPConnectionRequestAddress", },
    {"UDPConnectionRequestAddressNotificationLimit", },
    {"STUNEnable", },
    {"STUNServerAddress", },
    {"STUNServerPort", },
    {"STUNUsername", },
    {"STUNPassword", },
    {"STUNMaximumKeepAlivePeriod", },
    {"STUNMinimumKeepAlivePeriod", },
    {"NATDetected", },
{"", },

{"UPnP", },
    {"Device", },

```

```

        {"UPnPIGD", },
        {"", },
{"", },

{"IPPingDiagnostics", },
    {"DiagnosticsState", },
    {"Interface", },
    {"Host", },
    {"NumberOfRepetitions", },
    {"Timeout", },
    {"DataBlockSize", },
    {"DSCP", },
    {"SuccessCount", },
    {"FailureCount", },
    {"AverageResponseTime", },
    {"MinimumResponseTime", },
    {"MaximumResponseTime", },
{"", },

{"DownloadDiagnostics", },
    {"DiagnosticsState", },
    {"Interface", },
    {"DownloadURL", },
    {"DSCP", },
    {"EthernetPriority", },
    {"ROMTime", },
    {"BOMTime", },
    {"EOMTime", },
    {"TestBytesReceived", },
// {"TotalBytesReceived", },
    {"TCPOpenRequestTime", },
    {"TCPOpenResponseTime", },
{"", },

{"UploadDiagnostics", },

```

```

        {"DiagnosticsState", },
        {"Interface", },
        {"UploadURL", },
        {"DSCP", },
        {"EthernetPriority", },
        {"TestFileLength", },
        {"ROMTime", },
        {"BOMTime", },
        {"EOMTime", },
//      {"TotalBytesSent", },
        {"TCPOpenRequestTime", },
        {"TCPOpenResponseTime", },
        {"", },

{"Time", },
    {"NTPServer1", },
    {"NTPServer2", },
    {"", },

{"UserInterface", },
    {"User", },
        {"1", },
            {"Enable", },
            {"RemoteAccessCapable", },
            {"X_WebPort", },
            {"X_WebIdleTimeout", },
            {"X_WebAllowRemoteIP", },
            {"Username", },
            {"Password", },
            {"", },
        {"", },
    {"", },

{"Layer3Forwarding", },
    {"DefaultConnectionService", },

```

```

{"ForwardNumberOfEntries", },
{"Forwarding", },
  {"1", },
    {"Enable", },
    {"Status", },
    {"Type", },
    {"DestIPAddress", },
    {"DestSubnetMask", },
    {"SourceIPAddress", },
    {"SourceSubnetMask", },
    {"GatewayIPAddress", },
    {"Interface", },
    {"ForwardingMetric", },
  {"", },
{"", },
{"", },
{"LANConfigSecurity", },
  {"ConfigPassword", },
{"", },

{"LANDevice", },
  {"1", },
    {"LANEthernetInterfaceNumberOfEntries", },
    {"LANUSBInterfaceNumberOfEntries", },
    {"LANWLANConfigurationNumberOfEntries", },
    {"LANHostConfigManagement", },
      {"DHCPServerConfigurable", },
      {"DHCPServerEnable", },
      {"DHCPRelay", },
      {"MinAddress", },
      {"MaxAddress", },
      {"ReservedAddresses", },
      {"SubnetMask", },
      {"DNSServers", },
      {"DomainName", },
      {"IPRouters", },
      {"DHCPLeaseTime", },

```



```

{"IPInterfaceNumberOfEntries", },
{"IPInterface", },
  {"1", },
    {"Enable", },
    {"IPInterfaceIPAddress", },
    {"IPInterfaceSubnetMask", },
    {"IPInterfaceAddressingType", },
  {"", },
{"", },
{"", },
{"LANEthernetInterfaceConfig", },
  {"1", },
    {"Enable", },
    {"Status", },
    {"MACAddress", },
    {"MACAddressControlEnabled", },
    {"MaxBitRate", },
    {"DuplexMode", },
  {"", },
{"", },
{"WLANConfiguration", },
  {"1", },
    {"Enable", },
    {"Status", },
    {"BSSID", },
    {"MaxBitRate", },
    {"Channel", },
    {"AutoChannelEnable", },
    {"SSID", },
    {"BeaconType", },
    {"MACAddressControlEnabled", },
    {"Standard", },
    {"WEPKeyIndex", },
    {"KeyPassphrase", },
    {"WEPEncryptionLevel", },
    {"BasicEncryptionModes", },
    {"BasicAuthenticationMode", },
    {"WPAEncryptionModes", },

```

```

    {"WPAAuthenticationMode", },
    {"IEEE11iEncryptionModes", },
    {"IEEE11iAuthenticationMode", },
    {"PossibleChannels", },
    {"ChannelsInUse", },
    {"BasicDataTransmitRates", },
    {"OperationalDataTransmitRates", },
    {"PossibleDataTransmitRates", },
    {"RadioEnabled", },
    {"AutoRateFallBackEnabled", },
    {"TotalBytesSent", },
    {"TotalBytesReceived", },
    {"TotalPacketsSent", },
    {"TotalPacketsReceived", },
    {"TotalAssociations", },
    {"AssociatedDevice", },
        {"1", },
            {"AssociatedDeviceMACAddress", },
            {"AssociatedDeviceIPAddress", },
            {"AssociatedDeviceAuthenticationState", },
            {"X_AssociatedDeviceSignalStrength", },
        {"", },
    {"", },
    {"WEPKey", },
        {"1", },
            {"WEPKey", },
        {"", },
    {"", },

    {"", },
    {"", },

{"Hosts", },
    {"HostNumberOfEntries", },
    {"Host", },
        {"1", },
            {"IPAddress", },
            {"AddressSource", },

```

```

        {"LeaseTimeRemaining", },
        {"MACAddress", },
        {"HostName", },
        {"InterfaceType", },
        {"Active", },
        {"", },
        {"", },
        {"", },
        {"", },
        {"", },
        {"", },
        {"WANDevice", },
        {"1", },
        {"WANConnectionNumberOfEntries", },
        {"WANCommonInterfaceConfig", },
        {"EnabledForInternet", },
        {"WANAccessType", },
        {"Layer1UpstreamMaxBitRate", },
        {"Layer1DownstreamMaxBitRate", },
        {"PhysicalLinkStatus", },
        {"TotalBytesSent", },
        {"TotalBytesReceived", },
        {"TotalPacketsSent", },
        {"TotalPacketsReceived", },
        {"", },
        {"WANConnectionDevice", },
        {"1", },
        {"WANIPConnectionNumberOfEntries", },
        {"WANPPPPConnectionNumberOfEntries", },
        {"WANIPConnection", },
        {"1", },
        {"Enable", },
        {"ConnectionStatus", },
        {"PossibleConnectionTypes", },
        {"ConnectionType", },
        {"Name", },
        {"Uptime", },

```

