



User Guide
cnPilot R195W Model

System Release 4.4.2



Accuracy

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

Copyrights

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

Restrictions

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

License Agreements

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

High Risk Materials

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").

This product is not restricted in the EU. 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.

Contents

About This User Guide	3
Contacting Cambium Networks	4
Purpose	5
Cross references	5
Feedback	5
Declaration of Conformity	6
Part 15 FCC Rules	6
Class B Digital Device or Peripheral	6
GNU GPL Information	7
Conventions, warnings, cautions, and notes	9
Conventions	9
Warnings	9
Cautions	9
Notes	9
Chapter 1: Product Description	10
Hardware Installation	11
Chapter 2: Basic Settings	12
Web Management Interface	12
Accessing and Configuring cnPilot Home Router via cnMaestro	16
Configuring via Voice Commands	17
Chapter 3: Advanced Configuration	24
Two-Level Management	25
Setting the Time Zone	26
Status	27
Configuring an Internet Connection	32
Network	34
WAN	34
IPv6 Address configuration	46
LAN	51
Wireless	63
WDS	76
SIP	77
FXS1	85
FXS2	95
Security	96
Application	99
Storage	101

Administration.....	104
Management.....	104
Firmware Upgrade	111
Provision	111
SNMP.....	114
TR-069.....	115
Scheduled Tasks.....	129
Diagnosis	130
Operating Mode	133
System Log	133
Logout	134
Reboot	134
Chapter 4: Troubleshooting Guide.....	135
Configuring PC to get IP Address automatically	135
Cannot connect to the Web GUI	135
Forgotten Password.....	135
cnMaestro On-boarding troubleshooting	135
Appendix: Third Party Software.....	138
Appendix: Part Numbers.....	139
Glossary	140

About This User Guide

Thank you for choosing Cambium cnPilot Home & Small Business Wi-Fi Router with ATA (optional) and PoE(optional).

This manual provides basic information about how to install and deploy the cnPilot Home Routers.

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

The cnPilot Home Router is a managed device (that yet can act as a stand-alone router if desired). In addition to Wi-Fi, this product provides high quality voice calls (VoIP models only) 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 can interoperate with many other SIP devices and softwares.



This guide contains the following chapters:

- [Chapter 1: Product description](#)
- [Chapter 2: Basic Settings](#)
- [Chapter 3: Advanced Configuration](#)
- [Chapter 4: Troubleshooting Guide](#)

Contacting Cambium Networks

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

Purpose

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.

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 an 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.
-

**Note**

RF Exposure Statement.

- The distance between user and products should be no less than 20cm.
 - Operations in the 5.15-5.25GHz band are restricted to indoor usage only.
-

GNU GPL Information

cnPilot Home Router 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.

IC Warning

This device complies with Industry Canada licence-exempt RSS standard(s). Operation is subject to the following two conditions:

- (1) this device may not cause interference, and
- (2) this device must accept any interference, including interference that may cause undesired operation of the device.

Le présent appareil est conforme aux CNR d'Industrie Canada applicables aux appareils radio exempts de licence. L'exploitation est autorisée aux deux conditions suivantes:

- (1) il ne doit pas produire de brouillage et
- (2) l'utilisateur du dispositif doit être prêt à accepter tout brouillage radioélectrique reçu, même si ce brouillage est susceptible de compromettre le fonctionnement du dispositif.

- This Class B digital apparatus complies with Canadian ICES-003.
- Cet appareil numérique de la classe B est conforme à la norme NMB-003 du Canada.



Note

- The distance between user and products should be no less than 20cm
 - Operations in the 5.15-5.25GHz band are restricted to indoor usage only
-

CE Note

Manufacturer: Cambium Networks Inc.

Address: Unit B2 Linhay Business Park Eastern Rd Ashburton, Devon TQ13 7UP United Kingdom

Hereby, Cambium Networks Inc. declares that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU.

Importers: XXXXXXXX

Address: XXXXXXXX

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

Hardware Version: R195W_V1_2

Software Version: V3.20(201901291603)

The wireless operation frequency

WIFI: 2412MHz-2472MHz, Max EIRP Power 18.95dBm

WIFI: 5180-5240MHz, Max EIRP Power 21.85dBm

WIFI: 5180-5240MHz, Max EIRP Power 21.85dBm

WIFI: 5745-5825MHz, Max EIRP Power 13.36dBm

Safety warning and Attentions

If use adapter, adapter must be comply 2014/30/EU Directive

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

Do not store or use your product in temperatures higher than 45°C

RF Exposure Statement

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



Conventions, warnings, cautions, and notes

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

Conventions

The following convention is used throughout this User Guide:
cnPilot Home Router: (cnPilot R195W model)

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:

- [Hardware Installation](#)

Hardware Installation

Before configuring your router, please see the procedure below for instructions on connecting the cnPilot Home Router 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 (If available).
5. 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 Router device. Using other power adapters may damage the cnPilot Home Router 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.
-

Chapter 2: Basic Settings

This chapter covers:

- [Web Management Interface](#)
- [Accessing and Configuring cnPilot Home Router via cnMaestro](#)
- [Configuring via Voice Commands](#)

Web Management Interface

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



Note

By default, http access is disabled. Only https is allowed.

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 4: Troubleshooting Guide](#).

EZ UI

cnPilot Home Routers provides an additional simplified management interface for home users. The home users can connect to any of the LAN port of the device and access the **EZ UI** by entering <https://mywifi.net> in the browser.

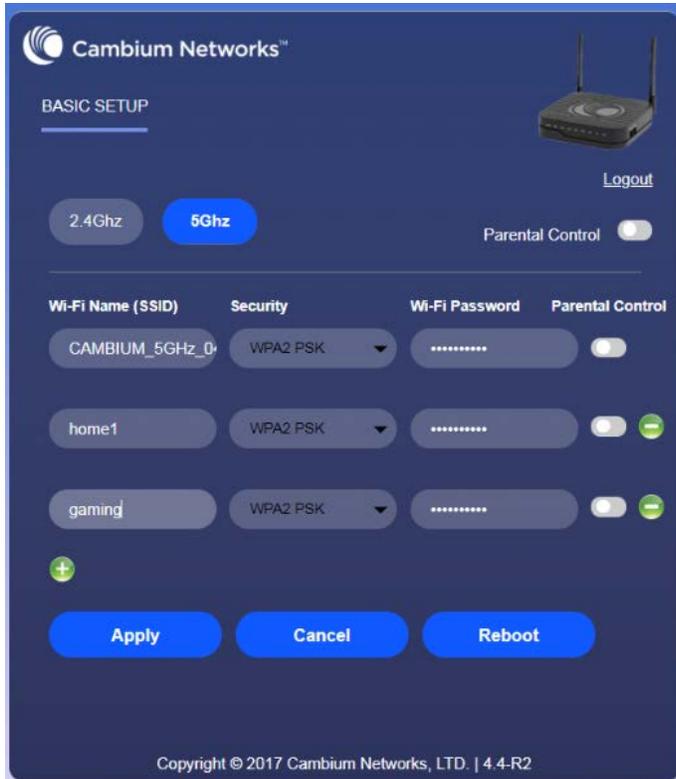
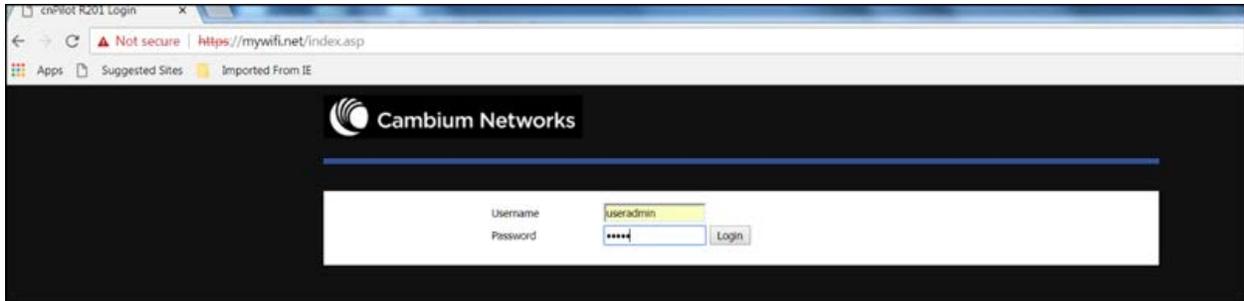
Home users needs to provide the default **Basic User** credentials as **useradmin/admin**.



Note

Please check with your ISP in case the Basic User credentials have been changed for improved security.

Figure 3 EZ UI



The ISP allows the home user to access the EZ UI through a wireless client connected to the cnPilot Home Router. Using the EZ UI, the user can easily change the basic device configurations such as Wi-Fi names, Wi-Fi passwords and parental control.

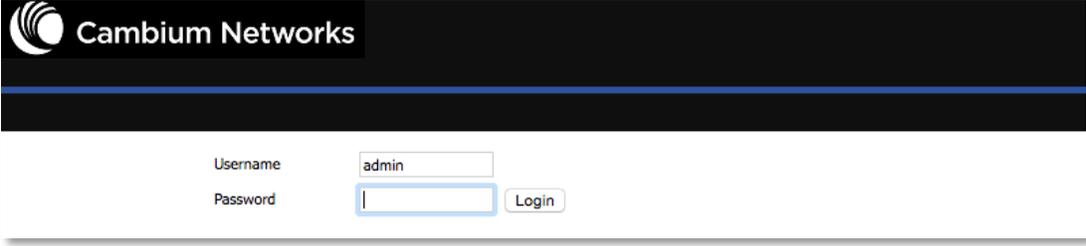


Note

Management access from a wireless client is disabled by default.

Refer [Enabling Mangement access for wireless client](#) on "how to enable management access for wireless clients".

Open a web browser on your PC and type <https://192.168.11.1/>. The following window appears that prompts for Username and Password.

Figure 1 Login Prompt – LAN Port

Username

Password

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

**Note**

If you are unable to access the web configuration, please see [Chapter 4: 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

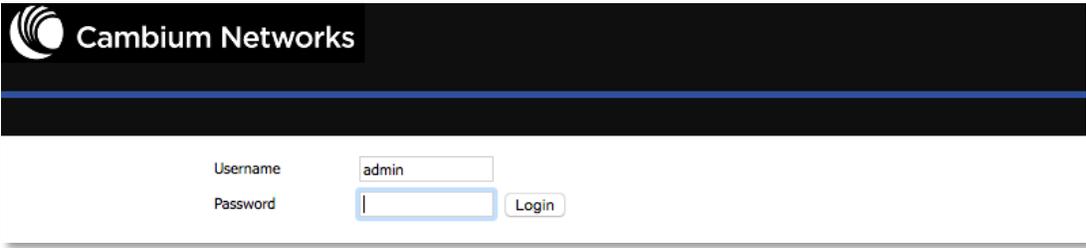
**Note**

By default, the web access from WAN interface is disabled from 4.3.3 release onwards for security reasons.

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 **Status** page.

