COMTREND

VR-3053

Home Gateway

User Manual

261099-049

Version A1.0, June 14, 2019

Preface

This manual provides information related to the installation and operation of this device. The individual reading this manual is presumed to have a basic understanding of telecommunications terminology and concepts.

If you find the product to be inoperable or malfunctioning, please contact technical support for immediate service by email at INT-support@comtrend.com

For product update, new product release, manual revision, or software upgrades, please visit our website at http://www.comtrend.com

Important Safety Instructions

With reference to unpacking, installation, use, and maintenance of your electronic device, the following basic guidelines are recommended:

- Do not use or install this product near water, to avoid fire or shock hazard. For example, near a bathtub, kitchen sink or laundry tub, or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
- Do not connect the power supply cord on elevated surfaces. Allow it to lie freely. There should be no obstructions in its path and no heavy items should be placed on the cord. In addition, do not walk on, step on, or mistreat the cord.
- Use only the power cord and adapter that are shipped with this device.
- To safeguard the equipment against overheating, make sure that all openings in the unit that offer exposure to air are not blocked.
- Avoid using a telephone (other than a cordless type) during an electrical storm. There may be a remote risk of electric shock from lightening. Also, do not use the telephone to report a gas leak in the vicinity of the leak.
- Never install telephone wiring during stormy weather conditions.

CAUTION:

- To reduce the risk of fire, use only No. 26 AWG or larger telecommunication line cord.
- Always disconnect all telephone lines from the wall outlet before servicing or disassembling this equipment.
- Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user authority to operate the equipment.
- Do not stack equipment or place equipment in tight spaces, in drawers, or on carpets. Be sure that your equipment is surrounded by at least 2 inches of air space.
- If this Home Gateway Router cause harm to the telephone network, the telephone company will notify you in advance that temporary discontinuance of service may be required. But if advance notice isn't practical, the telephone company will notify the customer as soon as possible. Also you will be advised of your right to file a complaint with the FCC if you believe it is necessary.

- To prevent interference with cordless phones, ensure that gateway is at least 5 feet (1.5m)from the cordless phone base station.
- If you experience trouble with this equipment, you disconnect it from the network until the problem has been corrected or until you are sure that equipment is not malfunctioning.
- If your home has specially wired alarm equipment connected to the telephone line, ensure the installation of this equipment does not disable alarm equipment consult your telephone company or a qualified installer.

WARNING(ATTENTION)

- Disconnect the power line from the device before servicing.
- For indoor use only
- Do NOT open the casing
- Do NOT use near water
- Do NOT insert sharp objects into the RJ-11 jack
- Keep away from the fire
- For use in ventilated environment / space
- Use 26 AWG or larger cable connect to RJ-11 port

- Débranchez l'alimentation électrique avant l'entretien
- Cet appareil est conçu pour l'usage intérieur seulement
- N'ouvrez pas le boîtier
- N'utilisez pas cet appareil près de l'eau
- N'insérez pas d'objets tranchants dans la prise
- RJ-11N'approchez pas du feu
- Veuillez utiliser dans un environnement aéré
- Veuillez utiliser fil électrique de 26AWG pour port RJ-11

Power Specifications(Alimentation) :
Input 12Vdc, 2A

FCC & ISED

User Information

Any changes or modifications not expressly approved by the party responsible for compliance could void your authority to operate the equipment.

Aucune modification apportée à l'appareil par l'utilisateur, quelle qu'en soit la nature. Tout changement ou modification peuvent annuler le droit d'utilisation de l'appareil par l'utilisateur.

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.

This Class B digital apparatus complies with Canadian ICES-003.
To reduce potential radio interference to other users, the antenna type and its gain should be so chosen that the equivalent isotropically radiated power (e.i.r.p.) is not more than that permitted for successful communication.
This device complies with Part 15 of the FCC Rules and 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.

Cet appareil numérique de la classe B est conforme à la norme NMB-003 Canada.
Pour réduire le risque d'interférence aux autres utilisateurs, le type d'antenne et son gain doivent être choisies de façon que la puissance isotrope rayonnée équivalente (PIRE) ne dépasse pas ce qui est nécessaire pour une communication réussie.
Cet appareil est conforme à la norme RSS Industrie Canada exempts de licence norme(s).

Son fonctionnement est soumis aux deux conditions suivantes:
1. Cet appareil ne peut pas provoquer d'interférences et
2. Cet appareil doit accepter toute interférence, y compris les interférences qui peuvent causer un mauvais fonctionnement du dispositif.

Radiation Exposure

FCC

1. This Transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

2. This equipment complies with FCC RF radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with a minimum distance of 20 centimeters between the radiator and your body.