```

{"LastConnectionError", },
{"RSIPAvailable", },
{"NATEnabled", },
{"AddressingType", },
{"ExternalIPAddress", },
{"SubnetMask", },
{"DefaultGateway", },
{"DNSEnabled", },
{"DNSOverrideAllowed", },
{"DNSServers", },
{"MACAddress", },
{"ConnectionTrigger", },
{"RouteProtocolRx", },
{"PortMappingNumberOfEntries", },
{"PortMapping", },
  {"1", },
    {"PortMappingEnabled", },
    {"PortMappingLeaseDuration", },
    {"RemoteHost", },
    {"ExternalPort", },
    {"InternalPort", },
    {"PortMappingProtocol", },
    {"InternalClient", },
    {"PortMappingDescription", },
  {"", },
{"", },
{"Stats", },
  {"EthernetBytesSent", },
  {"EthernetBytesReceived", },
  {"EthernetPacketsSent", },
  {"EthernetPacketsReceived", },
{"", },
{"", },
{"WANPPPOConnection", },
  {"1", },
    {"Enable", },
    {"ConnectionStatus", },

```

```

{"PossibleConnectionTypes", },
{"ConnectionType", },
{"Name", },
{"Uptime", },
{"LastConnectionError", },
{"RSIPAvailable", },
{"NATEnabled", },
{"Username", },
{"Password", },
{"ExternalIPAddress", },
{"DNSEnabled", },
{"DNSOverrideAllowed", },
{"DNSServers", },
{"MACAddress", },
{"TransportType", },
{"PPPoEACName", },
{"PPPoEServiceName", },
{"ConnectionTrigger", },
{"RouteProtocolRx", },
{"PortMappingNumberOfEntries", },
{"PortMapping", },
  {"1", },
    {"PortMappingEnabled", },
    {"PortMappingLeaseDuration", },
    {"RemoteHost", },
    {"ExternalPort", },
    {"InternalPort", },
    {"PortMappingProtocol", },
    {"InternalClient", },
    {"PortMappingDescription", },
  {"", },
{"", },
{"Stats", },
  {"EthernetBytesSent", },
  {"EthernetBytesReceived", },
  {"EthernetPacketsSent", },
  {"EthernetPacketsReceived", },
{"", },

```



```

        {"EventSubscription", },
        {"ResponseMap", },
{"", },
{"Codecs", },
    {"1", },
        {"EntryID", },
        {"Codec", },
        {"BitRate", },
        {"PacketizationPeriod", },
        {"SilenceSuppression", },
    {"", },
{"", },
{"", },
{"VoiceProfile", },
    {"1", },
        {"Enable", },
        {"Reset", },
        {"NumberOfLines", },
        {"Name", },
        {"SignalingProtocol", },
        {"MaxSessions", },
        {"DTMFMethod", },
        {"DTMFMethodG711", },
        {"SIP", },
            {"ProxyServer", },
            {"ProxyServerPort", },
            {"ProxyServerTransport", },
            {"RegistrarServer", },
            {"RegistrarServerPort", },
            {"RegistrarServerTransport", },
            {"UserAgentDomain", },
            {"UserAgentPort", },
            {"UserAgentTransport", },
            {"OutboundProxy", },
            {"OutboundProxyPort", },
            {"Organization", },
            {"RegistrationPeriod", },
            {"RegisterExpires", },

```