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

Figure 2 Login Prompt – WAN Port

Username

Password

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

**Note**

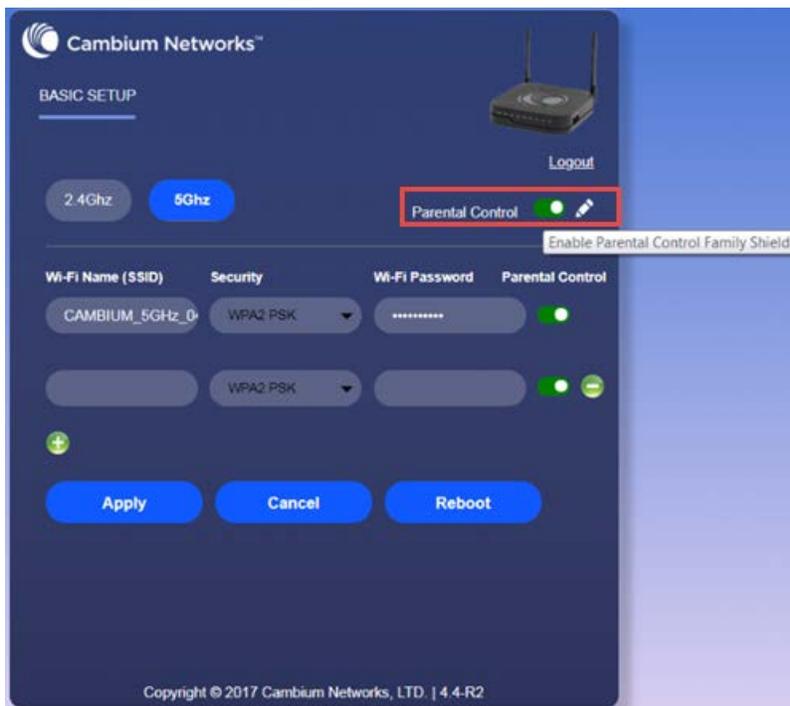
If you fail to access to the web configuration, see [Chapter 4: Troubleshooting Guide](#) for more information.

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

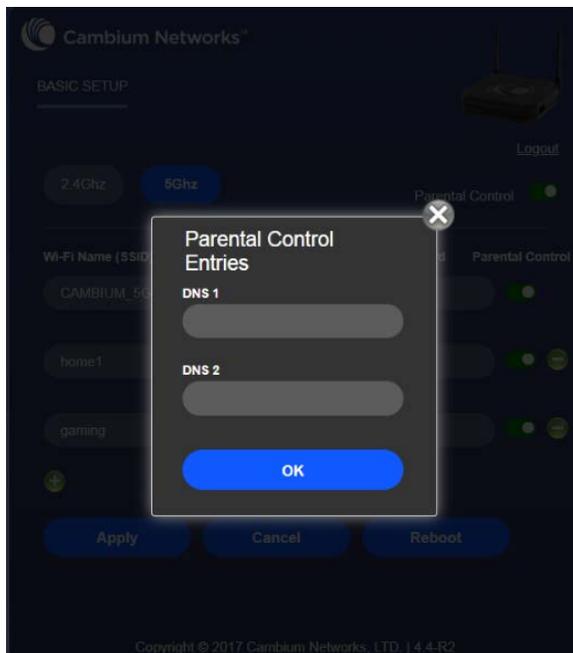
Parental Control

cnPilot Home Routers provide parental control feature for home users. Parental control allows home users to restrict access to unlawful/adult content over their WiFi network. This feature is based on external DNS filtering (like OpenDNS).

Parental Control feature is only available while using EZ UI. To enable parental control feature, tap on the **Parental Control** button.



To configure cnPilot Home Router with the DNS server IP(s) provided by the Parental control service provider:



Parental control feature can be applied only to a specific WiFiName/SSID while the other SSIDs can be free from any such restrictions. Once the device is setup for Parental control service, any DNS request from its clients will be forwarded to the external DNS servers configured for filtering/restricting the content.

When Parental control is enabled, it is applied to all the LAN clients and it cannot be disabled for specific LAN ports.

Accessing and Configuring cnPilot Home Router via cnMaestro

cnMaestro, Cambium's next generation network management system is the recommended method for managing Cambium's cnPilot Home Routers. 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 Home Routers.

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.

Preparing the device:

The prerequisites at device side are:

- 1 Power on the cnPilot Home Router. 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

- 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>

For details on Onboarding cnPilot Wi-Fi routers and the related details, please refer the cnMaestro User Guide posted in the [cnMaestro User Guide](#).

Performing Speed Test

The cnPilot Home Routers support speed test service and it can be triggered from cnMaestro On-Premises server.



Note

The port that is used for Wi-Fi performance in cnMaestro On-Premises is 18301 (UDP and TCP).

The cnMaestro On-Premises supports the speed test feature from 1.5.1 release onwards. For more information, refer to the section on Wi-Fi performance in [On-Premises User Guide](#).

Configuring via Voice Commands

cnPilot Home Routers 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 1 Voice Menu Setting Options

Operation code	Menu Navigation
----------------	-----------------

<p>1 Network configuration</p>		<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “1”. 3. Prompt “Please enter password”, user needs to input password and press “#” key, if user wants to configure Network. 4. The different options are described below. The unit reports “Operation Successful” if the changes are successful. The cnPilot Home Router returns to the prompt “please enter your option ...” 5. To quit, enter “*”
<p>1 Network configuration</p>	<p>1. WAN Port Connection Type</p>	<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “1”, and cnPilot Home Router reports the current WAN port connection type 3. Prompt “Please enter password”, user needs to input password and press “#” key, if user wants to configuration WAN port connection type. The password in IVR is same as web management interface login, the user may use phone keypad to enter password directly 4. 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. 5. Prompt “Please enter password”, user needs to input password and press “#” key if user wants to configuration WAN port connection type. 6. 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 Router returns to the prompt “please enter your option ...” 7. To quit, enter “*”

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

	5. DNS	<ol style="list-style-type: none"> 1. Pick up phone and press "*****" to start IVR 2. Choose "5", and cnPilot Home Router reports current DNS 3. Input the new DNS and press # key: 4. Use "*" to replace ".", user can input 192*168*20*1 to set the new gateway 192.168.20.1. 5. Press "#" key to indicate that you have finished. Report "operation successful" if user operation is ok. 6. If you want to quit, press "**".
2 Phone Port Configuration		<ol style="list-style-type: none"> 1. Pick up phone and press "*****" to start IVR 2. Choose "2", and cnPilot Home Router reports the current Phone port connection type 3. Prompt "Please enter password", user needs to input password and press "#" key, if user wants to configuration Phone port connection type. 4. Prompt "Please enter password", user needs to input password and press "#" key if user wants to configuration WAN port connection type. 5. To quit, enter "**"
3 Factory Reset		<ol style="list-style-type: none"> 1. Pick up phone and press "*****" to start IVR 2. Choose "3", and cnPilot Home Router reports "Factory Reset" 3. Prompt "Please enter password", the method of inputting password is the same as operation 1. 4. If you want to quit, press "**". Prompt "operation successful" if password is right and then cnPilot Home Router will be in factory default configuration. 5. Press "7" reboot to make changes effective.
4 Reboot		<ol style="list-style-type: none"> 1. Pick up phone and press "*****" to start IVR 2. Choose "4", and cnPilot Home Router reports "Reboot" 3. Prompt "Please enter password", the method of inputting password is same as operation 1. 4. cnPilot Home Router reboots if password is right and operation is ok.

5 WAN Port Login	<ol style="list-style-type: none">1. Pick up phone and press "****" to start IVR2. Choose "5", and cnPilot Home Router reports "WAN Port Login"3. Prompt "Please enter password", the method of inputting password is same as operation 1.4. If user wants to quit, press "*".5. Report "operation successful" if user operation is ok.
6 WEB Access Port	<ol style="list-style-type: none">1. Pick up phone and press "****" to start IVR2. Choose "6", and cnPilot Home Router reports " WEB Access Port"3. Prompt "Please enter password", the method of inputting password is same as operation 1. Report "operation successful" if user operation is ok.4. Report the current WEB Access Port5. Set the new WEB access port and press "#" key.6. Report "operation successful" if user operation is successful.
7 Firmware Version	<ol style="list-style-type: none">1. Pick up phone and press "****" to start IVR2. Choose "7" and cnPilot Home Router reports the current Firmware version

**Note**

1. While using Voice menu, press * (star) to return to main menu.
2. If any changes made in the IP assignment mode, the router must be rebooted 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 Router is connected.
5. The default LAN port IP address of cnPilot Home Routers is 192.168.11.1 and this address should not be assigned to the WAN port IP address of cnPilot Home Router 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'

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, enter the extension or phone number 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 want 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 want 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: Advanced Configuration

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

This chapter covers:

- [Two-Level Management](#)
- [Setting the Time Zone](#)
- [Status](#)
- [Configuring an Internet Connection](#)
- [Network](#)
- [Wireless](#)
- [SIP](#)
- [FXS1](#)
- [FXS2](#)
- [Security](#)
- [Application](#)
- [Administration](#)
- [System Log](#)
- [Logout](#)
- [Reboot](#)

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 Router 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.

**Note**

It is highly recommended to change the admin/user passwords to non-default values.

Setting the Time Zone

Table 2 Setting time zone

Time/Date Setting

NTP Settings

NTP Enable Enable

Current Time 1970 - 01 - 01 . 08 : 01 :
13

Sync with host

NTP Settings (GMT+08:00) China Coast, Hong Kong

Primary NTP Server

Secondary NTP Server

NTP synchronization(1 - 1440m)

Daylight Saving Time

Daylight Saving Time Disable

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

Status

Table 3 Status > Basic Page

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

Product Information

Product Information

Product Name	cnPilot R200P
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

SIP Account Status

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**FXS Port Status**

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

Network Status**Active WAN Interface**

Connection Type	DHCP
IP Address	192.168.210.230 Renew
Link-Local IPv6 Address	
Subnet Mask	255.255.255.0
Default Gateway	192.168.210.254
Primary DNS	8.8.8.8
Secondary DNS	8.8.4.4
IPv6 PD Prefix	
IPv6 Domain Name	
IPv6 Primary DNS	
IPv6 Secondary DNS	
WAN Port Status	1000Mbps 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

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

Refresh Clear Save

Manufacturer:CAMBIUM NETWORKS

ProductClass:cnPilot R200P

SerialNumber:

BuildTime:201711212052

IP:192.168.11.1

HWVer:V1.3

SWVer:4.3.4-R5

```
<Tue Nov 21 07:04:20 2017> DEV_MANAGER[13914]: Not able to find [ device_id ] in keystore
<Tue Nov 21 07:04:20 2017> DEV_MANAGER[13914]: Required on-boarding credentials not configured, cann...
<Tue Nov 21 07:04:20 2017> DEV_MANAGER[13914]: Unable to discover cnMaestro URL (re-discover in 68 s...
<Tue Nov 21 07:04:20 2017> DEV_MANAGER[13914]: Attempting (re)connection in 68 seconds
<Tue Nov 21 07:05:29 2017> DEV_MANAGER[13914]: Not able to find [ device_id ] in keystore
<Tue Nov 21 07:05:29 2017> DEV_MANAGER[13914]: Required on-boarding credentials not configured, cann...
<Tue Nov 21 07:05:29 2017> DEV_MANAGER[13914]: Unable to discover cnMaestro URL (re-discover in 73 s...
<Tue Nov 21 07:05:29 2017> DEV_MANAGER[13914]: Attempting (re)connection in 73 seconds
<Tue Nov 21 07:06:43 2017> DEV_MANAGER[13914]: Not able to find [ device_id ] in keystore
<Tue Nov 21 07:06:43 2017> DEV_MANAGER[13914]: Required on-boarding credentials not configured, cann...
<Tue Nov 21 07:06:43 2017> DEV_MANAGER[13914]: Unable to discover cnMaestro URL (re-discover in 65 s...
<Tue Nov 21 07:06:43 2017> DEV_MANAGER[13914]: Attempting (re)connection in 65 seconds
<Tue Nov 21 07:07:49 2017> DEV_MANAGER[13914]: Not able to find [ device_id ] in keystore
<Tue Nov 21 07:07:49 2017> DEV_MANAGER[13914]: Required on-boarding credentials not configured, cann...
<Tue Nov 21 07:07:49 2017> DEV_MANAGER[13914]: Unable to discover cnMaestro URL (re-discover in 76 s...
<Tue Nov 21 07:07:49 2017> DEV_MANAGER[13914]: Attempting (re)connection in 76 seconds
<Tue Nov 21 07:09:06 2017> DEV_MANAGER[13914]: Not able to find [ device_id ] in keystore
<Tue Nov 21 07:09:06 2017> DEV_MANAGER[13914]: Required on-boarding credentials not configured, cann...
<Tue Nov 21 07:09:06 2017> DEV_MANAGER[13914]: Unable to discover cnMaestro URL (re-discover in 303 ...
<Tue Nov 21 07:09:06 2017> DEV_MANAGER[13914]: Attempting (re)connection in 5 minutes
<Tue Nov 21 07:14:10 2017> DEV_MANAGER[13914]: Not able to find [ device_id ] in keystore
<Tue Nov 21 07:14:10 2017> DEV_MANAGER[13914]: Required on-boarding credentials not configured, cann...
<Tue Nov 21 07:14:10 2017> DEV_MANAGER[13914]: Unable to discover cnMaestro URL (re-discover in 341 ...
<Tue Nov 21 07:14:10 2017> DEV_MANAGER[13914]: Attempting (re)connection in 5 minutes
```

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**.

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 4](#) below.

Table 4 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		Help	
WAN			
Connect Name	1_TR069_VOICE_INTERNET_R_VID_	Delete Connect	
Service	TR069_VOICE_INTERNET		
IP Protocol Version	IPv4		
WAN IP Mode	Static	WAN IP Mode: <i>Static IP</i> - Set the IP Address, Subnet Mask and Default Gateway that you have gotten from you ISP provider.	
NAT Enable	Enable	<i>DHCP</i> - You will get an IP Address, Subnet Mask and Default Gateway from some DHCP Server.	
VLAN Mode	Disable	<i>PPPoE</i> - Set the PPPoE Account and PPPoE Password that you have gotten from your ISP provider.	
VLAN ID	1 (1-4094)		
Static			
IP Address	192.34.30.69		
Subnet Mask	255.255.255.248		
Default Gateway	192.34.30.65		
DNS Mode	Manual		
Primary DNS Address	66.185.0.68		
Secondary DNS Address			
Port Bind			
<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
Connect Name	Use keywords to indicate WAN port service model
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, Static or Bridge
NAT Enable	Enable or disable NAT

VLAN ID	 Note 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"> 1. When DNS mode is Auto, the device under LAN port will automatically obtains the preferred DNS and alternate DNS. 2. When DNS mode is Manual, the user should manually configure the preferred DNS and alternate DNS
----------	---

Primary DNS	Enter the preferred DNS address
Secondary DNS	Enter the secondary DNS address

DHCP	(displayed when WAN IP Mode is set to DHCP)
-------------	--

DHCP Renew	Refresh the DHCP IP
DHCP Vendor (Option60)	Specify the DHCP Vendor field Display the vendor and product name

Network

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.



Note

1. By default, Management access over WAN is disabled for security concerns and can be enabled if required. For more details, please refer [Enabling Management access for wireless clients](#)
2. By default, SNMP access over WAN interface is disabled for security concerns and can be enabled if required. For more details, please refer [Enabling SNMP access over WAN](#)

WAN Settings

Table 5 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 (Set Top Box).
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)

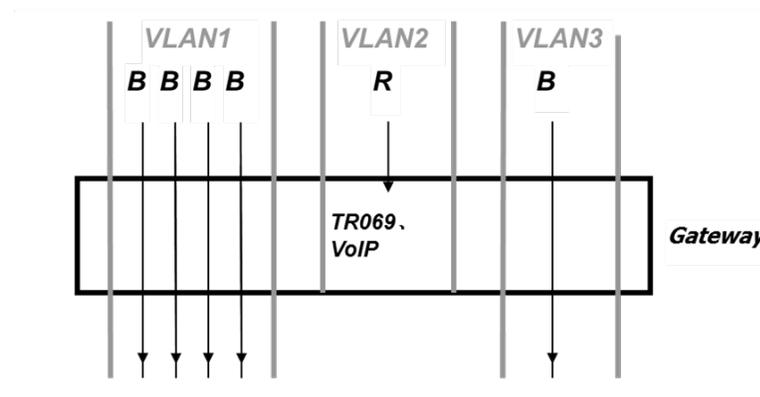
2_INTERNET_B_VID (Second Interface, Service is INTERNET, Bridge Mode, VLAN is disabled)

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.

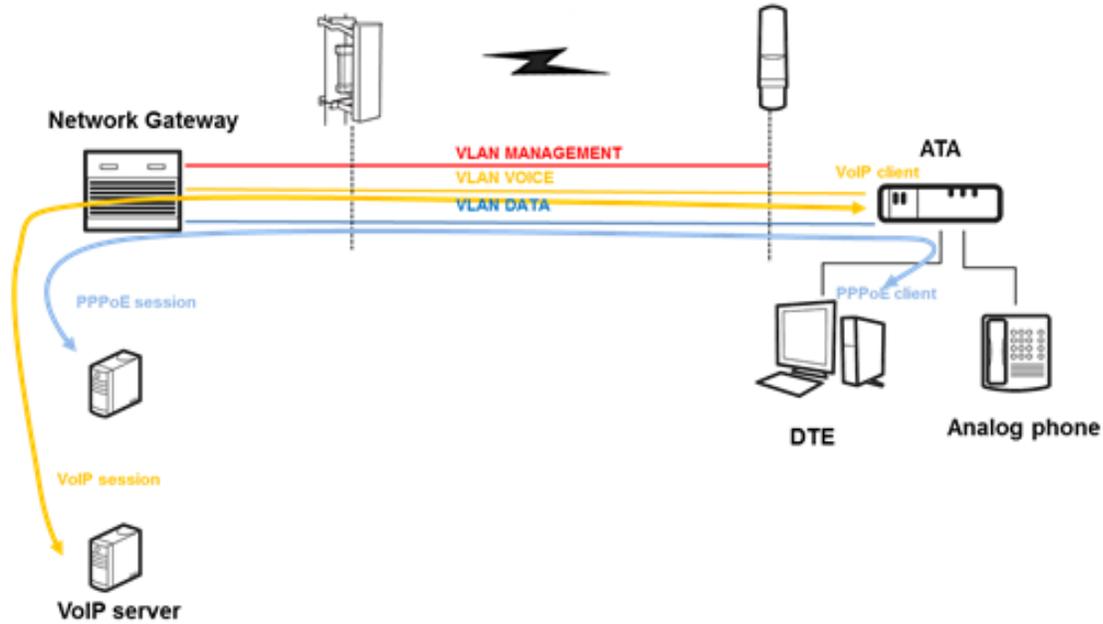
Figure 3 Multi VLAN



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



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 6 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 Auto and Manual .

Primary DNS Address	The primary DNS of Internet port
Secondary DNS Address	The secondary DNS of Internet port

DHCP

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

Table 7 DHCP

INTERNET

WAN

Connect Name: Delete Connect

Service:

IP Protocol Version:

WAN IP Mode:

MAC Address Clone:

NAT Enable:

Overwrite NAT IP:

VLAN Mode:

VLAN ID: (1-4094)

DNS Mode:

Primary DNS:

Secondary DNS:

DHCP

DHCP Renew:

DHCP Vendor(Option 60):

Port Bind

Port_1 Port_2 Port_3 Port_4

Wireless(SSID) Wireless(SSID1) Wireless(SSID2) Wireless(SSID3)

Note: A port can be mapped to only a single WAN profile. If a port is selected in multiple WAN profiles then, only the most recent selection is retained.

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
DNS Mode	Select DNS mode, options are Auto and Manual.
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 8 PPPoE

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

Field Name	Description
PPPoE Account	Enter a valid user name provided by the ISP
PPPoE Password	Enter a valid password provided by the ISP.
Confirm Password	Enter your PPPoE password again
Service Name	Enter a service name for PPPoE authentication.

If it is left empty, the service name is auto detected.

Operation Mode Select the mode of operation, options are **Keep Alive**, **On Demand** and **Manual**:

- When the mode is **Keep Alive**, the user sets the 'keep alive redial period' values range from 0 to 3600s, the default setting is 5 minutes;
- When the mode is **On Demand**, the user sets the 'on demand idle time' value in the range of 0-60 minutes, the default setting is 5 minutes;

Operation Mode

On Demand ▾

On Demand Idle Time(0-60m)

5

- When the mode is **Manual**, there are no additional settings to configure

Keep Alive Redial Period Set the interval to send Keep Alive messaging

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.

Following is an 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 9 Bridge Mode

INTERNET

WAN

Connect Name: 1_MANAGEMENT_VOICE_INTERNET_R_VID Delete Connect

Service: MANAGEMENT_VOICE_INTERNET

IP Protocol Version: IPv4

WAN IP Mode: Bridge

Bridge Type: IP Bridge

DHCP Service Type: Pass Through

VLAN Mode: Disable

VLAN ID: 1 (1-4094)

Port Bind

Port_1 Port_2 Port_3 Port_4

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

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

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

	DHCP packet from the WAN interface to the LAN interface. Local DHCP service will not allocate IP to clients of LAN port.
Local Service	Gateway will not forward DHCP packets between LAN and WAN, it also blocks DHCP packets from the WAN port. Clients connected to the LAN port can get IP from DHCP server run in gateway.
VLAN Mode	
Disable	The WAN interface is untagged. LAN is untagged.
Enable	The WAN interface is tagged. LAN is untagged.
Trunk	Only valid in bridge mode. All ports, including WAN and LAN, belong to this VLAN Id and all ports are tagged with this VLAN id. Tagged packets can pass through WAN and LAN.
VLAN ID	Set the VLAN ID.
	<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p>Note</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.

