



User Guide
cnPilot R195P Model

System Release 4.6



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	3
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
IC Warning.....	7
CE Note.....	8
Conventions, warnings, cautions, and notes	10
Conventions.....	10
Warnings	10
Cautions.....	10
Notes	10
Chapter 1: Product Description.....	11
LED Indicators and Interfaces	12
Hardware Installation	13
Chapter 2: Basic Settings	14
Web Management Interface	14
Accessing and Configuring cnPilot Home Router via cnMaestro	18
Configuring via Voice Commands.....	19
Chapter 3: Advanced Configuration.....	27
Two-Level Management	28
Setting the Time Zone	29
Status	30
Configuring an Internet Connection	35
Network	37
WAN	37
IPv6 Address configuration	49
LAN	55
Wireless	67
WDS.....	79
SIP	80
FXS1	86
FXS2	96

Security	97
Application	102
Storage	104
Administration	107
Management	107
Firmware Upgrade	114
Provision	114
SNMP	117
TR-069	118
Scheduled Tasks	133
Diagnosis	134
Operating Mode	137
System Log	137
Logout	138
Reboot	138
Chapter 4: Troubleshooting Guide	139
Configuring PC to get IP Address automatically	139
Cannot connect to the Web GUI	139
Forgotten Password	139
cnMaestro On-boarding troubleshooting	139
Appendix: Third Party Software	142
Appendix: General Details	143
Glossary	144

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Support website:

<https://www.cambiumnetworks.com/support>

Address:

Cambium Networks Limited,
Linhay Business Park,
Eastern Road,
Ashburton,
Devon, UK,
TQ13 7UP

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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.

Warning

This device complies with Part 15 of the FCC Rules. Operation is subject to the following two conditions: (1) this device may not cause harmful interference, and (2) this device must accept any interference received, including interference that may cause undesired operation.

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

Note: 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.

RF Exposure Statement

To maintain compliance with FCC's RF Exposure guidelines. This equipment should be installed and operated with minimum distance between 20cm the radiator your body: Use only the supplied antenna.

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。



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

- 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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。



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: v4.5

Software Version: 4.6-R7(201911271410)

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 comply with 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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

CE

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 R195P 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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Chapter 1: Product Description

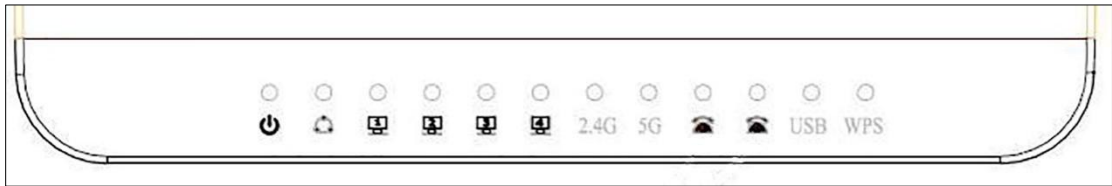
This chapter covers:

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

LED Indicators and Interfaces

Figure 1 cnPilot LED Indicators



LED	Status	Explanation
USB	On (Green)	Connected
	Off	Disconnected
2.4G/5G	Blinking (Green)	The port is passing data
	On (Green)	The port is connected
WAN	Off	The port is disconnected
	Blinking (Green)	The data is transmitting
	On (Green)	The port is connected at 100/1000 Mbps
LAN 1/2/3/4	Off	The port is disconnected
	Blinking (Green)	The port is transmitting data
POWER	ON (Green)	Router is powered on and running normally
	Off	The router is powered off

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**.

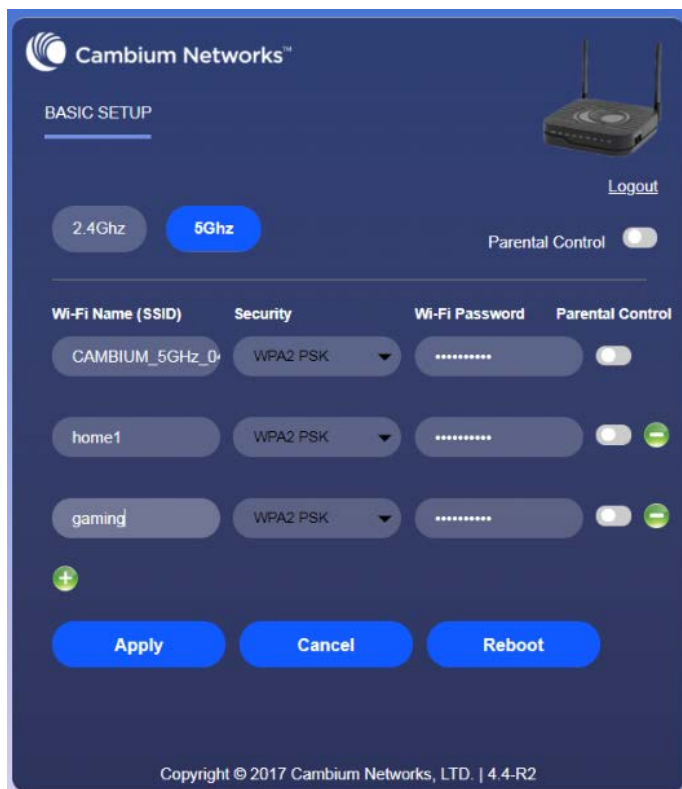
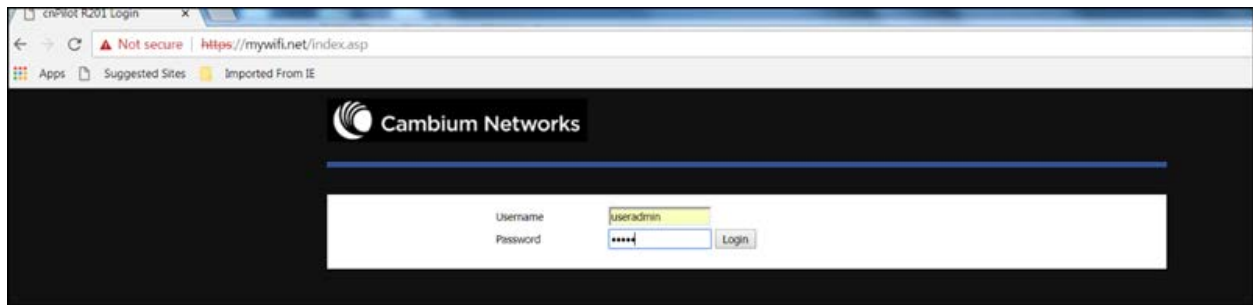


Note

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

Figure 3 EZ UI

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。



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.

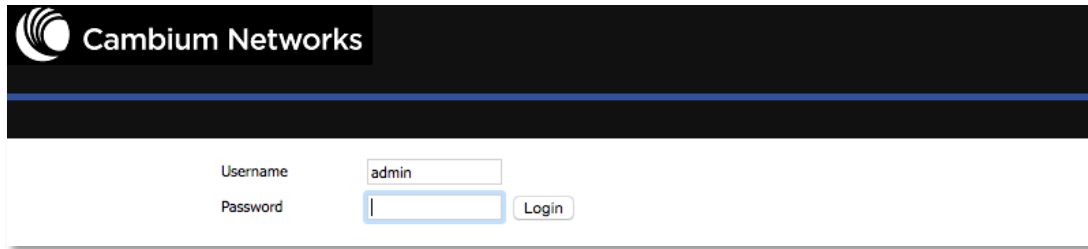
Refer [Enabling Mangement access for wireless client](#) on "how to enable management access for wireless clients".

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Figure 2 Login Prompt – LAN Port



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

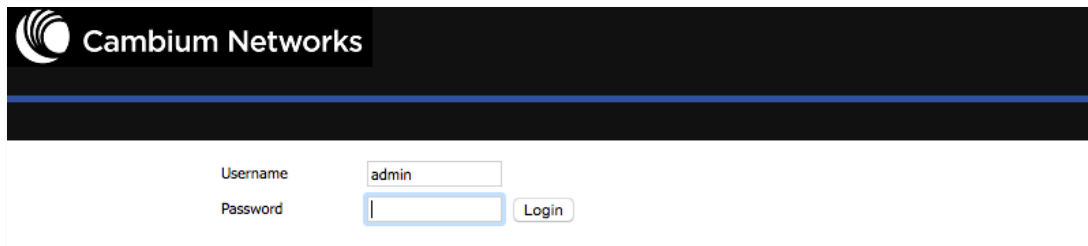
By default, the web access from WAN interface is disabled from 4.3.3 release onwards for security reasons.