```

        {"UseCodecPriorityInSDPResponse", },
{"", },
{"RTP", },
    {"LocalPortMin", },
    {"LocalPortMax", },
    {"DSCPMark", },
    {"TelephoneEventPayloadType", },
{"", },
{"Line", },
    {"1", },
        {"Enable", },
        {"Status", },
        {"CallState", },
        {"SIP", },
            {"AuthUserName", },
            {"AuthPassword", },
            {"URI", },
        {"", },
        {"Codec", },
            {"TransmitCodec", },
            {"ReceiveCodec", },
            {"TransmitBitRate", },
            {"ReceiveBitRate", },
            {"TransmitSilenceSuppression", },
            {"ReceiveSilenceSuppression", },
            {"TransmitPacketizationPeriod", },
            {"List", },
                {"1", },
                    {"EntryID", },
                    {"Codec", },
                    {"BitRate", },
                    {"PacketizationPeriod", },
                    {"SilenceSuppression", },
                    {"Enable", },
                    {"Priority", },
                {"", },
            {"", },
        {"", },

```





## Diagnosis

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

**Table 82** Diagnosis

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage	Administration
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR069	cnMaestro	Diagnosis	
Operating Mode									

[Help](#)

---

**Packet Trace**

Packet Trace

Tracking Interface:

Packet Trace:

---

**Ping Test**

Ping Test

Dest IP/Host Name:

WAN Interface:

---

**Traceroute Test**

Traceroute Test

Dest IP/Host Name:

WAN Interface:

## Description

### 1. Packet Trace

Users can use the packet trace feature to intercept packets which traverse the device. Click the Start button to start home gateway tracking and keep refreshing the page until the message trace shows to stop, click the Save button to save captured packets.

### 2. Ping Test

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

**Ping Test**

**Ping Test**

Dest IP/Host Name

WAN Interface

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

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

▲ ▼

### 3. Traceroute Test

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

**Traceroute Test**

**Traceroute Test**

Dest IP/Host Name

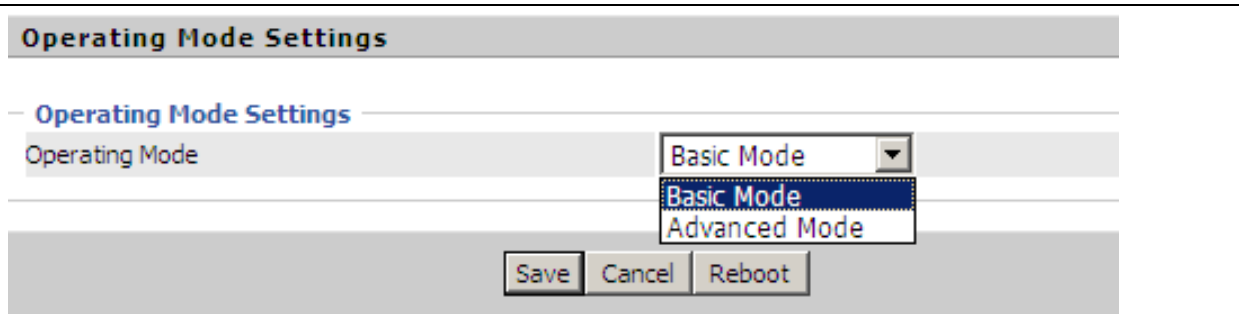
WAN Interface

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

▲ ▼

# Operating Mode

**Table 83** Operating mode



## Description

Choose the Operation Mode as Basic Mode or Advanced Mode.

## System Log

**Table 84** System log

### Description

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

## Logout

**Table 85** Logout

### 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: IPv6 address configuration on WAN interface

---

The R200/201 devices support IPv6 addressing starting from firmware version 4.3.

This chapter covers:

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

## Introduction

DHCPv6 protocol is used to automatically provision/configure IPv6 capable end points in a local network. In addition to acquiring an IPv6 IP address for the WAN interface and its associated LAN/WLAN clients, the R200/201 devices are also capable of prefix delegation.

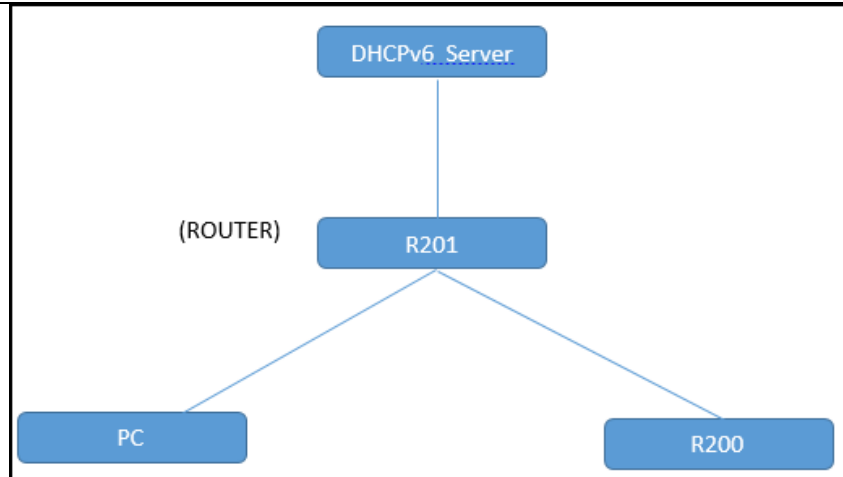
The R200/R201 devices support the following types of modes of IPv6 addresses:

- Stateless DHCPv6
- Statefull DHCPv6

Table 86 **IPv6 Modes**

Mode	Description
Stateless	In Stateless DHCPv6 mode, the R200/R201 devices listen for ICMPv6 Router Advertisements messages which are periodically sent out by the routers on the local link or requested by the node using a Router Advertisements solicitation message. The device derives a unique IPv6 address using prefix receives from the router and its own MAC address.

---

**Statefull**

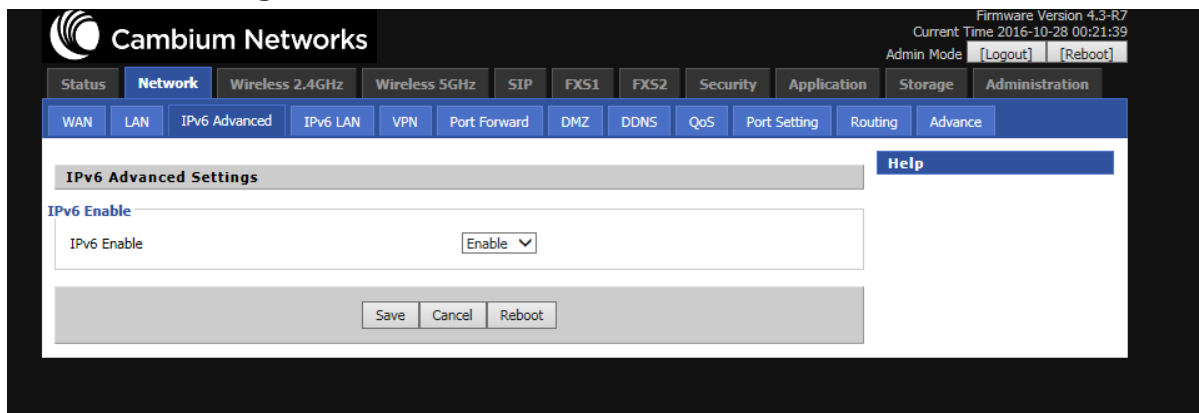
In Statefull DHCPv6 mode, the client works exactly as IPv4 DHCP, in which hosts receive both their IPv6 addresses and additional parameters from the DHCP server.

## Enabling IPv6

To enable IPv6 functionality:

1. Navigate to **Network > IPv6 Advanced** page.
2. Select **Enable** from the **IPv6 Enable** drop-down list.
3. Click **Save**.

Table 87 **Enabling IPv6**

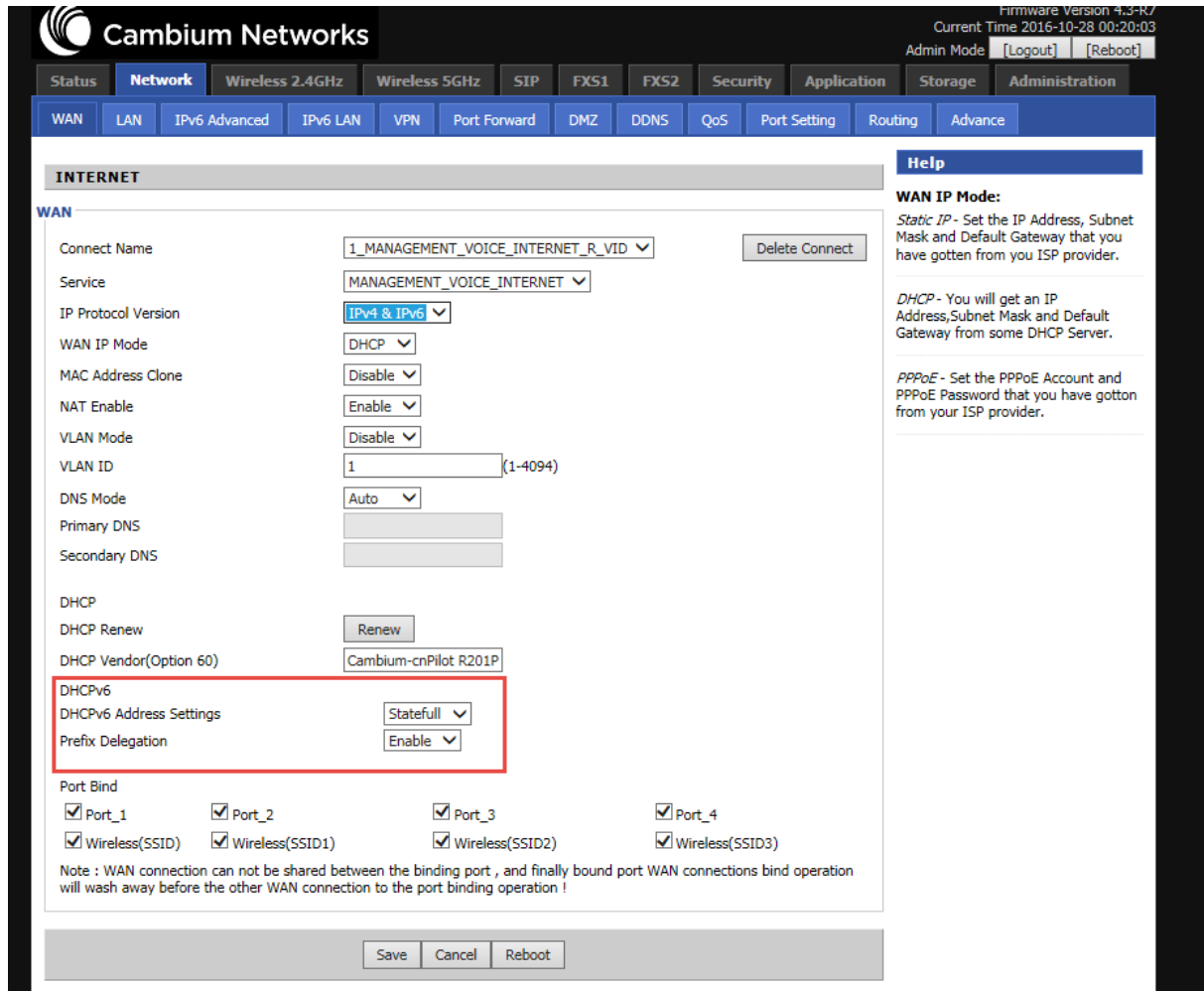


## Configuring IPv6

### Configuring Statefull IPv6

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

Table 88 Configuring Statefull IPv6

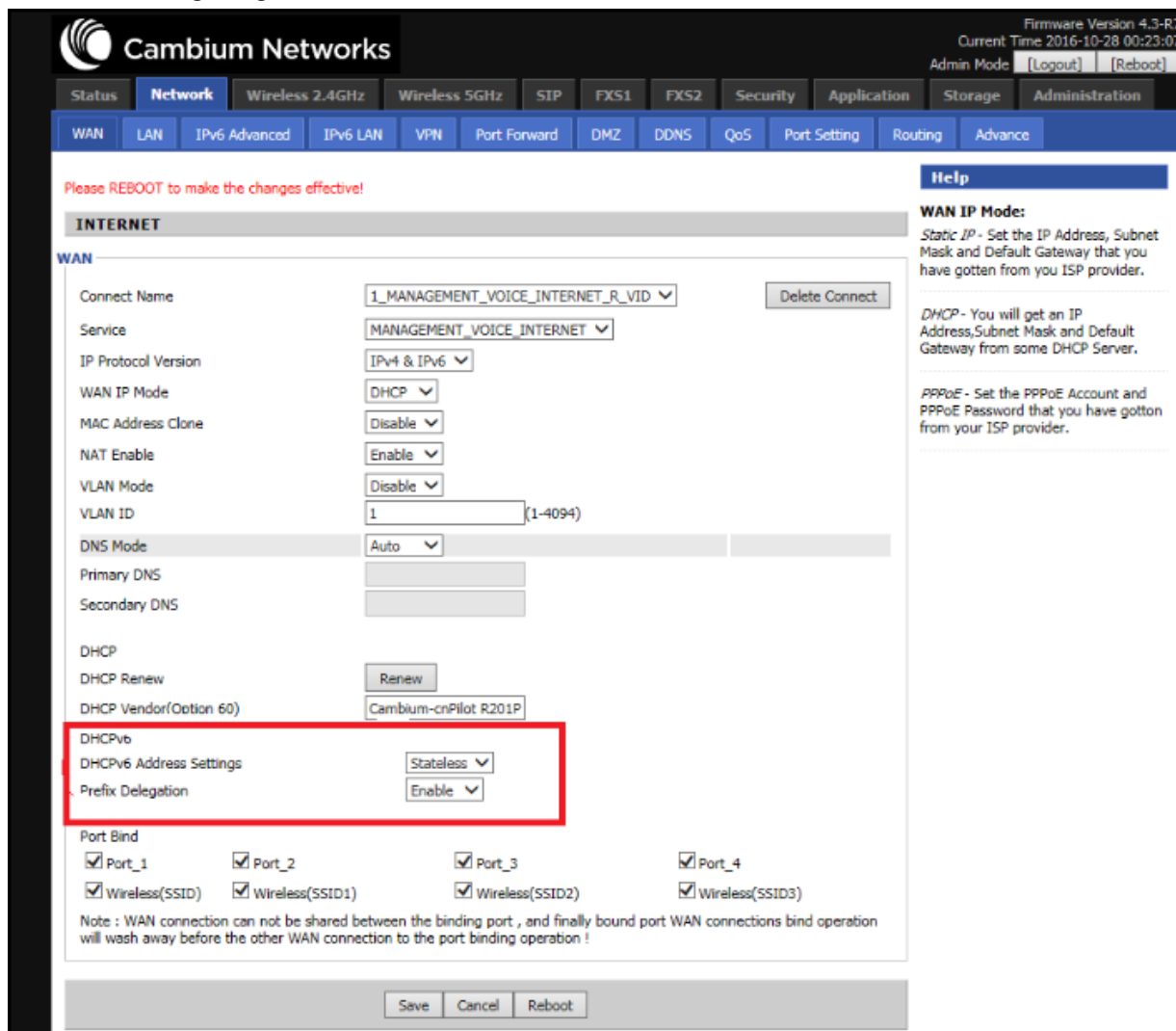


Field Name	Description
IP Protocol Version	Enable IPv4 and IPv6 option.
WAN IP Mode	Set it to DHCP.
NAT Enable	Select Enable.
DHCPv6 Address Settings	Set it to statefull mode.
Prefix Delegation	Select Enable.



## Configuring Stateless IPv6

Table 89 Configuring Stateless IPv6



Field Name	Description
IP Protocol Version	Enable IPv4 and IPv6 option.
WAN IP Mode	Set it to DHCP.
NAT Enable	Select Enable.
DHCPv6 Address Settings	Set it to stateless mode.
Prefix Delegation	Select Enable.

## Viewing WAN port status

To view the status of WAN port:

1. Navigate to **Status** page.

The screenshot displays the network configuration status. It is divided into two main sections: FXS Port Status and Network 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	<input type="button" value="Renew"/>