Q-in-Q

Q-in-Q tunneling allow service providers to create a Layer 2 Ethernet connection between two customer sites. Providers can segregate different customers' VLAN traffic on a link (for example, if the customers use overlapping VLAN IDs) or bundle different customer VLANs into a single service VLAN. Data centers can use Q-in-Q tunneling to isolate customer traffic within a single site or to enable customer traffic flows between cloud data centers in different geographic locations. Q-in-Q tunneling adds a service VLAN tag (802.1Q based) before the customer's 802.1Q VLAN tags.

In Q-in-Q tunneling, as a packet travels from a customer VLAN (C-VLAN) to a service provider's or data center VLAN (S-VLAN), another 802.1Q tag for the appropriate S-VLAN is added before the C-VLAN tag. The C-VLAN tag remains and is transmitted through the network. As the packet leaves the S-VLAN in the downstream direction, the S-VLAN 802.1Q tag is removed.

Figure 5 Q-in-Q Frame Format

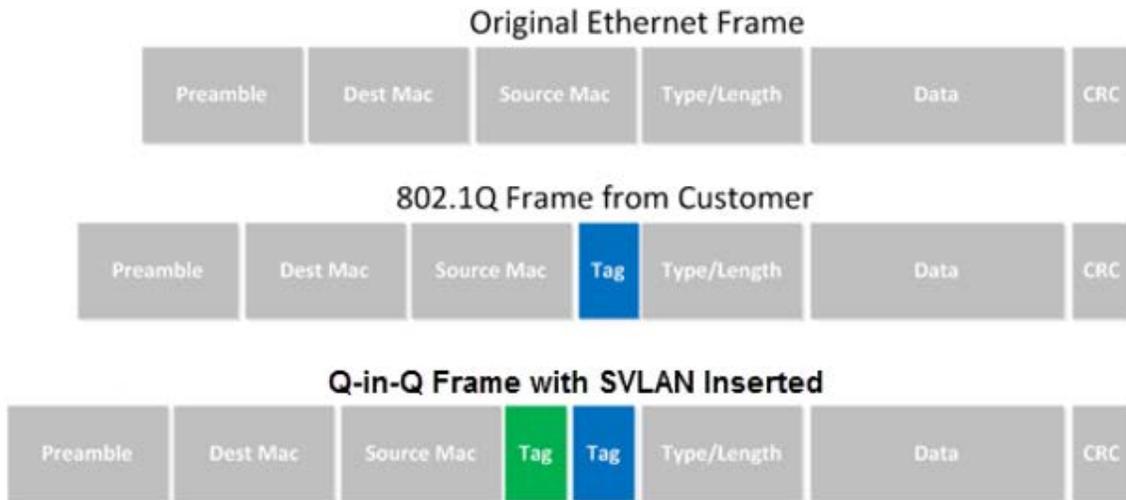


Table 10 Q-in-Q

The screenshot shows the Cambium Networks web interface for WAN configuration. The 'SVLAN (Q-in-Q)' section is highlighted with a red box. The configuration includes:

- Connect Name: 1_MANAGEMENT_VOICE_INTERNET_R_VID
- Service: MANAGEMENT_VOICE_INTERNET
- IP Protocol Version: IPv4
- WAN IP Mode: DHCP
- MAC Address Clone: Disable
- NAT Enable: Enable
- Overwrite NAT IP: (empty field)
- VLAN Mode: Enable
- VLAN ID: 10 (1-4094)
- 802.1p: 0
- SVLAN (Q-in-Q): Enable**
- SVLAN ID: 20 (1-4094)**
- DNS Mode: Auto
- Primary DNS: (empty field)
- Secondary DNS: (empty field)
- DHCP Renew: Renew
- DHCP Vendor(Option 60): Cambium-cnPilot R201
- Port Bind: Port_1, Port_2, Port_3, Port_4 (all checked)
- Wireless(SSID): Wireless(SSID), Wireless(SSID1), Wireless(SSID2), Wireless(SSID3) (all checked)

Field Name	Description
------------	-------------

VLAN Mode	Enable VLAN Mode.
SVLAN(Q-in-Q)	Enable Q-in-Q feature.
SVLAN ID	Enter a value for SVLAN ID (1-4094).

**Note**

Please ensure that Hardware NAT Enable option is disabled in the LAN page for R201/R201P/R201W models. The Hardware NAT Enable option is available only for R201 models. Please refer the image shown below:

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

PC Port(LAN)

PC Port(LAN)

Local IP Address:

Local Subnet Mask:

Local DHCP Server:

DHCP Start Address:

DHCP End Address:

DNS Mode:

Primary DNS:

Secondary DNS:

Client Lease Time(0-86400s):

DHCP Static Allotment

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

DNS Proxy:

Hardware NAT Enable:

Help

PC Port(LAN):
NAT - The product will be same as router.

Bridge - The LAN port is same as WAN port.

Local DHCP Server - It will assign IP Addressed set here to devices connect to the LAN port.

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 11 MAC clone

Status	Network	Wireless 2.4GHz	Wireless 5GHz	SIP	FXS1	FXS2	Security	Application	Storage	Administration	
WAN	LAN	IPv6 Advanced	IPv6 LAN	VPN	Port Forward	DMZ	DDNS	QoS	Port Setting	Routing	Advance

INTERNET

WAN

Connect Name: Delete Connect

Service:

IP Protocol Version:

WAN IP Mode:

MAC Address Clone: Get Current PC MAC

MAC Address:

NAT Enable:

Overwrite NAT IP:

VLAN Mode:

VLAN ID: (1-4094)

DNS Mode:

Primary DNS:

Secondary DNS:

DHCP

DHCP Renew:

DHCP Vendor(Option 60):

Port Bind

Port_1 Port_2 Port_3 Port_4

Wireless(SSID) Wireless(SSID1) Wireless(SSID2) Wireless(SSID3)

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.

Procedure

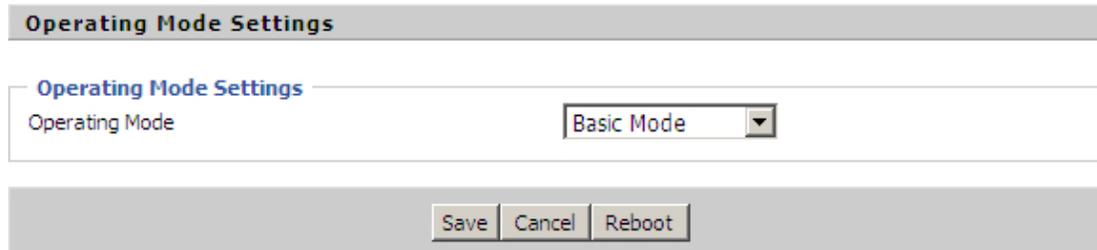
1. Press the button gets PC's MAC address

2. Press the button to save your changes if users don't want to use MAC clone, press the button to cancel the changes

3. Press the button to make the changes effective.

Fast Bridge Setting

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

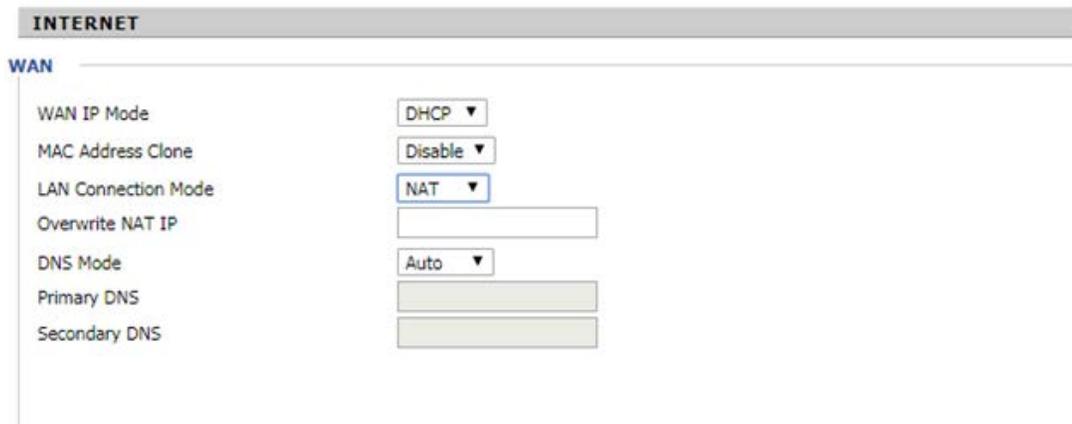


Operating Mode Settings

Operating Mode Settings

Operating Mode

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



INTERNET

WAN

WAN IP Mode

MAC Address Clone

LAN Connection Mode

Overwrite NAT IP

DNS Mode

Primary DNS

Secondary DNS

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

TR069_VOICE_INTERNET Vlan Status	
Connection Type	DHCP
MAC Address	00:21:F2:14:08:13
IP Address	192.168.10.225
Subnet Mask	255.255.255.0
Default Gateway	192.168.10.1
Primary DNS	192.168.10.1
Secondary DNS	

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

VPN Status	
VPN Type	Disable
Initial Service IP	
Virtual IP Address	

PC Port Status	
IP Address	192.168.0.1
Subnet Mask	255.255.255.0
Port Status	Link Down

IPv6 Address configuration

The cnPilot Home Router devices support IPv6 addressing starting from firmware version 4.3.

This section 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 cnPilot Home Router devices are also capable of prefix delegation.

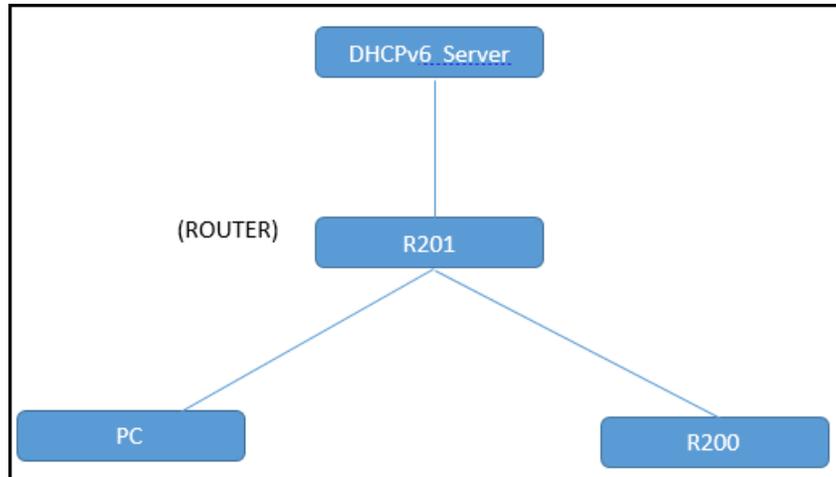
The cnPilot Home Router devices support the following types of modes of IPv6 addresses:

- Stateless DHCPv6

- Statefull DHCPv6

Table 12 **IPv6 Modes**

Mode	Description
Stateless	In Stateless DHCPv6 mode, the cnPilot Home Router 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.