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 3 Login Prompt – WAN Port



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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。



Note

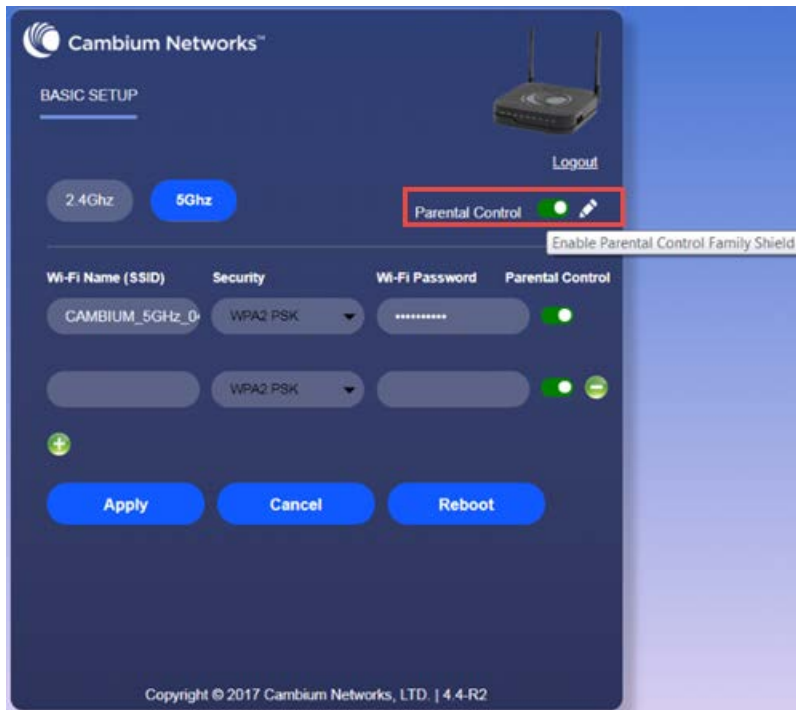
If you fail to access to the web configuration, see [Chapter 4: Troubleshooting Guide](#) for more information.

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).

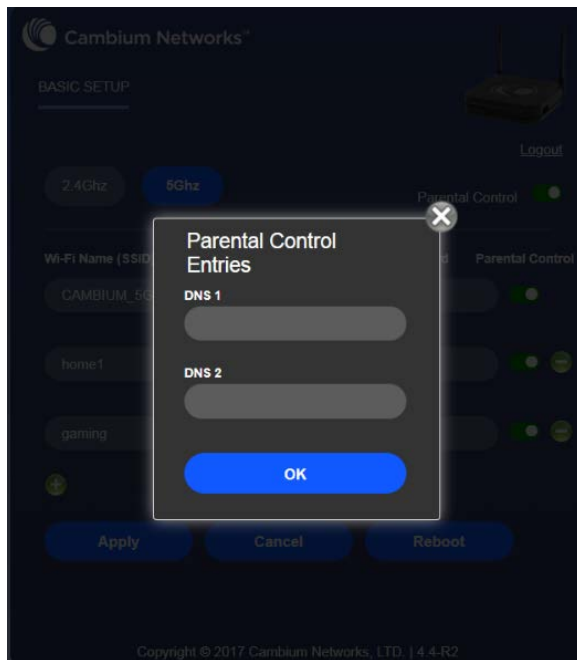
Parental Control feature is only available while using EZ UI. To enable parental control feature, tap on the **Parental Control** button.



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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。



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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。


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 Serve

- 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
----------------	-----------------

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

<div>1</div> <div>Network configuration</div>	<div><div>1. Pick up phone and press “****” to start IVR</div><div>2. Choose “1”.</div><div>3. Prompt "Please enter password", user needs to input password and press “#” key, if user wants to configure Network.</div><div>4. The different options are described below.</div><div>The unit reports “Operation Successful” if the changes are successful. The cnPilot Home Router returns to the prompt “please enter your option ...”</div><div>5. To quit, enter “*”</div></div>
---	--

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

1 Network configuration	1. WAN Port Connection Type	<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 “*”.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 <p>Report “operation successful” if user operation is ok.</p> <ol style="list-style-type: none"> 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. <p>Report “operation successful” if user operation is ok.</p> <ol style="list-style-type: none"> 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. <p>Report “operation successful” if user operation is ok.</p> <ol style="list-style-type: none"> 6. If you want to quit, press “**”.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

<p>2</p> <p>Phone Port Configuration</p>	<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 “*”
<p>3</p> <p>Factory Reset</p>	<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 “*”. <p>Prompt “operation successful” if password is right and then cnPilot Home Router will be in factory default configuration.</p> <ol style="list-style-type: none"> 5. Press “7” reboot to make changes effective.
<p>4</p> <p>Reboot</p>	<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.
<p>5</p> <p>WAN Port Login</p>	<ol style="list-style-type: none"> 1. Pick up phone and press “****” to start IVR 2. Choose “5”, and 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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

- 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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

Sync with host

NTP Settings

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

Primary NTP Server

pool.ntp.org

Secondary NTP Server

cn.pool.ntp.org

NTP synchronization(1 - 1440m)

60

Daylight Saving Time

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 <div>Sync with host</div> 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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 .

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorageAdministration

WANLANVPNPort ForwardDMZDDNSQoSMAC ClonePort SettingRoutingAdvance

INTERNET

WAN

Connect Name1_TR069_VOICE_INTERNET_R_VID_

Delete Connect

ServiceTR069_VOICE_INTERNET

IP Protocol VersionIPv4

WAN IP ModeStatic

NAT EnableEnable

VLAN ModeDisable

VLAN ID1(1-4094)

Static

IP Address192.34.30.69

Subnet Mask255.255.255.248

Default Gateway192.34.30.65

DNS ModeManual

Primary DNS Address66.185.0.68

Secondary DNS Address

Port Bind

☒ Port_1

☒ Port_2

☒ Port_3

☒ Port_4

☒ Wireless(SSID1)

☒ Wireless(SSID2)

☒ Wireless(SSID3)

☒ Wireless(SSID4)

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

Help

WAN IP Mode:

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


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

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

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

VLAN ID	<div>Note Multiple WAN connections may be created with the same VLAN ID</div>
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 Mangement 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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

For example:

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

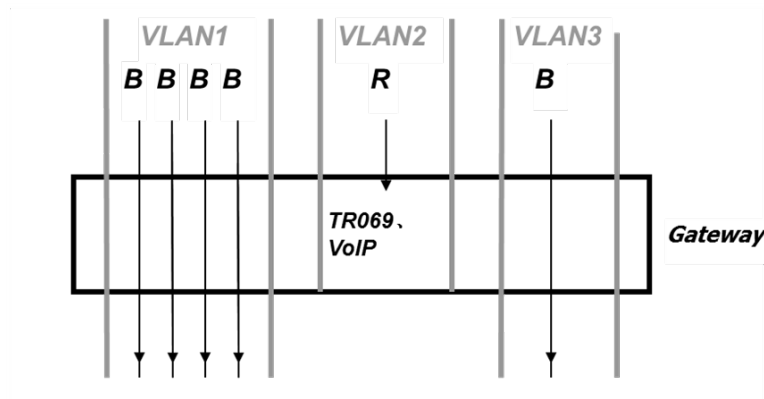
2_INTERNET_B_VID (Second Interface, Service is INTERNET, Bridge Mode, VLAN is disabled)