Link-Local IPv6 Address	fe80::204:56ff:fe04:b001/64
IPv6 Address	<b>fec0::102/64</b>
Subnet Mask	255.255.255.0
Default Gateway	
Primary DNS	
Secondary DNS	
IPv6 PD Prefix	2001:db8:5eeb::/48
IPv6 Domain Name	domain.example
IPv6 Primary DNS	fec0::105
IPv6 Secondary DNS	fec0::106
WAN Port Status	1000Mbps Full

**TR069\_VOICE\_INTERNET Vlan Status**

Connection Type	
MAC Address	00:04:56:04:B0:01
IP Address	

## IPv6 DHCP configuration for LAN/WLAN clients

Wired and wireless clients connected to R200/201 can obtain their IPv6 addresses based on how the LAN side DHCPv6 parameters are configured. The R200/201 can be either configured as a DHCPv6 server in which the LAN/WLAN clients get IPv6 addresses from the configured pool.

If DHCP server is disabled on the R200/201, the clients will get IPv6 addresses from the external DHCPv6 server configured in the network.

## LAN DHCPv6

When IPv6 is enabled, the LAN/WLAN clients of R200/R201 can be configured to receive IPv6 addresses from locally configured IPv6 pool or from an external DHCPv6 server.

To enable LAN DHCPv6 service:

The screenshot displays the Cambium Networks web interface for configuring IPv6 LAN settings. The interface includes a navigation menu at the top with options like Status, Network, Wireless 2.4GHz, Wireless 5GHz, SIP, FXS1, FXS2, Security, Application, Storage, and Administration. The 'Network' section is expanded to show sub-menus for WAN, LAN, IPv6 Advanced, IPv6 LAN, VPN, Port Forward, DMZ, DDNS, QoS, Port Setting, Routing, and Advance. The 'IPv6 LAN Setting' page is active, showing a list of configuration parameters:

- IPv6 Address:
- IPv6 Prefix Length:  (0-128)
- DHCPv6 Server:
- DHCPv6 Status:  (dropdown)
- DHCPv6 Mode:  (dropdown)
- Domain Name:
- Server Preference:  (0-255)
- Primary DNS Server:
- Secondary DNS Server:
- Lease Time:  (0-86400sec)
- IPv6 Address Pool:  -  /
- Router Advertisement:  (dropdown)
- Advertise Interval:  (10-1800sec)
- RA Managed Flag:  (dropdown)
- RA Other Flag:  (dropdown)
- Prefix:  /
- Prefix Lifetime:  (0-3600sec)

At the bottom of the configuration area, there are three buttons: Save, Cancel, and Reboot.

---

## Chapter 5: Managing device via cnMaestro

---

cnMaestro is a suite of cloud-based tools for network management: inventory management, onboarding devices, daily operations and maintenance. cnMaestro offers full visibility across the entirety of a network.

This chapter covers:

- [Preparing the device](#)
- [Login to cnMaestro](#)
- [On Boarding of cnPilot R200/R201](#)
- [Configuring the Devices](#)
- [Approving On Boarded devices](#)
- [Unclaiming the Devices](#)

## Preparing the device

---

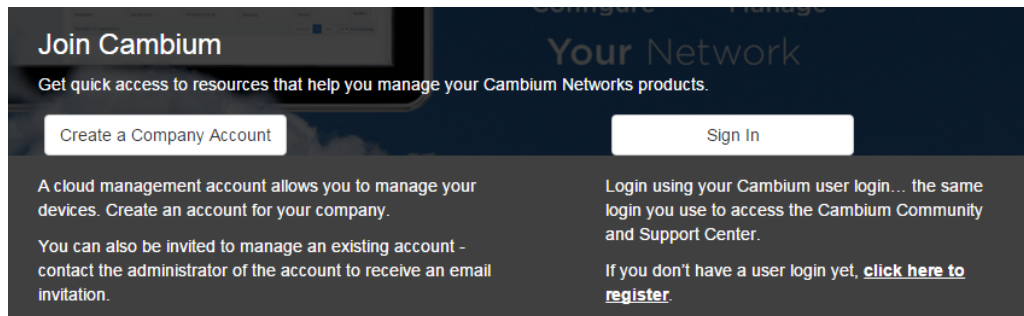
The prerequisites at device side are:

- 1 Power on the cnPilot.Home R200/201. Configure the IP Address using either the DHCP or Static mode.
- 2 Check for the Internet connectivity. This is required, as the device needs to communicate with the cnMaestro Server hosted in the AWS.
- 3 Allow the IP Addresses of the devices in the Firewall Server using an ACL. Also, enable the protocols like HTTP/HTTPS and SSL.  
This is required as the device communicates with the cnMaestro Server using web sockets and for security reasons SSL certificates are exchanged between the device and the cnMaestro Server. The cnMaestro uses [s3.amazonaws.com](https://s3.amazonaws.com) link to download software images for device firmware upgrade
- 4 By default, the cnMaestro Server URL will be configured in the devices for communication with cnMaestro. The default URL is <https://cloud.cambiumnetworks.com>

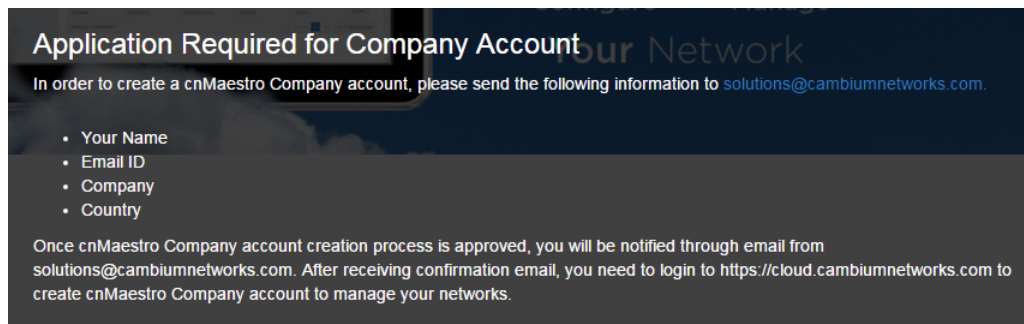
# Login to cnMaestro

Follow the below steps:

- 1 Open a browser session and launch the URL  
<https://cloud.cambiumnetworks.com>
- 2 Sign in using your Cambium support center account credentials if you already have an Account or click the link "Click Here to Register" for the registration



- 3 After sign in, create the company Account (it requires Approval from the Solutions@cambiumnetworks.com to create an account)



- 4 Once account is approved and created, user can login to the cnMaestro Server.

- 5 If the user has single company account, he will be automatically redirected to that account after log in.
- 6 If the user has multiple accounts, once signed in the user needs to select the company account he wants to access.



✓ Select Account

- KREDDUM
- KREDDUM\_ONSNOQA
- KREDDUM\_QACLOUD
- KRISHNA
- TOS\_TEST

🚪 Logout

# On Boarding of cnPilot R200/R201

---

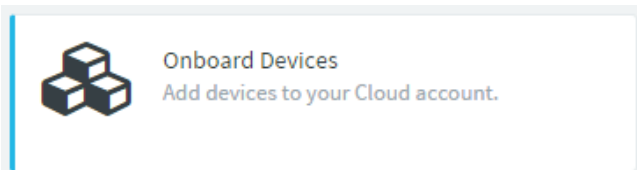
The device can be On Boarded using

- Serial Number or
- Cambium ID.

## On Boarding using Serial Number

The devices can be On Boarded on cnMaestro using device's Serial Number. The procedure is supported for the cnPilot R200/R201 Devices.

- 1 Click the Onboard Devices widget in home page



- 2 Provide the Serial number of the device in the combo box and click "Claim Devices" button.

Cambium ID'. At the bottom of the form, there is a 'Clear' button on the left and a 'Claim Devices' button on the right."/>