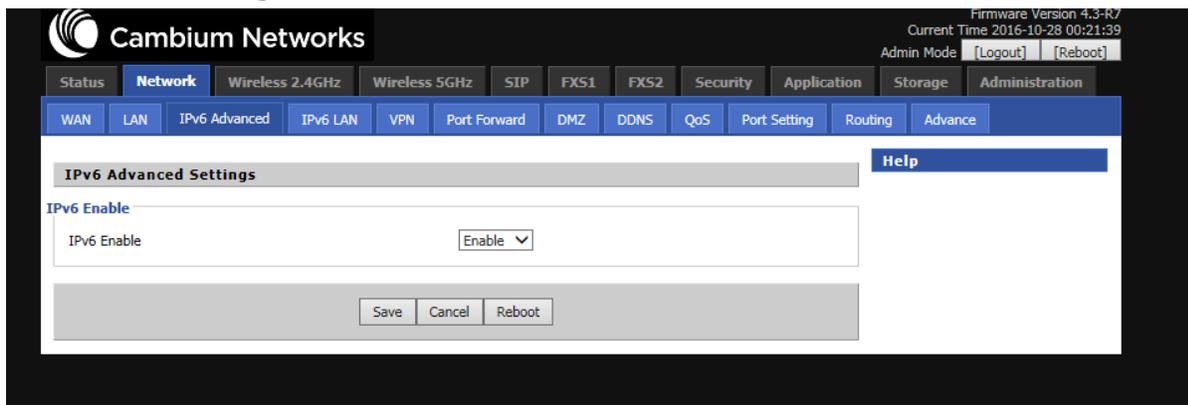


Enabling IPv6

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 13 **Enabling IPv6**

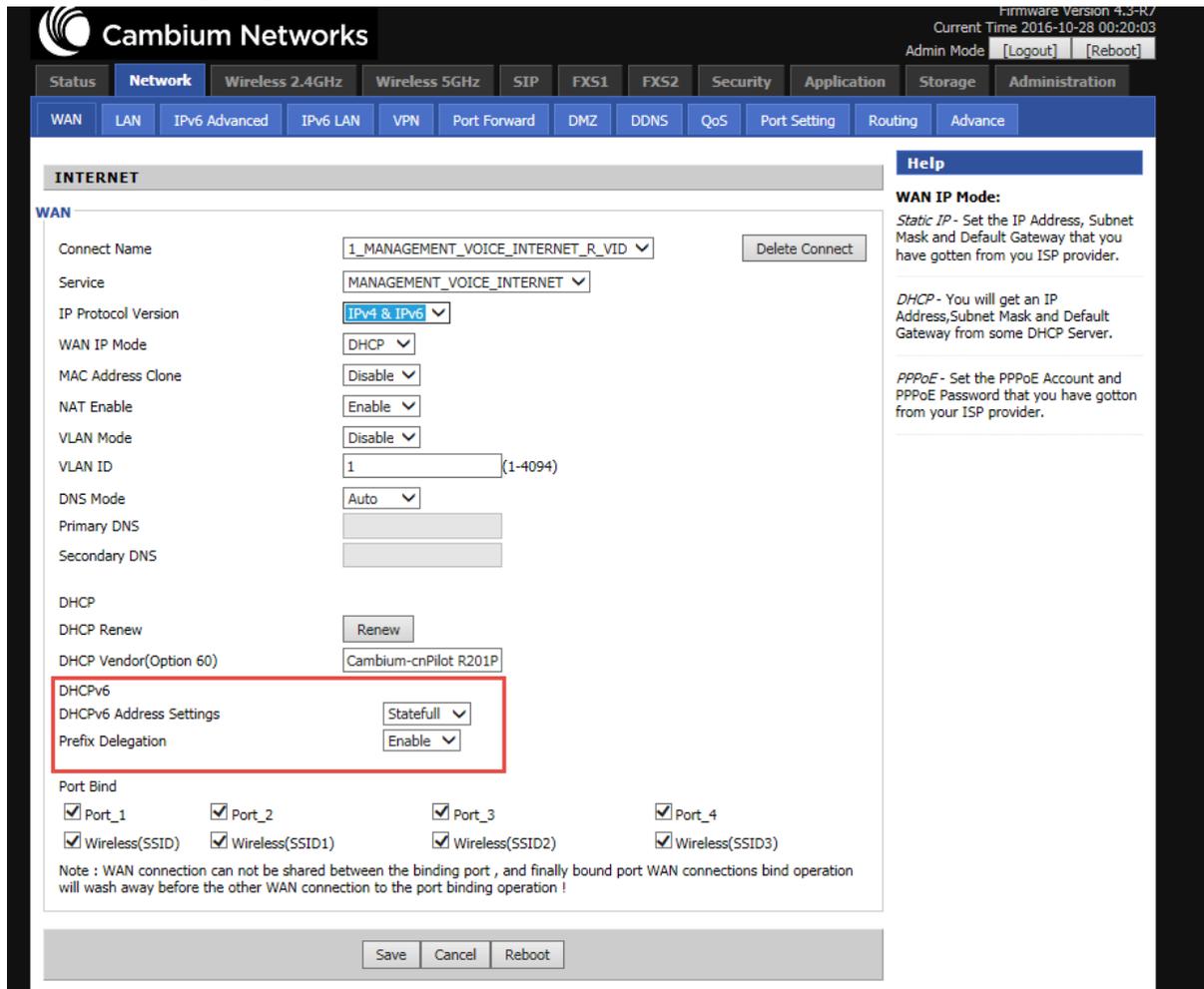


Configuring IPv6

Configuring Statefull IPv6

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

Table 14 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 15 Configuring Stateless IPv6

The screenshot shows the Cambium Networks web interface for configuring the WAN interface. The 'INTERNET' tab is selected, and the 'WAN' section is active. A red box highlights the 'DHCPv6' section, specifically the 'DHCPv6 Address Settings' dropdown set to 'Stateless' and the 'Prefix Delegation' dropdown set to 'Enable'. Other settings include 'IP Protocol Version' set to 'IPv4 & IPv6', 'WAN IP Mode' set to 'DHCP', and 'NAT Enable' set to 'Enable'. A 'Please REBOOT to make the changes effective!' message is displayed at the top.

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 router's status page. It is divided into two main sections: **FXS Port Status** and **Network Status**.

FXS Port Status section:

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

Network Status section:

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	fec0::102/64
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 cnPilot Home Routers can obtain their IPv6 addresses based on how the LAN side DHCPv6 parameters are configured. The cnPilot Home Routers can be either configured as a DHCPv6 server in which the LAN/WLAN clients get IPv6 addresses from the configured pool.

If DHCP server is disabled on the cnPilot Home Routers, the clients will get IPv6 addresses from the external DHCPv6 server configured in the network.

LAN DHCPv6

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

To enable LAN DHCPv6 service:

Cambium Networks Firmware Version 4.3-R3
Current Time 2016-10-27 08:21:11
Admin Mode [Logout] [Reboot]

Status **Network** Wireless 2.4GHz Wireless 5GHz SIP FXS1 FXS2 Security Application Storage Administration

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

IPv6 LAN Setting Help

IPv6 LAN Setting

IPv6 Address

IPv6 Prefix Length (0-128)

DHCPv6 Server

DHCPv6 Status

DHCPv6 Mode

Domain Name

Server Preference (0-255)

Primary DNS Server

Secondary DNS Server

Lease Time (0-86400sec)

IPv6 Address Pool - /

Router Advertisement

Advertise Interval (10-1800sec)

RA Managed Flag

RA Other Flag

Prefix /

Prefix Lifetime (0-3600sec)

LAN

LAN Port

Using the LAN ports the user can plug computers and other devices that need an Internet connection.

Table 16 LAN port

Status	Network	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 pool.

DNS Mode	Select DNS mode, options are Auto and Manual.
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 17 DHCP server settings

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

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

Table 18 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.

VPN

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

Table 19 VPN

The screenshot shows the 'VPN Settings' page in the router's web interface. The navigation bar includes 'Status', 'Network', 'Wireless', 'SIP', 'FXS1', 'FXS2', 'Security', 'Application', 'Storage', and 'Administration'. The 'Network' menu is expanded, showing 'WAN', 'LAN', 'IPv6 Advanced', 'IPv6 LAN', 'VPN', 'Port Forward', 'DMZ', 'DDNS', 'QoS', 'Port Setting', 'Routing', and 'Advance'. The 'VPN' sub-menu is active. The 'VPN Settings' page has a 'Help' button and a 'VPN Settings:' section with a note: 'PPTP/L2TP - The Initial Service IP is the IP Address of a server that provides PPTP/L2TP services.' The 'Administration' section contains the following fields:

- VPN Enable: L2TP (dropdown)
- Initial Service IP: (text input)
- User Name: (text input)
- Password: (password input)
- L2TP Tunnel Name: (text input)
- L2TP Tunnel Password: (password input)
- VPN As Default Route: Disable (dropdown)

At the bottom of the page, there are 'Save', 'Cancel', and 'Reboot' buttons.

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.
L2TP Tunnel Name	Enter the name for L2TP tunnel.
L2TP Tunnel Password	Enter the password for L2TP tunnel.
VPN As Default Route	Enable/Disable the VPN as default route.

DMZ

Table 20 DMZ

Status **Network** 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 Disable ▾

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

Port Forward

Table 21 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
-----	---------	------------	-------------	--------------	----------

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 server.
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.

DDNS Setting

Table 22 DDNS setting

The screenshot shows the DDNS Setting configuration page. The navigation menu includes Status, Network (selected), Wireless, SIP, FXS1, FXS2, Security, Application, Storage, and Ad. The sub-menus under Network are WAN, LAN, VPN, Port Forward, DMZ, DDNS (selected), QoS, MAC Clone, Port Setting, and Routing. The DDNS Setting section contains the following fields:

- Dynamic DNS Provider: None (dropdown menu)
- Account: [text input field]
- Password: [text input field]
- DDNS URL: [text input field]
- Status: DDNS updated Fail!

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

Advance

Table 23 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 Router can provide
Mss Mode	Choose Mss Mode as Manual or Auto.
Mss Value	Set the value of TCP
AntiDos-p	You can choose to enable or prohibit
IP conflict detection	You can choose to enable or prohibit
IP conflict Detecting Interval	Detect IP address conflicts of the time interval

Port Setting

Table 24 Port setting

Status	Network	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 25 QoS

WAN	LAN	VPN	Port Forward	DMZ	QoS	MAC Clone	Port Setting	Routing	Advance						
QoS setting															
oS setting															
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	Check the items you want to delete, click the Delete option
Add	Click Add to add a new rule.