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 4 Multi VLAN

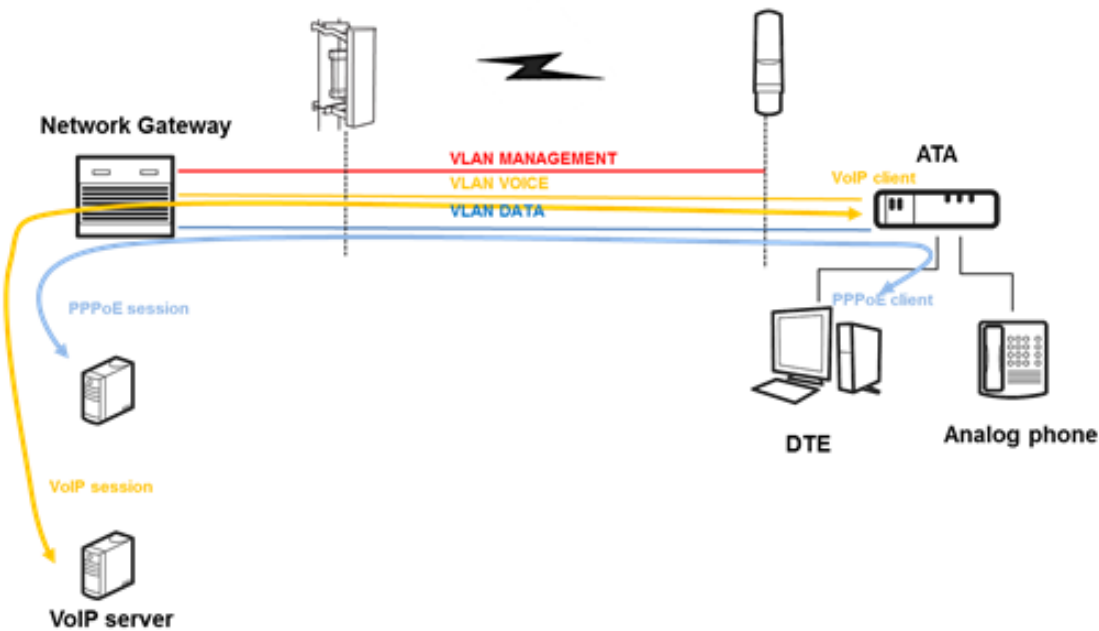


There are several advanced functions available when using Multi WAN setting:

- 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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Figure 5 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	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	

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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	1_MANAGEMENT_VOICE_INTERNET_B_VID Delete Connect
Service	MANAGEMENT_VOICE_INTERNET
IP Protocol Version	IPv4
WAN IP Mode	DHCP
MAC Address Clone	Disable
NAT Enable	Enable
Overwrite NAT IP	
VLAN Mode	Disable
VLAN ID	1 (1-4094)
DNS Mode	Auto
Primary DNS	15.1.1.2
Secondary DNS	
DHCP	
DHCP Renew	Renew
DHCP Vendor(Option 60)	CAMBIUM-cnPilot R200I
Port Bind	
<input checked="" type="checkbox"/> Port_1	<input checked="" type="checkbox"/> Port_2
<input checked="" type="checkbox"/> Wireless(SSID)	<input checked="" type="checkbox"/> Wireless(SSID1)
<input checked="" type="checkbox"/> Port_3	<input checked="" type="checkbox"/> Port_4
<input checked="" type="checkbox"/> Wireless(SSID2)	<input checked="" type="checkbox"/> 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.	
<p><i>Static IP</i> - Set the IP Address, Subnet Mask and Default Gateway that you have gotten from you ISP provider.</p> <p><i>DHCP</i> - You will get an IP Address, Subnet Mask and Default Gateway from some DHCP Server.</p> <p><i>PPPoE</i> - Set the PPPoE Account and PPPoE Password that you have gotten from your ISP provider.</p>	

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

VLAN Mode

Disable ▾

VLAN ID

1 (1-4094)

DNS Mode

Auto ▾

Primary DNS

Secondary DNS

PPPoE

PPPoE Account

PPPoE Password

.....

Confirm Password

.....

Service Name

Leave empty to autodetect

Operation Mode

Keep Alive ▾

Keep Alive Redial Period(0-3600s)

5

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

If it is left empty, the service name is auto detected.	
Operation Mode	<p>Select the mode of operation, options are Keep Alive, On Demand and Manual:</p> <ul style="list-style-type: none"> When the mode is Keep Alive, the user sets the 'keep alive redial period' values range from 0 to 3600s, the default setting is 5 minutes; When the mode is On Demand, the user sets the 'on demand idle time' value in the range of 0-60 minutes, the default setting is 5 minutes; <div> <div>Operation Mode</div> <div>On Demand ▼</div> </div> <div> <div>On Demand Idle Time(0-60m)</div> <div>5</div> </div> <ul style="list-style-type: none"> When the mode is Manual, there are no additional settings to configure
Keep Alive Redial Period	Set the interval to send Keep Alive messaging

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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>  Note Multiple WAN connections may be created with the same VLAN ID </div>	
802.1p	Set the priority of VLAN, Options are 0~7.

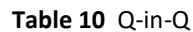
Q-in-Q

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 6 Q-in-Q Frame Format

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Page 45

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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:

WANLANIPv6 AdvancedIPv6 LANVPNPort ForwardDMZDDNSQoSPort SettingRoutingAdvance

PC Port(LAN)

PC Port(LAN)

Local IP Address192.168.11.1

Local Subnet Mask255.255.255.0

Local DHCP ServerEnable

DHCP Start Address192.168.11.2

DHCP End Address192.168.11.254

DNS ModeManual

Primary DNS192.168.11.1

Secondary DNS8.8.8.8

Client Lease Time(0-86400s)86400

DHCP Client List

DHCP Static Allotment

NO.

MAC

IP Address

Delete SelectedAddEdit

DNS ProxyEnable

Hardware NAT EnableDisable

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

1_MANAGEMENT_VOICE_INTERNET_R_VID

Delete Connect

Service

MANAGEMENT_VOICE_INTERNET

IP Protocol Version

IPv4

WAN IP Mode

DHCP

MAC Address Clone

Enable

MAC Address

Get Current PC MAC

NAT Enable

Enable

Overwrite NAT IP

VLAN Mode

Disable

VLAN ID

1

(1-4094)

DNS Mode

Auto

Primary DNS

172.16.5.200

Secondary DNS

DHCP

DHCP Renew

Renew

DHCP Vendor(Option 60)

Cambium-cnPilot R201P

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

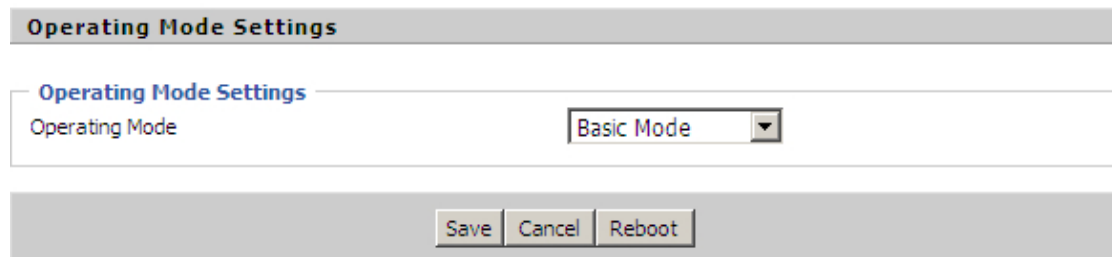
- Press the button **Get Current PC MAC** gets PC's MAC address
- Press the button **Save** to save your changes if users don't want to use MAC clone, press the button **Cancel** to cancel the changes
- Press the button **Reboot** to make the changes effective.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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**.