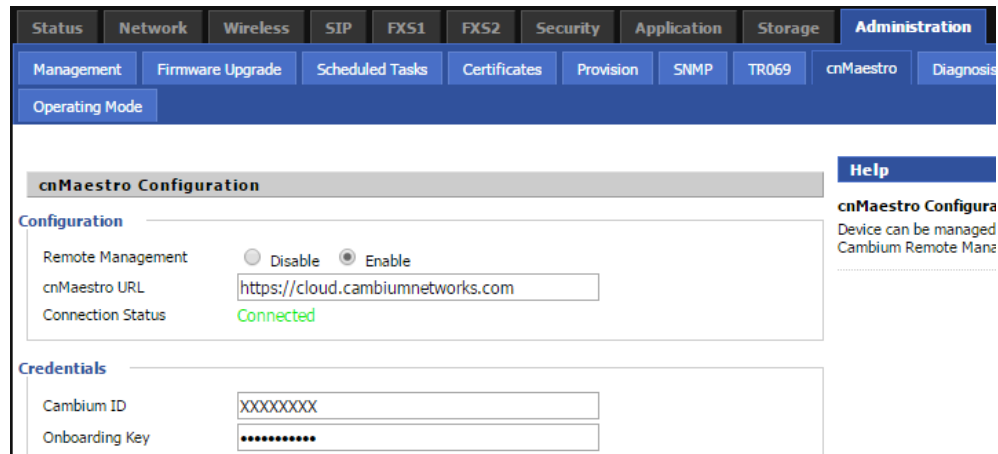
- 3 Serial Number can be found on the device enclosure and can be seen in the Device GUI Home page after logging into the device.
- 4 Claim the single or multiple serial numbers separated by comma or new line.  
To claim bulk number of devices, user can connect to bar code machine scanner to laptop where cnMaestro GUI is running and scan the serial numbers of the devices.
- 6 Go to "On board" tab after claiming the devices to proceed with Approval procedure [Approving On Boarded devices](#).



## Onboarding using Cambium ID

The Cambium ID based On Boarding can be done either from cnPilot R200/R201 GUI or CLI (not from cnMaestro).

- 1 Login to cnPilot R200/R201 GUI and navigate to Administration > cnMaestro page



The screenshot displays the 'Administration' section of the cnPilot R200/R201 GUI. The 'cnMaestro Configuration' page is shown, featuring a navigation bar with tabs for Status, Network, Wireless, SIP, FXS1, FXS2, Security, Application, Storage, and Administration. The Administration tab is active, showing sub-tabs for Management, Firmware Upgrade, Scheduled Tasks, Certificates, Provision, SNMP, TR069, cnMaestro, and Diagnosis. The 'cnMaestro Configuration' section is expanded, showing the following details:

- Configuration:**
  - Remote Management:  Disable  Enable
  - cnMaestro URL:
  - Connection Status: Connected
- Credentials:**
  - Cambium ID:
  - Onboarding Key:

A 'Help' button is visible on the right side of the page, with a tooltip that reads: 'cnMaestro Configura Device can be managed Cambium Remote Man'.

- 2 Enter the Cambium ID and On Boarding key and click Save.  
Reboot of the device is required in case of cnPilot R200/R201 devices.
- 3 The Cambium ID and On Boarding key details are given during company account creation in the cnMaestro Server. These details can also be found at the Home Page > On Board Devices > Claim From Device page in cnMaestro server.
- 4 Go to the Home Page->On Board Devices-> Onboard page in cnMaestro server to proceed with Device Approval process.

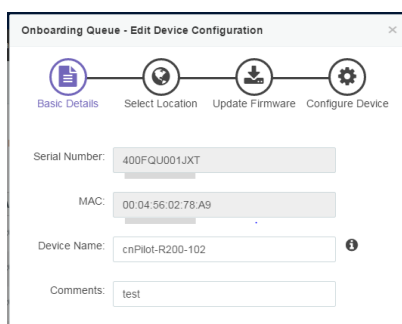
# Configuring the Devices

---

## Basic Details

User can update device name and comments for a device. In case, user does not enter device name, it will be read from the device after On Boarding. The device basic details can be configured later from the Configure > Devices page.

**Figure 5** Basic details



Onboarding Queue - Edit Device Configuration

Basic Details Select Location Update Firmware Configure Device

Serial Number: 400FQU001JXT

MAC: 00:04:56:02:78:A9

Device Name: cnPilot-R200-102

Comments: test

## Set Device Location

The Location configuration page allows to configure device location in google map. The device location can be configured:

- Select the Network and Tower under which the device will be placed
- Set Latitude and Longitude coordinates to populate device location

In case the device location is not set, it will be placed under default cnMaestro network. User can set device location after on boarding of device from Configure > Device page. Navigate to the Mange > Organize menu for creating new Network and Tower.

**Figure 6** Select Location

Basic Details   **Select Location**   Update Firmware   Configure Device

Configure Device Location

Network:  [Create Network / Tower](#)

Latitude:  Min = -90, Max = 90 ⓘ

Longitude:  Min = -180, Max = 180 ⓘ

Search Address

Cancel   Save

## Firmware Update

The Firmware Update page allows the user to upgrade the software to the latest available image before the device is onboarded to cnMaestro. It also shows the current version if the device is claimed via Cambium ID. User can upgrade later through Operate > Software Update page.

**Figure 7** Firmware update

Basic Details   Select Location   **Update Firmware**   Configure Device

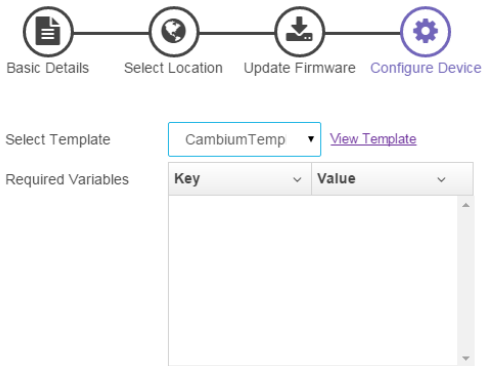
Active [Version](#)

Image Version  [Release Notes](#)

## Configure Devices

The Configure Devices page allows to select a pre-configured template file in order to push the configuration to the device before On Boarding. User can push the device template configuration later from Configure > Devices page. The Configuration Templates can be created from Configure > Templates page.

**Figure 8** Configure devices



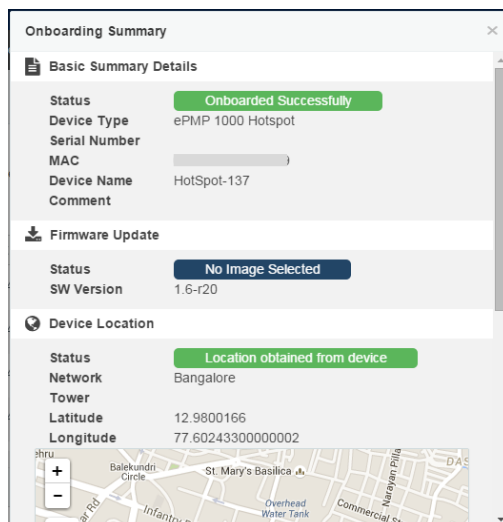
# Approving On Boarded devices

The approval procedure for On Boarded devices are:

- 1 Device goes through the following states based on the device trying to connect to the CnMaestro Server :

State	Approval state	Details
Waiting for Device	Before approval	Device is not communicating to cnMaestro Server
Queued	After approval	Device is not communicating to cnMaestro Server
Waiting for Approval	Before approval	Device is communicating to cnMaestro Server
Queued	After approval	Other devices are getting updated with the config and software Images
Updating	After approval	Current device is getting updated with the config and software Images
On Boarded	After approval	Device is successfully on boarded.