Note

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

Routing

Table 26 Routing

Static Routing Settings

Add a routing rule

Destination	<input type="text" value="1.1.1.1"/>
Host/Net	<input type="text" value="Net"/> ▼
Sub Netmask	<input type="text"/>
Gateway	<input type="text"/>
Interface	<input type="text" value="LAN"/> ▼
Comment	<input type="text"/>

Current Routing table in the system

No.	Destination	Mask	Gateway	Flags	Metric	Interface	Comment

Field Name	Description
Destination	Destination address
Host/Net	Indicates whether single host or a network is being specified. If Net, then one more option appears where user has to configure the subnet.
Gateway	Gateway IP address
Interface	Select the desired LAN/WAN interface.
Comment	Comment

Wireless



Note

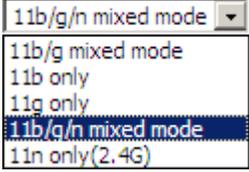
Starting from 4.4 release, any changes in the Wireless/Radio configuration performed on the cnPilot Home Routers can be applied on the fly and does not require a reboot. However, for all other configuration sections a reboot is required to make new configuration changes effective.

Basic

Table 27 Basic

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage	Administration	
Basic		Wireless Security	WMM	WDS	WPS	Station Info	Advanced			
Help										
Basic Wireless Settings										
Wireless Network										
Radio On/Off	Radio Off									
Wireless Connection Mode	AP									
Network Mode	11b/g/n mixed mode									
Multiple SSID	CAMBIUM_2.4GHZ_1	Hidden	<input type="checkbox"/>	Isolated	<input type="checkbox"/>	Max Client	16			
Multiple SSID1		Hidden	<input type="checkbox"/>	Isolated	<input type="checkbox"/>	Max Client	16			
Multiple SSID2		Hidden	<input type="checkbox"/>	Isolated	<input type="checkbox"/>	Max Client	16			
Multiple SSID3		Hidden	<input type="checkbox"/>	Isolated	<input type="checkbox"/>	Max Client	16			
broadcast(SSID)	<input checked="" type="radio"/> Enable <input type="radio"/> Disable									
AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable									
MBSSID AP Isolation	<input type="radio"/> Enable <input checked="" type="radio"/> Disable									
BSSID	00:04:56:03:47:38									
Frequency (Channel)	Auto									
HT Physical Mode	<input checked="" type="radio"/> Mixed Mode <input type="radio"/> Green Field									
Operating Mode	<input type="radio"/> 20 <input checked="" type="radio"/> 20/40									
Channel BandWidth	<input type="radio"/> Long <input checked="" type="radio"/> Short									
Guard Interval	<input type="radio"/> Disable <input checked="" type="radio"/> Enable									
Reverse Direction Grant(RDG)	<input type="radio"/> Disable <input checked="" type="radio"/> Enable									
STBC	<input type="radio"/> Disable <input checked="" type="radio"/> Enable									
Aggregation MSDU(A-MSDU)	<input checked="" type="radio"/> Disable <input type="radio"/> Enable									
Auto Block ACK	<input type="radio"/> Disable <input checked="" type="radio"/> Enable									
Decline BA Request	<input checked="" type="radio"/> Disable <input type="radio"/> Enable									
HT Disallow TKIP	<input type="radio"/> Disable <input checked="" type="radio"/> Enable									
HT LDPC	<input checked="" type="radio"/> Disable <input type="radio"/> Enable									

Field Name	Description
------------	-------------

Radio on/off	Select "Radio off" to disable wireless. Select "Radio on" to enable wireless.
Wireless connection mode	According to the wireless client type, select one of the modes. Modes are AP/ Repeater. Default is AP.
Network Mode	Choose one network mode from the drop-down list. For 5GHz radio the default is 11vht AC/AN/A. 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 R195W Routers support 4 SSIDs on each radio.
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 does not belong to this AP. When the option is enabled, the devices which do not belong to this AP cannot access the devices which are within the AP.
BSSID	MAC address of the AP.
Frequency (Channel)	You can select Auto Select.
HT Physical Mode Operating Mode	1. Mixed Mode: In this mode, the previous wireless card can recognize and connect to the Pre-N AP, but the throughput will be affected 2. Green Field: high throughput can be achieved, but it will affect backward compatibility, and security of the system
Channel Bandwidth	Select channel bandwidth, default is 20 MHz and 20/40 MHz. Default is 20/40
Guard Interval	Select long/short. default is short.
Reverse Direction Grant (RDG)	Enabled: Devices on the WLAN are able to transmit to each other without requiring an additional contention-based request to transfer (i.e. devices are able to transmit to another device on the network during TXOP)

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

Wireless Security

Table 28 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	Select the SSID for which security parameters need to be configured.
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 29 Wi-Fi Security Setting

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 30 WPA-PSK

WIFI Security Setting	
Select SSID	
SSID choice	CAMBIUM_2.4GHz_027898 ▼
"CAMBIUM_2.4GHz_027898"	
Security Mode	WPA2-PSK ▼
WPA	
WPA Algorithms	<input type="radio"/> TKIP <input checked="" type="radio"/> AES <input type="radio"/> TKIPAES
Pass Phrase	*****
Key Renewal Interval	3600 sec (0 ~ 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 31 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 32 Wireless Access Policy

Access policy

Policy Allow ▾

Add a station MAC

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

Example: Prohibit the device whose wireless network card MAC address is 00:1F: D0: 62: BA: FF's to access the wireless network, and allow other computers to access the network.

Implementation: As shown, the Policy is Reject, add 00:1F: D0: 62: BA: FF to the MAC, click Save and reboot the device settings to take effect.

WMM

Table 33 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"/>		
<input type="button" value="Apply"/> <input type="button" value="Cancel"/>								

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 34 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

Save Cancel Reboot

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

WDS Setting Help

WDS Config

WDS Mode	<input type="text" value="Lazy Mode"/>
Phy Mode	<input type="text" value="CCK"/>
EncrypType	<input type="text" value="NONE"/>
Encryp Key	<input type="text"/>
EncrypType	<input type="text" value="NONE"/>
Encryp Key	<input type="text"/>
EncrypType	<input type="text" value="NONE"/>
Encryp Key	<input type="text"/>
EncrypType	<input type="text" value="NONE"/>
Encryp Key	<input type="text"/>

Save Cancel Reboot

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 35 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"> cnPilot Wi-Fi R195W Routers use a default security policy to allow other non-WPS users to access and apply.

- WPS Mode**
- **PIN** : Enter the PIN code of the wireless device which accesses to this LAN in the following option, and press apply. Then cnPilot Home Router R195W 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 36 Station info

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

Advanced Wireless	
Advanced Wireless	
BG Protection Mode	Auto ▾
Beacon Interval	100 ms (range 20 - 999, default 100)
Data Beacon Rate (DTIM)	3 (range 1 - 255, default 3)
Fragment Threshold	2346 (range 256 - 2346, default 2346)
RTS Threshold	2347 (range 1 - 2347, default 2347)
TX Power	12.5% ▾ (5dBm)
Short Preamble	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Short Slot	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Tx Burst	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Pkt_Aggregate	<input checked="" type="radio"/> Enable <input type="radio"/> Disable
Country Code	JP (Japan) ▾
Wi-Fi Multimedia	
WMM Capable	
Multiple SSID	<input checked="" type="checkbox"/>
Multiple SSID1	<input type="checkbox"/>
Multiple SSID2	<input type="checkbox"/>
Multiple SSID3	<input type="checkbox"/>
APSD Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
DLS Capable	<input type="radio"/> Enable <input checked="" type="radio"/> Disable
Multicast-to-Unicast Converter	
Multicast-to-Unicast	<input type="radio"/> Enable <input checked="" type="radio"/> Disable

Field Name	Description
BG Protection Mode	Select G protection mode, options are on, off and automatic.
Beacon Interval	The interval of sending a wireless beacon frame, within this range, it will send a beacon frame for the information of the surrounding radio network.
Data Beacon Rate(DTIM)	Specify the interval of transmitting the indication message, it is a kind of cut down operation, and it is used for informing the next client which is going to receive broadcast multi-cast.
Fragment Threshold	Specify the fragment threshold for the packet, when the length of the packet exceeds this value, the packet is divided.
RTS Threshold	Specify the packet RTS threshold, when the packet exceeds this value, the router will send RTS to the destination site consultation

TX Power	Define the transmission power of the current AP, the greater it is, the stronger the signal is.
Short Preamble	Default is enable, cnPilot R195W Routers 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.
Wi-Fi Multimedia (WMM)	
WMM Capable	Enable/Disable WMM.
APSD Capable	Enable/Disable APSD. Once it is enabled, it may affect wireless performance, but can play a role in energy-saving power
WMM Parameters	Press WMM Configuration , the webpage will jump to the configuration page of Wi-Fi multimedia.
Multicast-to-Unicast Converter	Enable/Disable Multicast-to-Unicast. By default, it is Disabled.

WDS

See [WDS](#).

WPS

See [WPS](#).

Station Info

See [Station Info](#).

Advanced

See [Advanced](#).

SIP

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

SIP Settings

Table 38 SIP settings

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage
SIP Settings		VoIP QoS						
SIP Parameters								
SIP Parameters								
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="button" value="Enable"/>		RFC 2543 Call Hold	<input type="button" value="Enable"/>				
SRTP	<input type="button" value="Disable"/>		SRTP Prefer Encryption	<input type="button" value="AES_CM"/>				
Service Type	<input type="button" value="Common"/>							
Response Status Code Handling								
Retry Reg RSC	<input type="text"/>							
NAT Traversal								
NAT Traversal								
NAT Traversal	<input type="button" 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 service type.
NAT Traversal	<ol style="list-style-type: none"> 1. Enable/Disable NAT Traversal 2. cnPilot Home Router supports STUN Traversal; if user wants to traverse NAT/Firewall, select the STUN.
STUN Server Address	Add the correct STUN service provider IP address.
NAT Refresh Interval	Set NAT Refresh Interval, default is 60s.
STUN Server Port	Set STUN Server Port, default is 5060.