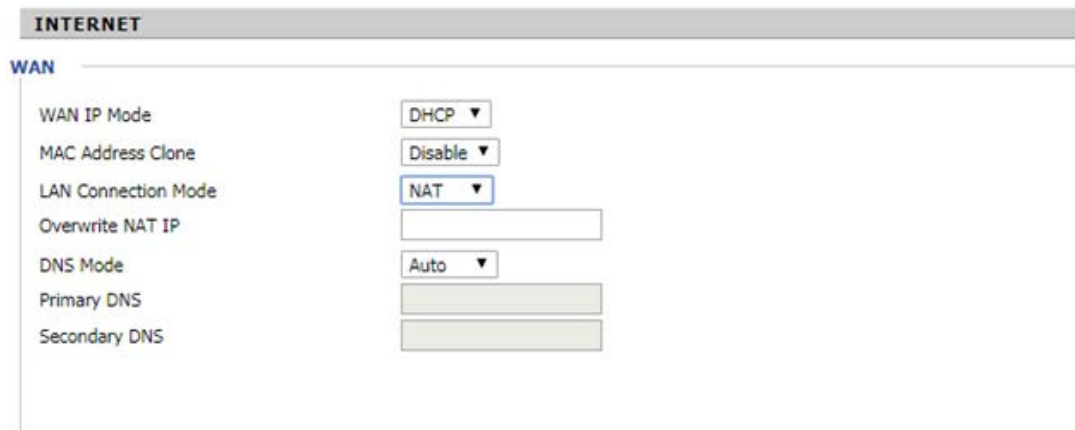


Operating Mode Settings

Operating Mode: Basic Mode

Save Cancel Reboot

- 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: DHCP

MAC Address Clone: Disable

LAN Connection Mode: NAT

Overwrite NAT IP:

DNS Mode: Auto

Primary DNS:

Secondary DNS:

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

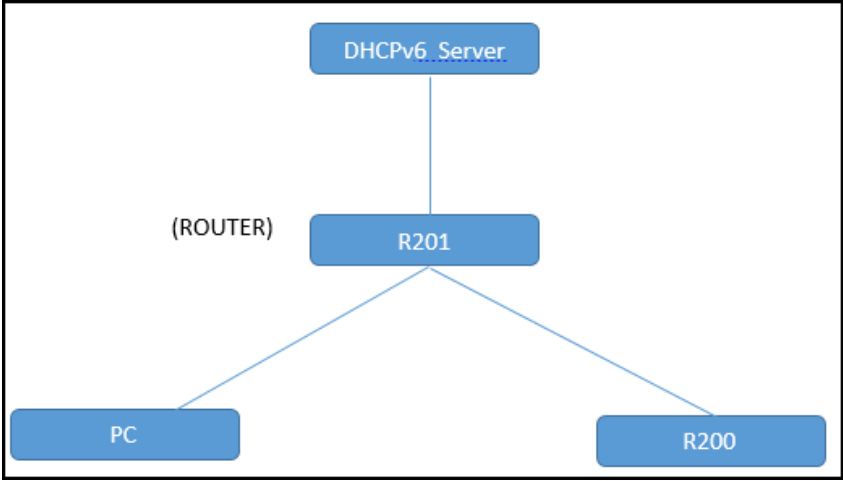
DHCPv6 protocol is used to automatically provision/configure IPv6 capable end points in a local network. In addition to acquiring an IPv6 IP address for the WAN interface and its associated LAN/WLAN clients, the cnPilot Home Router devices are also capable of prefix delegation.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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	<p>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.</p> <div><pre>graph TD; DHCPv6_Server[DHCPv6_Server] --- R201[R201]; R201 --- PC[PC]; R201 --- R200[R200];</pre></div>
Statefull	<p>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.</p>

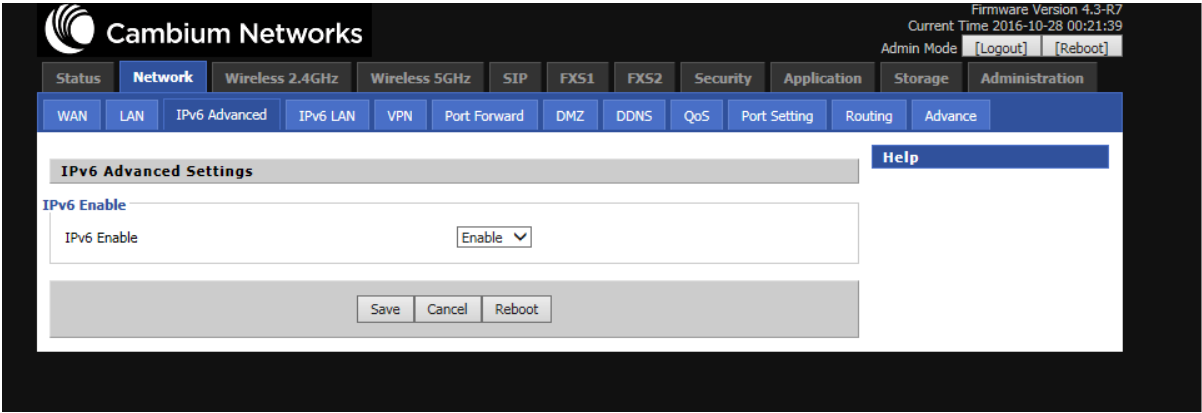
Enabling IPv6

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。



Configuring IPv6

Configuring Statefull IPv6

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

Table 14 Configuring Statefull IPv6

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Cambium Networks

Firmware Version 4.3-R7

Current Time 2016-10-28 00:20:03

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

INTERNET

WAN

Connect Name

1_MANAGEMENT_VOICE_INTERNET_R_VID

Delete Connect

Service

MANAGEMENT_VOICE_INTERNET

IP Protocol Version

IPv4 & IPv6

WAN IP Mode

DHCP

MAC Address Clone

Disable

NAT Enable

Enable

VLAN Mode

Disable

VLAN ID

1

(1-4094)

DNS Mode

Auto

Primary DNS

Secondary DNS

DHCP

DHCP Renew

Renew

DHCP Vendor(Option 60)

Cambium-cnPilot R201P

DHCPv6

DHCPv6 Address Settings

Statefull

Prefix Delegation

Enable

Port Bind

☒ Port_1

☒ Port_2

☒ Port_3

☒ Port_4

☒ Wireless(SSID)

☒ Wireless(SSID1)

☒ Wireless(SSID2)

☒ Wireless(SSID3)

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

Save

Cancel

Reboot

Help

WAN IP Mode:

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

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

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

Field Name	Description
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.

Page 52

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。
错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Configuring Stateless IPv6

Table 15 Configuring Stateless IPv6

The screenshot shows the Cambium Networks web interface. The top navigation bar includes tabs for Status, Network, Wireless 2.4GHz, Wireless 5GHz, SIP, FXS1, FXS2, Security, Application, Storage, and Administration. The Network tab is active, and the sub-tab is IPv6 Advanced. The main content area is titled 'INTERNET' and shows the 'WAN' configuration. The 'Connect Name' is '1_MANAGEMENT_VOICE_INTERNET_R_VID' and the 'Service' is 'MANAGEMENT_VOICE_INTERNET'. The 'IP Protocol Version' is set to 'IPv4 & IPv6'. The 'WAN IP Mode' is set to 'DHCP'. The 'NAT Enable' is set to 'Enable'. The 'VLAN Mode' is set to 'Disable' and the 'VLAN ID' is '1'. The 'DNS Mode' is set to 'Auto'. The 'DHCP' section shows 'DHCP Renew' as 'Renew' and 'DHCP Vendor (Option 60)' as 'Cambium-cnPilot R201P'. The 'DHCPv6' section is highlighted with a red box, showing 'DHCPv6 Address Settings' set to 'Stateless' and 'Prefix Delegation' set to 'Enable'. The 'Port Bind' section shows checkboxes for Port_1, Port_2, Port_3, and Port_4, all of which are checked. The 'Wireless (SSID)' section shows checkboxes for Wireless (SSID1), Wireless (SSID2), and Wireless (SSID3), all of which are checked. A note at the bottom states: '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 !'. The bottom of the interface has 'Save', 'Cancel', and 'Reboot' buttons.