- 2 Once the device is in on boarding queue user can delete the device before approving it.
- 3 The "Approve All" option can be used if there are bulk number of devices. Configure the Basic and other settings later from the Configure->Devices page or Bulk Upgrade of the devices from the Operate->Software Update page.
- 4 User can monitor on boarded devices from Home > Monitor the device page or by selecting the options from the Monitor menu.
- 5 The device summary hyperlink in the configuration column of On Board page provides summary of device configuration. It also provides hyperlinks to configure and upgrade the device later.




# Unclaiming the Devices

The device unclaiming procedure is as follows:

**Figure 9** Unclaiming the devices

## Unclaim Devices



Device Type: All ▾

Type ▾	Serial No ▾	Device ▾	MAC ▾	IP Add... ▾	Stat... ▾	Durat... ▾	Unclai... ▾
ePMP 1...		HotSpot-137	██████████6	10.110.70.137	● On-board	0d 23h 39m	✘
cnPilot ...	4██████████9B	cnPilot-R201-107	██████████3	10.110.70.107	● On-board	1d 4h 47m	✘
cnPilot ...	4██████████N	cnPilot-R201-109	██████████3	10.110.70.109	● On-board	1d 4h 47m	✘

- 1 If the user wants to delete the devices from his account he need to go to the Operate >On Board Devices> Unclaim page and click the Delete icon (✘).
- 2 Statistics collected from the time period when the device on boarded to the time it is being deleted are not deleted from the server. In case if the user on boards the device again the data will be preserved for Historical reference.
- 3 Uncalming will also help in transferring the device to the other cnMaestro Account. It is highly recommended that the user should unclaim the device from his account before he can transfer or claim the device in another account.

---

## Chapter 6: Troubleshooting Guide

---

This chapter covers:

- [Configuring PC to get IP Address automatically](#)
- [Cannot connect to the Web GUI](#)
- [Forgotten Password](#)
- [Fast Bridge Setting](#)
- [cnMaestro On Boarding troubleshooting](#)

## Configuring PC to get IP Address automatically

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

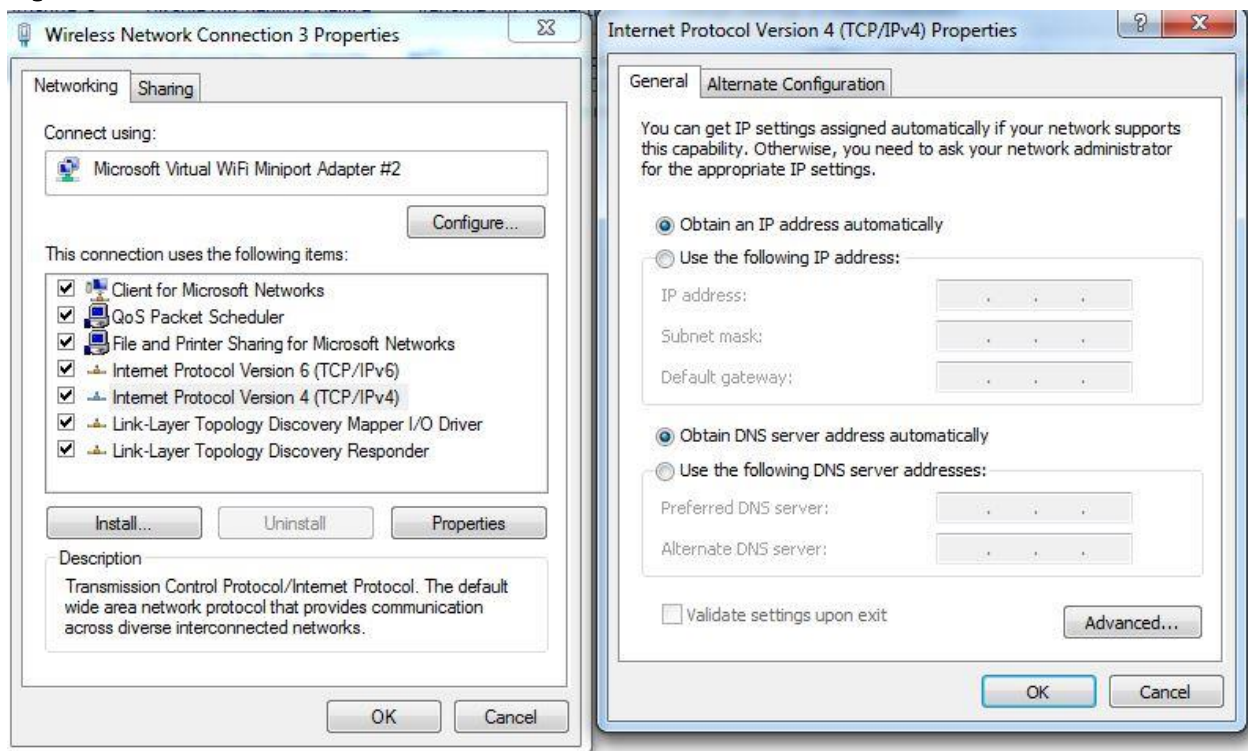
**Step 1 :** Click the “Start” button

**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 10](#).

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

**Figure 10** LAN



## 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.

---

<b>TR069_VOICE_INTERNET Vlan Status</b>	
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	

<b>Other Vlan Status</b>	
Connection Type	Bridge
MAC Address	
IP Address	
Subnet Mask	
Default Gateway	
Primary DNS	
Secondary DNS	

<b>VPN Status</b>	
VPN Type	Disable
Initial Service IP	
Virtual IP Address	

<b>PC Port Status</b>	
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.

---

## cnMaestro On Boarding troubleshooting

The On Boarding troubleshooting procedure is described below:

- 1 If during the Cambium ID on boarding if the device dashboard or home page shows the cnMaestro Connection status as

Error Status	Cause	Resolution
Failed to Resolve URL	The cloud URL is not being resolved by the device.	<ul style="list-style-type: none"> <li>• Ensure that the cnMaestro cloud URL is <a href="https://cloud.cambiumnetworks.com">https://cloud.cambiumnetworks.com</a></li> <li>• If the URL is correct, check the DNS settings and Internet connectivity.</li> <li>• If the internet connectivity and DNS works fine then check the firewall configuration for device IP Address and the protocols http/https/SSL are allowed as part of ACL</li> </ul>
Invalid Cambium ID/Password	Wrong configuration of cambium ID or On Boarding key	<ul style="list-style-type: none"> <li>• Ensure that the correct credentials is entered.</li> </ul>
Invalid Cookie or Cambium ID not configured	Device is unclaimed	<ul style="list-style-type: none"> <li>• Claim the device either by serial number or Cambium ID</li> </ul>
Device Not Claimed	Device is not claimed	<ul style="list-style-type: none"> <li>• Claim the device either by serial number or Cambium ID</li> </ul>
Connecting	Device is trying to connect to the cnMaestro server	<ul style="list-style-type: none"> <li>• Device is connecting state</li> </ul>

- 2 During the serial number on boarding following are the error messages:

Error Status	Cause	Resolution
Unknown Device	Device serial number is not known to cnMaestro server	<ul style="list-style-type: none"> <li>• Send a mail to <a href="mailto:solutions@cambiumnetworks.com">solutions@cambiumnetworks.com</a> for the serial numbers to be added to the server database</li> </ul>
Invalid Serial Number	Device serial number is less than 12 characters and given for claiming	<ul style="list-style-type: none"> <li>• Enter the correct serial number of the device or try on boarding using Cambium ID</li> </ul>
Already Managed by this account	Device is already managed by the current user account	<ul style="list-style-type: none"> <li>• Do not try both the serial number and cambium ID on boarding methods at the same time.</li> </ul>
Already Managed by other Account	Device is already claimed in another user account	<ul style="list-style-type: none"> <li>• Ensure that the entered serial number of device belongs to current user account.</li> </ul>