Dial Plan

Parameters and Settings

Table 39 Parameters and settings

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage
SIP Account		Preferences		Dial Plan	Blacklist	Call Log		

Dial Plan

General

Dial Plan: ▾

Unmatched Policy: ▾

No.	FXS	Digit Map	Action	Move Up	Move Down	
1	FXS 1	Line1	Dial Out	▲	▼	☐

FXS: ▾

Digit Map:

Action: ▾

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 Routers will reject the matched number, while Dial Out means cnPilot Home Routers 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 40 Adding one dial plan

Dial Plan					
General					
Dial Plan	Disable ▼				
Unmatched Policy	▼				
No.	FXS	Digit Map	Action	Move Up	Move Down
FXS	FXS 1 ▼				
Digit Map	<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 41 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 from 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	<dialled:substituted>	Replace dialled 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 42 Blacklist

Blacklist Upload && Download			
Blacklist Upload && Download			
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 Router; 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 43 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

VoIP QoS

Table 44 VoIP QoS

Status
Network
Wireless
SIP
FXS1
FXS2
Security
Application
Storage

SIP Settings
VoIP QoS

QoS Settings

Layer 3 QoS

SIP QoS(0-63)	46	
RTP QoS(0-63)	46	

Save Cancel 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 45 SIP Account – Basic

Basic	
Basic Setup	
Line Enable	Enable ▾
Outgoing Call without Registration	Disable ▾
Proxy and Registration	
Proxy Server	10.110.32.54
Outbound Server	
Backup Outbound Server	
Proxy Port	5060
Outbound Port	5060
Backup Outbound Port	5060
Subscriber Information	
Display Name	1000
Account	1000
Phone Number	1000
Password	*****
Audio Configuration	
Field Name	Description
Line Enable	Enable/Disable the line.
Peer To Peer	Enable/Disable PEER to PEER. If enabled, SIP-1 will not send register request to SIP server; but in Status/SIP Account Status webpage, Status is Registered; lines 1 can dial out, but the external line number cannot dial line1.
Proxy Server	The IP address or the domain of SIP Server
Outbound Server	The IP address or the domain of Outbound Server
Backup Outbound Server	The IP address or the domain of Backup Outbound Server
Proxy port	SIP Service port, default is 5060
Outbound Port	Outbound Proxy's Service port, default is 5060
Backup Outbound Port	Backup Outbound Proxy's Service port, default is 5060

Display Name	The number will be displayed on LCD
Phone Number	Enter telephone number provided by SIP Proxy
Account	Enter SIP account provided by SIP Proxy
Password	Enter SIP password provided by SIP Proxy

Audio Configuration

Table 46 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 Support	Enable/Disable silence support.
Echo Cancel	Enable/Disable echo cancel. By default, it is enabled.
Auto Gain Control	Enable/Disable auto gain.
T.38 Enable	Enable/Disable T.38
T.38 Redundancy	Enable/Disable T.38 Redundancy
T.38 CNG Detect Enable	Enable/Disable T.38 CNG Detect
gpmc attribute Enable	Enable/Disable gpmc attribute.

Supplementary Service Subscription

Table 47 Supplementary service

Supplementary Service Subscription			
Supplementary Services			
Call Waiting	Enable ▾	Hot Line	<input type="text"/>
MWI Enable	Enable ▾	Voice Mailbox Numbers	<input type="text"/>
MWI Subscribe Enable	Disable ▾	VMWI Serv	Enable ▾
DND	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 (indicates message waiting). 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 48 Advanced

Advanced

Advanced Setup

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

Field Name	Description
Domain Name Type	If or not use domain name in the SIP URI.
Carry Port Information	If or not carry port information in the SIP URI.
Signal Port	The local port of SIP protocol, default is 5060.
DTMF Type	Choose the DTMF type from Inbound, RFC2833 and SIP INFO.

RFC2833 Payload(>=96)	User can use the default setting.
Register Refresh 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 49 Volume settings

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

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

Regional

Table 50 Regional

Regional

Tone Type: USA ▼

Dial Tone:

Busy Tone:

Off Hook Warning Tone:

Ring Back Tone:

Call Waiting Tone:

Ringing Cadence:

Min Jitter Delay(0-600ms): Max Jitter Delay(20-1000ms):

Ringing Time(10-300sec):

Ring Waveform: Sinusoid ▼ Ring Voltage(40-63 Vrms):

Ring Frequency(15-30Hz): VMWI Ring Splash Len(0.1-10sec):

Flash Time Max(0.2-1sec): Flash Time Min(0.1-0.5sec):

Field Name	Description																
Tone Type	<p>Choose tone type as UK, China, US, Hong Kong and so on. A sample Tone Type for UK is shown below:</p> <table border="1" style="width: 100%; border-collapse: collapse; margin-bottom: 10px;"> <thead> <tr style="background-color: #cccccc;"> <th style="text-align: left;">COUNTRY/PARAMETER</th> <th style="text-align: left;">VALUE</th> </tr> </thead> <tbody> <tr> <td>U.K</td> <td></td> </tr> <tr> <td>Dial tone</td> <td>350@-19;440@-19;30(*0/1+2)</td> </tr> <tr> <td>Busy tone</td> <td>400@-19;30(.375/.375/1)</td> </tr> <tr> <td>Ring Back Tone</td> <td>400@-19;450@-19;10(0.4/0.2/1+2,0.4/2.0/1+2)</td> </tr> <tr> <td>On-hook Voltage</td> <td>50Vrms</td> </tr> <tr> <td>Impedance Matching</td> <td>370+620 310nF</td> </tr> <tr> <td>Ring Voltage</td> <td>55Vrms</td> </tr> </tbody> </table> <p>Note: Currently, selecting a particular country does not load the correct Ringing parameters as per standard. If standard based ringing cadence is desired then the user has to select Custom option from the drop-down list and enter the country specific parameters manually.</p>	COUNTRY/PARAMETER	VALUE	U.K		Dial tone	350@-19;440@-19;30(*0/1+2)	Busy tone	400@-19;30(.375/.375/1)	Ring Back Tone	400@-19;450@-19;10(0.4/0.2/1+2,0.4/2.0/1+2)	On-hook Voltage	50Vrms	Impedance Matching	370+620 310nF	Ring Voltage	55Vrms
COUNTRY/PARAMETER	VALUE																
U.K																	
Dial tone	350@-19;440@-19;30(*0/1+2)																
Busy tone	400@-19;30(.375/.375/1)																
Ring Back Tone	400@-19;450@-19;10(0.4/0.2/1+2,0.4/2.0/1+2)																
On-hook Voltage	50Vrms																
Impedance Matching	370+620 310nF																
Ring Voltage	55Vrms																
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
Ringing Cadence	The ringing pattern heard by the dialer before the called party picks up the call.
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 R195W Routers 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 51 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 52 Miscellaneous

Miscellaneous

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

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

FXS2

The settings of FXS2 are the same as FXS1. See [FXS1](#) on page 85.

Security

Filtering Setting

Table 53 Filtering setting

Basic Settings

Basic Settings

Filtering Disable ▾

Default Policy Drop ▾

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

Save Cancel

IP/Port Filter Settings

Mac address

Dest IP Address

Source IP Address

Protocol NONE ▾

Dest. Port Range -

Src Port Range -

Action Drop ▾

Comment

(The maximum rule count is 32)

Save Cancel

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

Content Filtering

Table 54 Content filtering

Basic Settings	
Basic Settings	
Filtering	Disable ▾
Default Policy	Drop ▾
The packet that don't match with any rules would be Drop	
<input type="button" value="Save"/> <input type="button" value="Cancel"/>	

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

Field Name	Description
Filtering	Enable/Disable content Filtering
Default Policy	The default policy is to accept or to prohibit filtering rules
Current Webs URL 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 55 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 56 IGMP

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

Storage

Disk Management

This page is used to manage the USB storage device.

Table 57 Disk Management

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage				
<div style="display: flex; justify-content: space-between;"> Disk Management Ftp Setting Smb Setting </div>												
Disk Management												
Folder List <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>									Directory Path	Partition	<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="RemoveDisk"/>	
Directory Path	Partition											
<input type="button" value="Add"/> <input type="button" value="Delete"/> <input type="button" value="RemoveDisk"/>												
Partition Status <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>									Partition	Path	<input type="button" value="Format"/> <input type="button" value="Re-allocate"/>	
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 58 FTP Setting

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage
Disk Management		Ftp Setting		Smb Setting				

FTP Setting

FTP Server Setup

FTP Server Enable Disable

FTP Server Name

Anonymous Login Enable Disable

FTP Port

Max. Sessions

Create Directory Enable Disable

Rename File/Directory Enable Disable

Remove File/Directory Enable Disable

Read File Enable Disable

Write File Enable Disable

Download Capability Enable Disable

Upload Capability Enable Disable

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

Smb Setting

Table 59 Smb setting

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage
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	Allows 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 60 Save Config File

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

Save Config File

Config File Upload && Download

Local File Choose File No file chosen

Upload Download

Administrator settings

Table 61 Administrator settings

Administrator Settings	
Password Reset	
User Type	Admin User ▼
New User Name	admin
New Password	<input type="text"/> (The maximum length is 25)
Confirm Password	<input type="text"/>
Language	
Language	English ▼
VPN Access	
Management Using VPN	Disable ▼
Web Access	
Remote Web Login	Enable ▼
Allow Wireless host	Disable ▼
Local Web Port	80
Web Port	80
Web SSL Port	443
Web Idle Timeout(0 - 60min)	5
Allowed Remote IP(IP1;IP2;...)	0.0.0.0
SSH Access	
Remote SSH	Disable ▼
Local SSH	Enable ▼
SSH Port	22
HostName	
HostName	cnPilot-R190V

Time/Date Setting

NTP Settings

NTP Enable:

Option 42:

Current Time: 2017 - 06 - 09 . 11 : 04 : 33

Sync with host:

Time Zone: (GMT-06:00) Central Time

Primary NTP Server: pool.ntp.org

Secondary NTP Server:

NTP synchronization(L - 1440min): 60

Daylight Saving Time

Daylight Saving Time:

System Log Setting

Syslog Setting

Syslog Enable:

Syslog Level: INFO

Login Syslog Enable:

Call Syslog Enable:

Net Syslog Enable:

Device Management Syslog Enable:

Device Alarm Syslog Enable:

Kernel Syslog Enable:

Remote Syslog Enable:

Remote Syslog Server:

Factory Defaults Setting

Factory Defaults Setting

Factory Defaults Lock:

Factory Defaults

Reset to Factory Defaults

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.
Management using VPN	
Remote Web Login	Enable/Disable remote Web login
Allow wireless host	To allow all the wireless clients connected to the cnPilot Home Router to access the management interface
Local 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.
SSH	Enable/Disable telnet.

Enabling Mangement access for wireless clients

To allow all the wireless clients connected to the cnPilot Home Router to access the management interface:

1. Navigate to **Administrator** tab.
2. Enable **Allow Wireless Host** option under **Web Access**.

The user must have administrator permissions to make this change.

Enabling SNMP access over WAN

To enable SNMP access over WAN:

1. Navigate to **Administrator > SNMP** tab.
2. Enable **Remote SNMP Login** option.

The user must have administrator permissions to make this change.

The screenshot displays the SNMP Configuration page. The navigation bar at the top includes tabs for Status, Network, Wireless 2.4GHz, Wireless 5GHz, SIP, FXS1, FXS2, Security, Application, Storage, and Administration. The Administration tab is active, and the SNMP sub-tab is selected. The main configuration area includes:

- SNMP Service: Enable (dropdown)
- Remote SNMP login: Disable (dropdown)
- Trap Server Address: (text input)
- Read Community Name: public (text input)
- Write Community Name: private (text input)
- Trap Community: trap (text input)
- Trap period interval(sec): 300 (text input)

At the bottom, there are buttons for Save, Cancel, and Reboot. A Help box on the right side of the page provides the following information:

Help
SNMP Configuration:
 Allow the device to be managed by the Manager which is set in the SNMP Manager IP.