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Viewing WAN port status

To view the status of WAN port:

1. Navigate to **Status** page.

FXS Port Status

FXS Port Status

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

Network Status

Internet Port Status

Connection Type	DHCP
IP Address	<div>Renew</div>
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

1 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:

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

The screenshot shows the Cambium Networks web interface. At the top, the logo and name 'Cambium Networks' are on the left, and 'Firmware Version 4.3-R7' and 'Current Time 2016-10-27 08:21:11' are on the right. Below this is a navigation bar with tabs: Status, Network (selected), Wireless 2.4GHz, Wireless 5GHz, SIP, FXS1, FXS2, Security, Application, Storage, and Administration. Under the Network tab, there are sub-tabs: WAN, LAN (selected), IPv6 Advanced, IPv6 LAN (selected), VPN, Port Forward, DMZ, DDNS, QoS, Port Setting, Routing, and Advance. The main content area is titled 'IPv6 LAN Setting' and contains a 'Help' button. The settings are as follows:

Setting	Value	Range/Options
IPv6 Address	FD00::1	
IPv6 Prefix Length	64	(0-128)
DHCPv6 Server		
DHCPv6 Status	Enable	Enable / Disable
DHCPv6 Mode	Statefull	Statefull / Stateless
Domain Name	cambiumnetworks.com	
Server Preference	255	(0-255)
Primary DNS Server	FD00::2	
Secondary DNS Server	FD00::3	
Lease Time	86400	(0-86400sec)
IPv6 Address Pool	FD00::100 - FD00::200 / 64	
Router Advertisement	Enable	Enable / Disable
Advertise Interval	30	(10-1800sec)
RA Managed Flag	Enable	Enable / Disable
RA Other Flag	Disable	Enable / Disable
Prefix		
Prefix Lifetime	3600	(0-3600sec)

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

LAN

LAN Port

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

192.168.11.1

Local Subnet Mask

255.255.255.0

Local DHCP Server

Enable

DHCP Start Address

192.168.11.2

DHCP End Address

192.168.11.254

DNS Mode

Manual

Primary DNS

192.168.11.1

Secondary DNS

8.8.8.8

Client Lease Time(0-86400s)

86400

DHCP Client List

DHCP Static Allotment

NO.	MAC	IP Address
1		
2		
3		

DNS Proxy

Enable

Save

Cancel

Reboot

Field Name	Description
IP Address	Enter the IP address of the router on the local area network. All the IP addresses of the computers which are in the router’s LAN must be in the same network segment with this address, and the default gateway of the computers must be this IP address. (The default is 192.168.11.1).
Local Subnet Mask	Enter the subnet mask to determine the size of the network (default is 255.255.255.0/24).
Local DHCP Server	Enable/Disable Local DHCP Server.
DHCP Start Address	Enter a valid IP address as a starting IP address of the DHCP server, and if the router’s LAN IP address is 192.168.11.1, starting IP address can be 192.168.11.2 or greater, but should be less than the ending IP address.
DHCP End Address	Enter a valid IP address as an end IP address of the DHCP pool.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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	192.168.11.1
Local Subnet Mask	255.255.255.0
Local DHCP Server	Enable ▼
DHCP Start Address	192.168.11.2
DHCP End Address	192.168.11.254
DNS Mode	Auto ▼

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Table 18 DHCP server, DNS and Client Lease Time

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

Field Name	Description
Primary DNS	Specify the Primary DNS address provided by your ISP. If your ISP does not provide it, the router will automatically apply default DNS Server IP address: 202.96.134.33 to this field.
Secondary DNS	Specify the Secondary DNS address provided by your ISP. If your ISP does not provide this address, the router will automatically apply default Secondary DNS Server IP of 202.96.128.86 to this field. If both the Primary IP and Secondary IP Address fields are left empty, the router will assign its own IP address to local users as a DNS proxy server and maintain a DNS cache.
Client Lease Time	It allows you to set the leased time for the specified PC.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

VPN

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

Table 19 VPN

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorageAdministration

WANLANIPv6 AdvancedIPv6 LANVPNPort ForwardDMZDDNSQoSPort SettingRoutingAdvance

VPN Settings

Administration

VPN Enable

L2TP

Initial Service IP

User Name

Password

L2TP Tunnel Name

L2TP Tunnel Password

VPN As Default Route

Disable

Save

Cancel

Reboot

Help

VPN Settings:

PPTP/L2TP - The Initial Service IP is the IP Address of a server that provides PPTP/L2TP services.

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

Save

Cancel

Reboot

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
-----	---------	------------	------------	----------

Delete Selected

Add

Edit

Port Forwarding

Comment

IP Address

Port Range

Protocol

TCP&UDP

Apply

Cancel

Virtual Servers

No.	Comment	IP Address	Public Port	Private Port	Protocol
-----	---------	------------	-------------	--------------	----------

Delete Selected

Add

Edit

Virtual Servers

Comment

IP Address

Public Port

Private Port

Protocol

TCP&UDP

Apply

Cancel

Page 61

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorageAd

WANLANVPNPort ForwardDMZDDNSQoSMAC ClonePort SettingRoutingA

DDNS Setting

DDNS Setting

Dynamic DNS Provider

None

Account

Password

DDNS URL

Status

DDNS updated Fail!

Field Name	Description
Dynamic DNS Provider	DDNS is enabled and select a DDNS service provider.
Account	Enter the DDNS service account.
Password	Enter the DDNS service account password.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

DDNS	Enter the DDNS domain name or IP address.
Status	See if DDNS is successfully upgraded.

Advance

Table 23 Advance

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorageWANLANMAC CloneVPNDMZPort ForwardAdvancePort SettingQoSRoute

Most Nat connections(512-8192)

4096

Mss Mode

Manual

Auto

Mss Value(1260-1460)

1260

AntiDos-P

Enable

Disable

IP conflict detection

Enable

Disable

IP Conflict Detecting Interval(0-3600)

0

Save

Cancel

Reboot

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Port Setting

Table 24 Port setting

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorageWANLANMAC CloneVPNDMZPort ForwardAdvancePort SettingQoSRouting

Port Setting

Port Setting

WANPort Speed NegoAuto

LAN1Port Speed NegoAuto

LAN2Port Speed NegoAuto

LAN3Port Speed NegoAuto

LAN4Port Speed NegoAuto

SaveCancelReboot

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

QoS

Table 25 QoS

WANLANVPNPort ForwardDMZQoSMAC ClonePort SettingRoutingAdvance

QoS setting

oS setting

QoS Enable

Disable

Upstream

(0-102400)kbit/s

Downstream

(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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Routing

Table 26 Routing

Static Routing Settings

Add a routing rule

Destination

1.1.1.1

Host/Net

Net

Sub Netmask

Gateway

Interface

LAN

Comment

Apply


Reset

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

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorageAdministration

BasicWireless SecurityWMMWDSWPSStation InfoAdvanced

Basic Wireless SettingsHelp

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

Isolated

Max Client

16

Multiple SSID1

Hidden

Isolated

Max Client

16

Multiple SSID2

Hidden

Isolated

Max Client

16

Multiple SSID3

Hidden

Isolated

Max Client

16

broadcast(SSID)

Enable

Disable

AP Isolation

Enable

Disable

MBSSID AP Isolation

Enable

Disable

BSSID

00:04:56:03:47:38

Frequency (Channel)

Auto

HT Physical Mode

Operating Mode

Mixed Mode

Green Field

Guard Interval

Long

Short

Reverse Direction Grant(RDG)

Disable

Enable

STBC

Disable

Enable

Aggregation MSDU(A-MSDU)

Disable

Enable

Auto Block ACK

Disable

Enable

Decline BA Request

Disable

Enable

HT Disallow TKIP

Disable

Enable

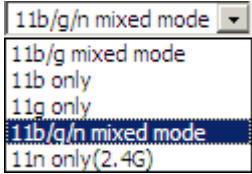
HT LDPC

Disable

Enable

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 R195P 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
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) Disabled: Devices on the WLAN must make a request for transmit when communicating with another device on the network

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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>

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Wireless Security

Table 28 Wireless security

StatusNetworkWirelessSTPFXS1FXS2SecurityApplicationStorageAd

BasicWireless SecurityWMMWDSWPSStation InfoAdvanced

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

SaveCancelReboot

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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	
<div>Select SSID<div>SSID choice<div>CAMBIUM_2.4GHz_027898</div>"CAMBIUM_2.4GHz_027898"Security Mode<div>WPA2-PSK</div>WPA<div>WPA Algorithms<div><div>TKIP</div><div><div>AES</div></div><div>TKIPAES</div></div>Pass Phrase<div>*****</div>Key Renewal Interval<div>3600</div>sec (0 ~ 4194303)</div></div></div>	
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:

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Table 31 WPAPSKWPA2PSK

WIFI Security Setting	
<div> <div>Select SSID</div> <div> <div>SSID choice</div> <div>Wireless_AP001118</div> </div> <div>"Wireless_AP001118"</div> <div> <div>Security Mode</div> <div>WPAPSKWPA2PSK</div> </div> <div>WPA</div> <div> <div>WPA Algorithms</div> <div> <div><input type="radio"/> TKIP</div> <div><input checked="" type="radio"/> AES</div> <div><input type="radio"/> TKIPAES</div> </div> </div> <div> <div>Pass Phrase</div> <div>23123123</div> </div> <div> <div>Key Renewal Interval</div> <div>3600</div> <div>Second in Month (0 ~ 4194303)</div> </div> </div>	
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
<p>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.</p>	

Wireless Access Policy:

Table 32 Wireless Access Policy

Access policy	<div> <div>Policy</div> <div> <div>Allow</div> <div>Disable</div> <div>Allow</div> <div>Reject</div> </div> </div>
Add a station MAC	<div> <div>Save</div> <div>Cancel</div> <div>Reboot</div> </div>

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.	

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

WMM

Table 33 WMM

StatusNetworkWireless 2.4GHzWireless 5GHzSIPFXS1FXS2SecurityApplication

BasicWireless SecurityWMMWDSWPSStation InfoAdvanced

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"/>

ApplyCancel

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

WDS

Table 34 WDS

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorage

BasicWireless SecurityWMMWDSWPSStation InfoAdvanced

WDS Setting

WDS Config

WDS Mode

Disable

SaveCancelReboot

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorageAdministration

BasicWireless SecurityWMMWDSWPSStation InfoAdvanced

WDS Setting

Help

WDS Config

WDS Mode

Lazy Mode

Phy Mode

CCK

EncrypType

NONE

Encryp Key

EncrypType

NONE

Encryp Key

EncrypType

NONE

Encryp Key

EncrypType

NONE

Encryp Key

SaveCancelReboot

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 Enable ▾ Apply								
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 Generate Reset OOB								
WPS Progress								
WPS Mode PIN PBC PIN Apply								
WPS Status								
WSC:Idle Cancel								
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 R195P Routers use a default security policy to allow other non-WPS users to access and apply.							

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

WPS Mode	<ul style="list-style-type: none">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 R195P 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	<p>WPS shows status in three ways:</p> <ul style="list-style-type: none">WSC: IdleWSC: 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	Adm
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.									

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

WDS

See [WDS](#).

WPS

See [WPS](#).

Station Info

See [Station Info](#).

Advanced

See [Advanced](#).

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 37 SIP settings

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorage

SIP SettingsVoIP QoS

SIP Parameters

SIP Parameters

SIP T1500MSMax Forward70

SIP Reg User Agent NameMax Auth2

Reg Retry Intvl30secReg Retry Long Intvl1200sec

Mark All AVT PacketsEnableSRTPDisable

Service TypeCommonSRTPTyping EncryptionAES_CM

Response Status Code Handling

Retry Reg RSC

NAT Traversal

NAT Traversal

NAT TraversalDisableNAT Refresh Interval(sec)60

STUN Server AddressSTUN Server Port3478

SaveCancelReboot

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Dial Plan

Parameters and Settings

Table 38 Parameters and settings

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorage

SIP AccountPreferencesDial PlanBlacklistCall Log

Dial Plan

General

Dial PlanDisable

Unmatched Policy

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

FXS

FXS 1

Digit Map

Action

Deny

OKCancel

SaveCancelReboot

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Blacklist

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

Table 39 Blacklist

Blacklist Upload && Download

Blacklist Upload && Download

Local File

Choose File

No file chosen

Upload CSV

Download CSV

Blacklist

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

Edit

Add

Delete

Move to phonebook

Description

Click

浏览...

 to select the blacklist file and click

upload CSV

 to upload it to cnPilot Home Router; Click

download CSV

 to save the blacklist file to your local computer.

Select one contact and click edit to change the information, click delete to delete the contact, click Move to phonebook to move the contact to phonebook.

Click Add to add one blacklist, enter the name and phone number, click OK to confirm and click cancel to cancel.

Name

Number

OK

Cancel

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Call Log

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

Table 40 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"/>	
11	123	10/29 15:07	00:00:01	<input type="checkbox"/>	

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"/>	
11	sipp	10/25 16:17	00:00:00	<input type="checkbox"/>	

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Missed Calls				
Index	NUMBER	Start Time	Duration	
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 41 VoIP QoS

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage
SIP Settings		VoIP QoS						
QoS Settings								
Layer 3 QoS								
SIP QoS(0-63)		<input type="text" value="46"/>						
RTP QoS(0-63)		<input type="text" value="46"/>						
<div>SaveCancelReboot</div>								

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 42 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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 43 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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 44 Supplementary service

Supplementary Service Subscription	
<div><div>Supplementary Services</div><div><div>Call Waiting</div><div>Enable ▾</div></div><div><div>MWI Enable</div><div>Enable ▾</div></div><div><div>MWI Subscribe Enable</div><div>Disable ▾</div></div><div><div>DND</div><div>Disable ▾</div></div><div><div>Hot Line</div><div></div></div><div><div>Voice Mailbox Numbers</div><div></div></div><div><div>VMWI Serv</div><div>Enable ▾</div></div></div>	
<div><div>Speed Dial</div><div><div>Speed Dial 2</div><div></div></div><div><div>Speed Dial 4</div><div></div></div><div><div>Speed Dial 6</div><div></div></div><div><div>Speed Dial 8</div><div></div></div><div><div>Speed Dial 3</div><div></div></div><div><div>Speed Dial 5</div><div></div></div><div><div>Speed Dial 7</div><div></div></div><div><div>Speed Dial 9</div><div></div></div></div>	
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).

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

	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 45 Advanced

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

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 46 Volume settings

Preferences	
Volume Settings	
Handset Input Gain	Handset Volume

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Regional

Table 47 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)

20

Max Jitter Delay(20-1000ms)

160

Ringing Time(10-300sec)

60

Ring Waveform

Sinusoid

Ring Voltage(40-63 Vrms)

45

Ring Frequency(15-30Hz)

20

VMWI Ring Splash Len(0.1-10sec)

0.5

Flash Time Max(0.2-1sec)

0.9

Flash Time Min(0.1-0.5sec)

0.1

Field Name	Description																
Tone Type	Choose tone type as UK, China, US, Hong Kong and so on. A sample Tone Type for UK is shown below: <table><tr><th>COUNTRY/PARAMETER</th><th>VALUE</th></tr><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 Maching</td><td>370+620 310nF</td></tr><tr><td>Ring Voltage</td><td>55Vrms</td></tr></table>	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 Maching	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 Maching	370+620 310nF																
Ring Voltage	55Vrms																
Dial Tone	Dial Tone																
Busy Tone	Busy Tone																
Off Hook Warning Tone	Off Hook warning tone																

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 R195P 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 48 Features and call forward

Features

All Forward

Disable ▾

Busy Forward

Disable ▾

No Answer Forward

Disable ▾

Call Forward

All Forward

Busy Forward

No Answer Forward

No Answer Timeout

20

Feature Code

Hold Key Code

*77

Transfer Key Code

*98

R Key Enable

Disable ▾

R Key Hold Code

R2 ▾

R Key Conference Code

R3 ▾

Conference Key Code

*88

IVR Key Code

R Key Cancel Code

R1 ▾

R Key Transfer Code

R4 ▾

Speed Dial Code

*74

Field	Description
-------	-------------

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Name		
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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Miscellaneous

Table 49 Miscellaneous

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

FXS2

The settings of FXS2 are the same as FXS1. See [FXS1](#) on page 86.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Security

Filtering Setting

Table 50 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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Delete	Delete selected item
--------	----------------------

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Content Filtering

Table 51 Content filtering

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Basic Settings

Basic Settings

Filtering

Disable

Default Policy

Drop

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

Save

Cancel

IP/Port Filter Settings

Interface

LAN

Mac address

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)

Save

Cancel

Field Name	Description
Filtering	Enable/Disable content Filtering

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 52 UPnP

UPnP

UPnP Setting

UPnP enable

Enable

Save

Cancel

Reboot

Field Name	Description
UPnP enable	Enable/Disable UPnP function.