After the error messages occurs, user can click the OK button in the error dialog and then rectify the serial numbers by giving correct ones and initiate the claiming procedure.

Else, use can clear the wrong serial numbers if it need not to be claimed. This allows not to re-enter serial number again and remove the invalid characters from entered serial number.

- 3 cnMaestro Account ID is the Cambium ID or Account Name chosen while creating the company account which indicates that the device belongs to that account. cnMaestro Account ID will be blank when the device is not claimed and will be populated when the device is claimed in the cnMaestro server. The Account ID will be available in the device dashboard or home page.

## 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. Save the configuration and reboot the device.
12. cnPilot Home R200P/R201P model has PoE out functionality on WAN port which can power a single PMP450 or ePMP 1000 SM (Subscriber Module).
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.

---

# Glossary

---

Term	Definition
ATA	Advanced Technology Attachment
Address Resolution Protocol	Protocol defined in RFC 826 to allow a network element to correlate a host IP address to the Ethernet address of the host. See <a href="http://www.faqs.org/rfcs/rfc826.html">http://www.faqs.org/rfcs/rfc826.html</a> .
Bridge	Network element that uses the physical address (not the logical address) of another to pass data. The bridge passes the data to either the destination address, if found in the simple routing table, or to all network segments other than the one that transmitted the data. Modules are Layer 2 bridges except that, where NAT is enabled for an SM, the SM is a Layer 3 switch. Compare to Switch and Router, and see also NAT.
DES	Data Encryption Standard. An over-the-air link option that uses secret 56-bit keys and 8 parity bits. DES performs a series of bit permutations, substitutions, and recombination operations on blocks of data.
DHCP	Dynamic Host Configuration Protocol, defined in RFC 2131. Protocol that enables a device to be assigned a new IP address and TCP/IP parameters, including a default gateway, whenever the device reboots. Thus DHCP reduces configuration time, conserves IP addresses, and allows modules to be moved to a different network within the system. See <a href="http://www.faqs.org/rfcs/rfc2131.html">http://www.faqs.org/rfcs/rfc2131.html</a> . See also Static IP Address Assignment.
DNS	Domain Name System, a system for naming computers and network services that is organized into a hierarchy of domains
File Transfer Protocol	Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. Defined in RFC 959. See <a href="http://www.faqs.org/rfcs/rfc959.html">http://www.faqs.org/rfcs/rfc959.html</a> .
FTP	File Transfer Protocol, defined in RFC 959. Utility that transfers of files through TCP (Transport Control Protocol) between computing devices that do not operate on the same platform. See <a href="http://www.faqs.org/rfcs/rfc959.html">http://www.faqs.org/rfcs/rfc959.html</a> .
FXS	Foreign Exchange Station means the wall jack or the interface to the telephone system which FXO devices can be connected to
Gateway	A network point that acts as an entrance to another network
GUI	Graphical user interface.

Term	Definition
HTTP	Hypertext Transfer Protocol, used to make the Internet resources available on the World Wide Web. Defined in RFC 2068. See <a href="http://www.faqs.org/rfcs/rfc2068.html">http://www.faqs.org/rfcs/rfc2068.html</a> .
HTTPS	Hypertext Transfer Protocol Secure (HTTPS)
ICMP	Internet Control Message Protocols defined in RFC 792, used to identify Internet Protocol (IP)-level problems and to allow IP links to be tested. See <a href="http://www.faqs.org/rfcs/rfc792.html">http://www.faqs.org/rfcs/rfc792.html</a> .
IGMP	The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IPv4/IPv6 networks to establish multicast group memberships.
IP	Internet Protocol defined in RFC 791. The Network Layer in the TCP/IP protocol stack. This protocol is applied to addressing, routing, and delivering, and re-assembling data packets into the Data Link layer of the protocol stack. See <a href="http://www.faqs.org/rfcs/rfc791.html">http://www.faqs.org/rfcs/rfc791.html</a> .
IP Address	32-bit binary number that identifies a network element by both network and host. See also Subnet Mask.
IPv4	Traditional version of Internet Protocol, which defines 32-bit fields for data transmission.
ISM	Industrial, Scientific, and Medical Equipment radio frequency band, in the 900-MHz, 2.4-GHz, and 5.8-GHz ranges.
L2TP over IPsec	Level 2 Tunneling Protocol over IP Security. One of several virtual private network (VPN) implementation schemes. Regardless of whether Subscriber Modules have the Network Address Translation feature (NAT) enabled, they support VPNs that are based on this protocol.
LED	Light-Emitting Diode
MAC Address	Media Access Control address. The hardware address that the factory assigns to the module for identification in the Data Link layer interface of the Open Systems Interconnection system. This address serves as an electronic serial number.