NTP settings

Table 62 NTP settings

Time/Date Setting	
NTP Settings	
NTP Enable	Enable ▼
Option 42	Disable ▼
Current Time	2016 - 01 - 19 . 05 : 55 : 06
Sync with host	Sync with host
NTP Settings	(GMT-06:00) Central Time ▼
Primary NTP Server	pool.ntp.org
Secondary NTP Server	
NTP synchronization(1 - 1440min)	60
Daylight Saving Time	
Daylight Saving Time	Disable ▼

Field Name	Description
NTP Enable	Enable/Disable NTP
Option 42	Enable/Disable DHCP option 42. This option specifies a list of the NTP servers available to the client by IP address.
Current Time	Display current time
NTP Settings	Setting the Time Zone
Primary NTP Server	Primary NTP server's IP address or domain name
Secondary NTP Server	Options for NTP server's IP address or domain name
NTP synchronization	NTP synchronization cycle, cycle time can be 1 to 1440 minutes in any one, the default setting is 60 minutes

Daylight Saving Time

Table 63 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 64 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 65 Factory Defaults Setting

Factory Defaults Setting	
<p>Factory Defaults Setting</p> <div style="border: 1px solid #ccc; padding: 10px;"> <p>Factory Defaults Lock Disable ▾</p> </div>	
Description	
<p>With this lock enabled, user cannot factory reset the box using the hardware switch.</p>	

Factory Defaults

Table 66 Factory Defaults

Factory Defaults	
Reset to Factory Defaults	Factory Default
Description	
<p>Click Factory Default to restore the cnPilot Home Router to factory settings.</p>	

Firmware Upgrade

Table 67 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 browse the file
3. Press to start upgrading

Provision

Provisioning allows cnPilot Home Router to auto-upgrade and auto-configure devices which support TFTP, HTTP and HTTPS .

- Before testing or using TFTP, user should have tftp server and upgrading file and configuring file.
- Before testing or using HTTP, user should have http server and upgrading file and configuring file.
- Before testing or using HTTPS, user should have https server and upgrading file and configuring file and CA Certificate file (should same as https server's) and Client Certificate file and Private key file

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

Table 68 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 R195W Routers will retry resync after the “Resync Error Retry Delay” time, default is 3600s.
Resync Error Retry Delay(rec)	Set the periodic time for resync, default is 3600s.
Forced Resync Delay(sec)	If it’s time to resync, but cnPilot R195W Router is busy now, in this case, cnPilot R195W Router will wait for a period time, the longest is “Forced Resync Delay”, default is 14400s, when the time over, cnPilot R195W Router will be 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 69 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 R195W Routers will try upgrading again after "Upgrade Error Retry Delay" period, default is 3600s.
Upgrade Rule	URL of upgrade file

SNMP

Table 70 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 71 TR069

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

TR069 Configuration	
ACS	
TR069 Enable	Disable ▾
CWMP	Enable ▾
ACS URL	<input type="text"/>
User Name	000456-C3VoIP-200P-400FQU001GLX
Password	●●●●●●●●●●
Periodic Inform Enable	Enable ▾
Periodic Inform Interval	30
Connect Request	
User Name	<input type="text"/>
Password	<input type="text"/>

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

Periodic Inform Enable	Enable the function of periodic inform or not. By default, it is Enabled
Periodic Inform Interval	Periodic notification interval with the unit in seconds. The default value is 43200s
Connect Request parameters	
User Name	The username used to connect the TR069 server to the DUT.
Password	The password used to connect the TR069 server to the DUT.

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", },
{"WPEncryptionLevel", },
{"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", },
        {"WANPPPConnectionNumberOfEntries", },
        {"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", },
    {"", },
    {"", },
{"", },
{"WANPPPConnection", },
    {"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", },

```



```

    {"PSTNSoftSwitchOver", },
    {"FaxT38", },
    {"FaxPassThrough", },
    {"ModemPassThrough", },
    {"ToneGeneration", },
    {"RingGeneration", },
    {"NumberingPlan", },
    {"ButtonMap", },
    {"VoicePortTests", },
    {"SIP", },
        {"Role", },
        {"Extensions", },
        {"Transports", },
        {"URISchemes", },
        {"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", },
    {"", },
  {"", },
{"", },
{"Session", },
  {"1", },
    {"SessionStartTime", },
    {"SessionDuration", },
    {"FarEndIPAddress", },
    {"FarEndUDPPort", },
    {"LocalUDPPort", },
  {"", },
{"", },
{"Stats", },
  {"ResetStatistics", },
  {"PacketsSent", },
  {"PacketsReceived", },
  {"BytesSent", },
  {"BytesReceived", },
  {"PacketsLost", },
  {"Overruns", },
  {"Underruns", },
  {"IncomingCallsReceived", },
  {"IncomingCallsAnswered", },
  {"IncomingCallsConnected", },
  {"IncomingCallsFailed", },
  {"OutgoingCallsAttempted", },
  {"OutgoingCallsAnswered", },

```


Table 72 Scheduled Tasks

Scheduled Tasks					
Scheduled Wifi					
No.	Enable	SSID	Week Select	Open Time	Close Time
<input type="button" value="Delete Selected"/> <input type="button" value="Add"/> <input type="button" value="Edit"/>					
Scheduled Reboot					
Scheduled Reboot	Disable ▼				
Scheduled Mode	EveryDay ▼				
Time	00 ▼	:	00 ▼		
Scheduled PPPOE					
Scheduled PPPOE	Disable ▼				
Scheduled Mode	EveryDay ▼				
Time	00 ▼	:	00 ▼		

Field Name	Description
Scheduled Wi-Fi	Select the Wi-Fi and click Edit to set the timings.
Scheduled Reboot	Set values for Scheduled Reboot, Scheduled Mode, and Time.
Scheduled PPPoE	Set values for Scheduled PPPoE, Scheduled Mode, and Time.

Diagnosis

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

Table 73 Diagnosis

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage	Administration
Management	Firmware Upgrade	Scheduled Tasks	Certificates	Provision	SNMP	TR069	cnMaestro	Diagnosis	
Operating Mode									
Packet Trace									Help
Packet Trace									
Tracking Interface		WAN							
Packet Trace		start stop save							
Ping Test									
Ping Test									
Dest IP/Host Name		<input type="text"/>							
WAN Interface		1_MANAGEMENT_VOICE_INTERNET_R_VID_							
<div style="border: 1px solid gray; height: 100px;"></div>									
Apply		Cancel							
Traceroute Test									
Traceroute Test									
Dest IP/Host Name		<input type="text"/>							
WAN Interface		1_MANAGEMENT_VOICE_INTERNET_R_VID_							
<div style="border: 1px solid gray; height: 100px;"></div>									
Apply		Cancel							

Description**1. Packet Trace**

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

2. Ping Test

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

Ping Test

Ping Test

Dest IP/Host Name

WAN Interface

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

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

3. Traceroute Test

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

Traceroute Test

Traceroute Test

Dest IP/Host Name

WAN Interface

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

Operating Mode

Table 74 Operating mode

Description

Choose the Operation Mode as Basic Mode or Advanced Mode(Default).

In Basic mode, multi WAN configuration is not allowed and the device can be configured either as a simple NAT or Bridge device.

System Log

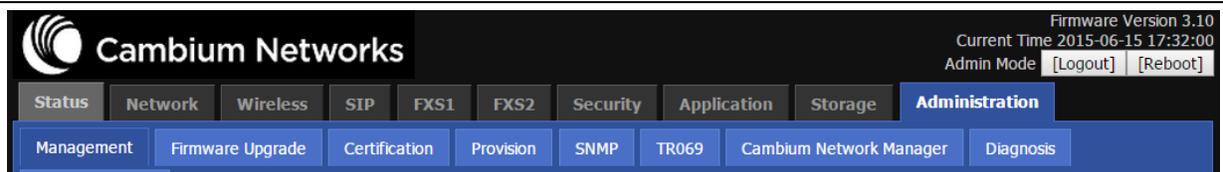
Table 75 System log

Description

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

Logout

Table 76 Logout



Description

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

Reboot

Press the **Reboot** button to reboot cnPilot Home Routers.

Chapter 4: Troubleshooting Guide

This chapter covers:

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

Configuring PC to get IP Address automatically

Please refer the [Quick Start Guide](#) to configure your PC to get IP Address automatically.

Cannot connect to the Web GUI

Solution:

- Check if the Ethernet cable is properly connected
Connect to LAN port and access <http://192.168.11.1>. Check on any other browser apart from Internet explorer such as Firefox or Mozilla
- Contact your administrator, supplier or ISP for more information or assistance.

Forgotten Password

The default password is admin/admin user/user, however if it had been changed to non-default, then factory reset may be required.



Note

On factory reset all the device configuration will be reset to default.

Solution:

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

If device is onboarded in cnMaestro then password can be set via config push.

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"> Ensure that the correct cnMaestro URL is configured. If the URL is correct, check the DNS settings and Internet connectivity. 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.
Invalid Cambium ID/Password	Wrong configuration of cambium ID or On Boarding key	<ul style="list-style-type: none"> Ensure that the correct credentials are entered.
Invalid Cookie or Cambium ID not configured	Device is unclaimed	<ul style="list-style-type: none"> Claim the device either by serial number or Cambium ID
Device Not Claimed	Device is not claimed	<ul style="list-style-type: none"> Claim the device either by serial number or Cambium ID
Connecting	Device is trying to connect to the cnMaestro server	<ul style="list-style-type: none"> Device is in connecting state

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

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.

Appendix: Third Party Software

The software may contain one or more items of Third-Party Software supplied by other third-party suppliers. The terms of this Agreement govern your use of any Third-Party Software license is included, in which case your use of the unless a separate third-party software license is included, in which case your use of the third-party software will then be governed by the separate third-party license.

Zap

Copyright (c) 2004-2009, Ruckus Wireless, Inc.

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- * Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- * Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
- * Neither the name of Ruckus Wireless nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDERS AND CONTRIBUTORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT, SHALL COPYRIGHT HOLDER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Appendix: General Details

Manufacturer: Cambium Networks Inc.

Address: 3800 Golf Road #360, Rolling Meadows, IL 60008 USA.

Importers:

Address:

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

Hereby, Cambium Networks Inc. agrees that this device is in compliance with the essential requirements and other relevant provisions of Directive 2014/53/EU. A copy of the declaration of conformity can be obtained with this user manual.

This product is not restricted in the EU.

Operation Temperature Range: 0~50 Degree C

Standard Power Supply:

12V, 1A

This equipment should be installed and operated with minimum distance 20cm between the radiator.

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 http://www.faqs.org/rfcs/rfc826.html .
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 http://www.faqs.org/rfcs/rfc2131.html . 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 http://www.faqs.org/rfcs/rfc959.html .
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 http://www.faqs.org/rfcs/rfc959.html .
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 http://www.faqs.org/rfcs/rfc2068.html .
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 http://www.faqs.org/rfcs/rfc792.html .
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 http://www.faqs.org/rfcs/rfc791.html .
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 http://www.faqs.org/rfcs/rfc1631.html .
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. RFC 1001 defines the concepts and methods . RFC 1002 defines the detailed specifications. See http://www.faqs.org/rfcs/rfc1001.html and http://www.faqs.org/rfcs/rfc1002.html .
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 http://www.faqs.org/rfcs/rfc1631.html .
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 http://www.faqs.org/rfcs/rfc1157.html .
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 http://www.faqs.org/rfcs/rfc2050.html . 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 http://www.faqs.org/rfcs/rfc793.html .
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