IGMP

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

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

Table 53 IGMP

IGMP

IGMP Setting

IGMP Proxy enable

Disable

Save

Cancel

Reboot

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Storage

Disk Management

This page is used to manage the USB storage device.

Table 54 Disk Management

Status

Network

Wireless

SIP

FXS1

FXS2

Security

Application

Storage

Disk Management

Ftp Setting

Smb Setting

Disk Management

Folder List

Directory Path

Partition

AddDeleteRemoveDisk

Partition Status

Partition

Path

FormatRe-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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

FTP Setting

Table 55 FTP Setting

Status	Network	Wireless	SIP	FXS1	FXS2	Security	Application	Storage
Disk Management	Ftp Setting	Smb Setting						
FTP Setting								
FTP Server Setup								
FTP Server								
FTP Server Name								
Anonymous Login								
FTP Port								
Max. Sessions								
Create Directory								
Rename File/Directory								
Remove File/Directory								
Read File								
Write File								
Download Capability								
Upload Capability								

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Smb Setting

Table 56 Smb setting

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorage

Disk ManagementFtp SettingSmb Setting

SMB Setting

SAMBA Server Setup

SAMBA Server

Enable

Disable

Workgroup

Workgroup

NetBIOS Name

FileShare

Sharing Directory List

Directory Name

Directory Path

Allowes Users

Add

Edit

Delete

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 57 Save Config File

Save Config File	
<div>Config File Upload && Download</div> <div><div>Local File</div><div><div>Choose File</div><div>No file chosen</div><div>Upload</div><div>Download</div></div></div>	
Field Name	Description
Config file upload and download	Upload: click on browse, select file in the local, press the upload button to begin uploading files
	Download: click to download, and then select contains the path to download the configuration file

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Administrator settings

Table 58 Administrator settings

Administrator Settings	
Password Reset	
User Type	Admin User ▼
New User Name	admin
New Password	<input type="password"/>
Confirm Password	<input type="password"/> (The maximum length is 25)
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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Time/Date Setting

NTP Settings

NTP Enable

Enable

Option 42

Disable

Current Time

2017 - 06 - 09 . 11 : 04 : 33

Sync with host

Sync with host

Time Zone

(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

System Log Setting

Syslog Setting

Syslog Enable

Enable

Syslog Level

INFO

Login Syslog Enable

Enable

Call Syslog Enable

Enable

Net Syslog Enable

Enable

Device Management Syslog Enable

Enable

Device Alarm Syslog Enable

Enable

Kernel Syslog Enable

Enable

Remote Syslog Enable

Disable

Remote Syslog Server

Factory Defaults Setting

Factory Defaults Setting

Factory Defaults Lock

Disable

Factory Defaults

Reset to Factory Defaults

Factory Default

Save Cancel Reboot

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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.

SNMP Configuration

SNMP Configuration

SNMP Service: Enable

Remote SNMP login: Disable

Trap Server Address: Disable

Read Community Name: public

Write Community Name: private

Trap Community: trap

Trap period interval(sec): 300

Save Cancel Reboot

Help

SNMP Configuration:

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

NTP settings

Table 59 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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Daylight Saving Time

Table 60 Daylight Saving Time

Daylight Saving Time

Daylight Saving Time

Enable

Offset

60

Min.

Start Month

April

Start Day of Week

Sunday

Start Day of Week Last in Month

First in Month

Start Hour of Day

2

Stop Month

October

Stop Day of Week

Sunday

Stop Day of Week Last in Month

Last in Month

Stop Hour of Day

2

Procedure
Step 1. Enable Daylight Savings Time.
Step 2. Set value of offset for Daylight Savings Time
Step 3: Set starting Month/Week/Day/Hour in Start Month/Start Day of Week Last in Month/Start Day of Week/Start Hour of Day, analogously set stopping Month/Week/Day/Hour in Stop Month/Stop Day of Week Last in Month/Stop Day of Week/Stop Hour of Day.
Step 4. Press Saving button to save and press Reboot button to active changes.

System Log Setting

Table 61 System log Setting

System Log Setting

Syslog Setting

Syslog Enable

Enable

Syslog Level

INFO

Remote Syslog Enable

Disable

Remote Syslog Server

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

	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 62 Factory Defaults Setting

<div>Factory Defaults Setting</div> <div>Factory Defaults Setting</div> <div>Factory Defaults Lock<div>Disable</div></div>	
Description	With this lock enabled, user cannot factory reset the box using the hardware switch.

Factory Defaults

Table 63 Factory Defaults

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Firmware Upgrade

Table 64 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 Upgrade Software ▾								
Local Upgrade Choose File No file chosen								
Upgrade								
Description								
1. Choose upgrade file type from Image File and Dial Rule								
2. Press “Browse” button to browse the file								
3. Press Upgrade 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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Table 65 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 R195P 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 R195P Router is busy now, in this case, cnPilot R195P Router will wait for a period time, the longest is “Forced Resync Delay”, default is 14400s, when the time over, cnPilot R195P 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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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 66 Firmware Upgrade

Firmware Upgrade

Upgrade Enable

Enable

Upgrade Error Retry Delay(sec)

3600

Upgrade Rule

Field Name	Description
Upgrade Enable	Enable firmware upgrade via provision or not.
Upgrade Error Retry Delay(sec)	If the last upgrade fails, cnPilot R195P Routers will try upgrading again after “Upgrade Error Retry Delay” period, default is 3600s.
Upgrade Rule	URL of upgrade file

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

SNMP

Table 67 SNMP

ManagementFirmware UpgradeCertificationProvisionSNMPTR069Cambium Network Ma

Operating Mode

SNMP Configuration

SNMP Configuration

SNMP ServiceEnable

Trap Server Address

Read Community Namepublic

Write Community Nameprivate

Trap Communitytrap

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 68 TR069

ManagementFirmware UpgradeCertificationProvisionSNMPTR069Cambium Network Management

Operating Mode

TR069 Configuration

ACS

TR069 Enable

Disable ▾

CWMP

Enable ▾

ACS URL

User Name

000456-C3VoIP-200P-400FQU001GLX

Password

.....

Periodic Inform Enable

Enable ▾

Periodic Inform Interval

30

Connect Request

User Name

Password

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。
错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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", },
```

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

```
{ "UI": {
  "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": { },
      "": { },
```

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

```
{ "", },
{ "", },
{"WLANConfiguration", },
{"1", },
    {"Enable", },
    {"Status", },
    {"BSSID", },
    {"MaxBitRate", },
    {"Channel", },
    {"AutoChannelEnable", },
    {"SSID", },
    {"BeaconType", },
    {"MACAddressControlEnabled", },
    {"Standard", },
    {"WEPKeyIndex", },
    {"KeyPassphrase", },
    {"WEPEncryptionLevel", },
    {"BasicEncryptionModes", },
    {"BasicAuthenticationMode", },
    {"WPAEncryptionModes", },
    {"WPAAuthenticationMode", },
    {"IEEE11iEncryptionModes", },
    {"IEEE11iAuthenticationMode", },
    {"PossibleChannels", },
    {"ChannelsInUse", },
    {"BasicDataTransmitRates", },
    {"OperationalDataTransmitRates", },
    {"PossibleDataTransmitRates", },
    {"RadioEnabled", },
    {"AutoRateFallbackEnabled", },
    {"TotalBytesSent", },
    {"TotalBytesReceived", },
    {"TotalPacketsSent", },
    {"TotalPacketsReceived", },
    {"TotalAssociations", },
    {"AssociatedDevice", },
    {"1", },
```

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