NAT	Network Address Translation defined in RFC 1631. A scheme that isolates Subscriber Modules from the Internet. See <a href="http://www.faqs.org/rfcs/rfc1631.html">http://www.faqs.org/rfcs/rfc1631.html</a> .
NEC	National Electrical Code. The set of national wiring standards that are enforced in the U.S.A.

Term	Definition
NetBIOS	Protocol defined in RFC 1001 and RFC 1002 to support an applications programming interface in TCP/IP. This interface allows a computer to transmit and receive data with another host computer on the network. <a href="http://www.faqs.org/rfcs/rfc1001.html">RFC 1001 defines the concepts and methods.</a> RFC 1002 defines the detailed specifications. See <a href="http://www.faqs.org/rfcs/rfc1001.html">http://www.faqs.org/rfcs/rfc1001.html</a> and <a href="http://www.faqs.org/rfcs/rfc1002.html">http://www.faqs.org/rfcs/rfc1002.html</a> .
Network Address Translation	Scheme that defines the Access Point Module as a proxy server to isolate registered Subscriber Modules from the Internet. Defined in RFC 1631. See <a href="http://www.faqs.org/rfcs/rfc1631.html">http://www.faqs.org/rfcs/rfc1631.html</a> .
Network Management Station	See NMS.
NMS	Network Management Station. A monitor device that uses Simple Network Management Protocol (SNMP) to control, gather, and report information about predefined network variables (objects). See also Simple Network Management Protocol.
NTP	Network Time Protocol (NTP) is a protocol that is used to synchronize computer clock times in a network of computers
PPPoE	Point to Point Protocol over Ethernet. Supported on SMs for operators who use PPPoE in other parts of their network operators who want to deploy PPPoE to realize per-subscriber authentication, metrics, and usage control.
QoS	Quality of Service (QoS) refers to the capability of a network to provide better service to selected network traffic over various technologies
RJ-45	Standard cable that is typically used for Ethernet connection. This cable may be wired as straight-through or as crossover. Later modules auto-sense whether the cable is straight-through or crossover.
Router	Network element that uses the logical (IP) address of another to pass data to only the intended recipient. Compare to Switch and Bridge.
SIP	Session Initiation Protocol
Simple Network Management Protocol	Standard that is used for communications between a program (agent) in the network and a network management station (monitor). Defined in RFC 1157. See <a href="http://www.faqs.org/rfcs/rfc1157.html">http://www.faqs.org/rfcs/rfc1157.html</a> .
SNMP	See Simple Network Management Protocol, defined in RFC 1157.
SNMPv3	SNMP version 3



Term	Definition
Static IP Address Assignment	Assignment of Internet Protocol address that can be changed only manually. Thus static IP address assignment requires more configuration time and consumes more of the available IP addresses than DHCP address assignment does. RFC 2050 provides guidelines for the static allocation of IP addresses. See <a href="http://www.faqs.org/rfcs/rfc2050.html">http://www.faqs.org/rfcs/rfc2050.html</a> . See also DHCP.
SSID	Service Set Identifier
Subnet Mask	32-bit binary number that filters an IP address to reveal what part identifies the network and what part identifies the host. The number of subnet mask bits that are set to 1 indicates how many leading bits of the IP address identify the network. The number of subnet mask bits that are set 0 indicate how many trailing bits of the IP address identify the host.
Switch	Network element that uses the port that is associated with the physical address of another to pass data to only the intended recipient. Compare to Bridge and Router.
TCP	Alternatively known as Transmission Control Protocol or Transport Control Protocol. The Transport Layer in the TCP/IP protocol stack. This protocol is applied to assure that data packets arrive at the target network element and to control the flow of data through the Internet. Defined in RFC 793. See <a href="http://www.faqs.org/rfcs/rfc793.html">http://www.faqs.org/rfcs/rfc793.html</a> .
TFTP	Trivial File Transfer Protocol, is a simple high-level protocol for transferring data servers
TKIP	Temporal Key Integrity Protocol
TR 069	TR-069 (Technical Report 069) is a technical specification that defines an application layer protocol for remote management of end-user devices
VLAN	Virtual local area network. An association of devices through software that contains broadcast traffic, as routers would, but in the switch-level protocol.
UPnP	Universal Plug and Play
USB	Universal Serial Bus
WDS	Wireless Distribution System
WLAN	Wireless Local Area Network
WMM	Wi-Fi Multimedia

## Glossary

Term	Definition
WPA2-PSK	Wi-Fi Protected Access 2 - Pre-Shared Key, and also called WPA or WPA2 Personal, it is a method of securing your network using WPA2 with the use of the optional Pre-Shared Key (PSK) authentication, which was designed for home users without an enterprise authentication server.
WPS	Wi-Fi Protected Setup