```
        {"AssociatedDeviceMACAddress", },
        {"AssociatedDeviceIPAddress", },
        {"AssociatedDeviceAuthenticationState", },
        {"X_AssociatedDeviceSignalStrength", },
        {"", },
    {"", },
    {"WEPKey", },
        {"1", },
            {"WEPKey", },
        {"", },
    {"", },

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

    {"Hosts", },
        {"HostNumberOfEntries", },
        {"Host", },
            {"1", },
                {"IPAddress", },
                {"AddressSource", },
                {"LeaseTimeRemaining", },
                {"MACAddress", },
                {"HostName", },
                {"InterfaceType", },
                {"Active", },
            {"", },
        {"", },
    {"", },
    {"", },
    {"", },

    {"WANDevice", },
        {"1", },
            {"WANConnectionNumberOfEntries", },
            {"WANCommonInterfaceConfig", },
```

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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


错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

```
        {"1", },
        {"PortMappingEnabled", },
        {"PortMappingLeaseDuration", },
        {"RemoteHost", },
        {"ExternalPort", },
        {"InternalPort", },
        {"PortMappingProtocol", },
        {"InternalClient", },
        {"PortMappingDescription", },
        {"", },
{"", },
{"Stats", },
    {"EthernetBytesSent", },
    {"EthernetBytesReceived", },
    {"EthernetPacketsSent", },
    {"EthernetPacketsReceived", },
    {"", },
{"", },
{"WANPPPOConnection", },
    {"1", },
        {"Enable", },
        {"ConnectionStatus", },
        {"PossibleConnectionTypes", },
        {"ConnectionType", },
        {"Name", },
        {"Uptime", },
        {"LastConnectionError", },
        {"RSIPAvailable", },
        {"NATEnabled", },
        {"Username", },
        {"Password", },
        {"ExternalIPAddress", },
        {"DNSEnabled", },
        {"DNSOverrideAllowed", },
        {"DNSServers", },
        {"MACAddress", },
```

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

```
{ "TransportType", },
{ "PPPoEACName", },
{ "PPPoEServiceName", },
{ "ConnectionTrigger", },
{ "RouteProtocolRx", },
{ "PortMappingNumberOfEntries", },
{ "PortMapping", },
    { "1", },
        { "PortMappingEnabled", },
        { "PortMappingLeaseDuration", },
        { "RemoteHost", },
        { "ExternalPort", },
        { "InternalPort", },
        { "PortMappingProtocol", },
        { "InternalClient", },
        { "PortMappingDescription", },
    { "", },
{ "", },
{ "Stats", },
    { "EthernetBytesSent", },
    { "EthernetBytesReceived", },
    { "EthernetPacketsSent", },
    { "EthernetPacketsReceived", },
{ "", },
{ "", },
    { "", },
        { "", },
            { "", },
                { "", },
                    { "", },
                        { "", },
                            { "", },
                                /*TR104 for VOIP setting*/

{ "Services", },
    { "VoiceService", },
        { "1", },
            { "VoiceProfileNumberOfEntries", },
            { "Capabilities", },
```

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

```
{ "MaxProfileCount", },
{ "MaxLineCount", },
{ "MaxSessionsPerLine", },
{ "MaxSessionCount", },
{ "SignalingProtocols", },
{ "Regions", },
{ "RTCP", },
{ "SRTP", },
{ "RTPRedundancy", },
{ "DSCPCoupled", },
{ "EthernetTaggingCoupled", },
{ "PSTNSoftSwitchOver", },
{ "FaxT38", },
{ "FaxPassThrough", },
{ "ModemPassThrough", },
{ "ToneGeneration", },
{ "RingGeneration", },
{ "NumberingPlan", },
{ "ButtonMap", },
{ "VoicePortTests", },
{ "SIP", },
    { "Role", },
    { "Extensions", },
    { "Transports", },
    { "URISchemes", },
    { "EventSubscription", },
    { "ResponseMap", },
{ "", },
{ "Codecs", },
    { "1", },
        { "EntryID", },
        { "Codec", },
        { "BitRate", },
        { "PacketizationPeriod", },
        { "SilenceSuppression", },
    { "", },
{ "", },
```

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

[illegible]

Firmware Upgrade

Under is firmware upgrading operation on FreeACS.

1. Equipment connection configure

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

StatusNetworkSIP AccountPhoneAdministration

ManagementFirmware UpgradeCertificationProvisionSNMPTR069DiagnosisOperating Mode

Please REBOOT to make the changes effective!

TR069 Configuration

ACS

TR069 Enable

Enable

CWMP

Enable

ACS URL

http://182.92.234.149:8080/tr069

User Name

user_ip542n

Password

Periodic Inform Enable

Enable

Periodic Inform Interval

600

Connect Request

User Name

11

Password

..

Save

Cancel

Reboot

Help

TR069 Configuration:

Allow the device to be managed by the ACS server which is set in the ACS URL.

Scheduled Tasks

In this page, the user can set time to automatically turned ON or OFF the Wi-Fi, Reboot, or restart PPPoE at a moment.

Table 69 Scheduled Tasks

Scheduled Tasks

Scheduled Wifi

No.

Enable

SSID

Week Select

Open Time

Close Time

Delete Selected

Add

Edit

Scheduled Reboot

Scheduled Reboot

Disable

Scheduled Mode

EveryDay

Time

00

:

00

Scheduled PPPOE

Scheduled PPPOE

Disable

Scheduled Mode

EveryDay

Time

00

:

00

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。

错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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.

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Table 70 Diagnosis

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorageAdministration

ManagementFirmware UpgradeScheduled TasksCertificatesProvisionSNMPTR069cnMaestroDiagnosis

Operating Mode

Packet Trace

Help

Packet Trace

Tracking Interface

WAN

Packet Trace

startstopsave

Ping Test

Ping Test

Dest IP/Host Name

WAN Interface

1_MANAGEMENT_VOICE_INTERNET_R_VID_

ApplyCancel

Traceroute Test

Traceroute Test

Dest IP/Host Name

WAN Interface

1_MANAGEMENT_VOICE_INTERNET_R_VID_

ApplyCancel

Description
<div>1. Packet Trace</div> <div>Users can use the packet trace feature to intercept packets which traverse the device. Click the Start button</div>

Page 135

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

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

1_TR069_VOICE_INTERNET_R_VID_

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

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

Apply

Cancel

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

www.google.com

WAN Interface

1_MANAGEMENT_VOICE_INTERNET_R_VID_

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

Apply

Cancel

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。 错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Operating Mode

Table 71 Operating mode

Operating Mode Settings

Operating Mode Settings

Operating Mode

Basic Mode

Basic Mode

Advanced Mode

Save

Cancel

Reboot

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 72 System log

StatusNetworkWirelessSIPFXS1FXS2SecurityApplicationStorageAdministration

BasicLAN HostSyslog

RefreshClearSave

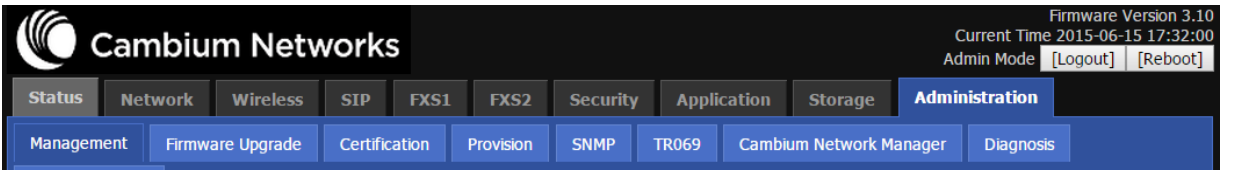
Manufacturer:CAMBIUM NETWORKS
ProductClass:C3VoIP-200P
SerialNumber:400FQU001GLX
BuildTime:201506180103
IP:192.168.11.1
HWVer:V1.3
SWVer:3.10-b1

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

错误!使用“开始”选项卡将 Heading 1 应用于要在此处显示的文字。错误!使用“开始”选项卡将 Heading 2 应用于要在此处显示的文字。

Logout


Table 73 Logout



Description

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

Reboot

Press the  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.
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 .

Term	Definition
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.
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 .

Term	Definition
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
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.

Term	Definition
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
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