ISED

This device complies with the ISED radiation exposure limit set forth for an

uncontrolled environment. This device should be installed and operated with minimum distance 20cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

Cet équipement est conforme avec l'exposition aux radiations ISED définies pour un environnement non contrôlé. Cet équipement doit être installé et utilisé à une distance minimum de 20 cm entre le radiateur et votre corps. Cet émetteur ne doit pas être co-localisées ou opérant en conjonction avec une autre antenne ou transmetteur.

The Ringer Equivalence Number (REN) indicates the maximum number of devices allowed to be connected to a telephone interface. The termination of an interface may consist of any combination of devices subject only to the requirement that the sum of the RENs of all the devices not exceed five.

Copyright

Copyright©2019 Comtrend Corporation. All rights reserved. The information contained herein is proprietary to Comtrend Corporation. No part of this document may be translated, transcribed, reproduced, in any form, or by any means without prior written consent of Comtrend Corporation.

This program is free software: you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation, either version 3 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program. If not, see http://www.gnu.org/licenses/

NOTE:	This document is subject to change without notice.

Protect Our Environment

This symbol indicates that when the equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separate from domestic waste.

The cardboard box, the plastic contained in the packaging, and the parts that make up this router can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste; you may be subject to penalties or sanctions under the law. Instead, please be responsible and ask for disposal instructions from your local government.

Save Our Environment
When this equipment has reached the end of its useful life, it must be taken to a recycling centre and processed separately from domestic waste.
The cardboard box, the plastic in the packaging, and the parts that make up this device can be recycled in accordance with regionally established regulations. Never dispose of this electronic equipment along with your household waste.
You may be subject to penalties or sanctions under the law. Instead, ask for disposal instructions from your municipal government.
Please be responsible and protect our environment.

Table of Contents

CHAPTER 1 INTRODUCTION **8**

CHAPTER 2 INSTALLATION **9**
2.1 HARDWARE SETUP 9
2.1.1 Back Panel *10*
2.1.2 Bottom Panel *12*
2.1.3 Front Panel *13*

CHAPTER 3 WEB USER INTERFACE **15**
3.1 DEFAULT SETTINGS 15
3.2 IP CONFIGURATION 16
3.3 LOGIN PROCEDURE 18

CHAPTER 4 BASIC SETUP **20**
4.1 INTERNET 21
4.2 WIFI 2.4GHZ 23
4.3 WIFI 5GHZ 24
4.4 LAN 25
4.4.1 Configuration *25*
4.4.2 Devices Connected *26*
4.5 FIREWALL 27
4.5.1 Main Firewall *27*
4.5.2 Parental Control *28*

CHAPTER 5 ADVANCED SETUP **30**
5.1 DSL 31
5.1.1 Mode Setting *31*
5.1.2 Status *32*
5.1.3 ATM Channel *33*
5.2 MULTIPLE BRIDGE 34
5.2.1 LAN VLAN *34*
5.2.2 Bridges *34*
5.3 MULTICAST 35
5.4 SYSTEM 36
5.4.1 Administration *36*
5.4.2 User Management *37*
5.4.3 System Time *38*
5.4.4 System Log *39*
5.4.5 Diagnostics *40*
5.5 DYNAMIC DNS 42
5.6 WIFI 2.4GHZ 45
5.6.1 Advanced *45*
5.6.2 SSIDs *47*
5.6.3 WPS *49*
5.6.4 MAC Filtering *51*
5.6.5 WDS *52*
5.6.6 Statistics *53*
5.6.7 Airtime Fairness *55*
5.7 WIFI 5GHZ 58
5.7.1 Advanced *58*
5.7.2 SSIDs *60*
5.7.3 WPS *62*
5.7.4 MAC Flitering *64*
5.7.5 WDS *66*
5.7.6 Statistics *67*
5.7.7 Airtime Fairness *69*
5.8 UPNP 72
5.9 QUALITY OF SERVICE 73

5.9.1 QoS *74*
5.9.2 QoS Graphs *77*
5.9.3 Queue Stats *78*
5.10 ADVANCED FIREWALL 79
5.10.1 Packet Filter *79*
5.10.2 URL Filter *81*
5.11 OAM DIAGNOSTICS 82
5.11.1 ATM OAM F5 Loopback *82*
5.12 NAT 83
5.12.1 DMZ *83*
5.12.2 Port Mapping *84*
5.12.3 Port Triggering *86*
5.13 DEVICE MANAGEMENT 88
5.14 ROUTING 90
5.14.1 Static Routing *90*
5.14.2 RIP *94*

CHAPTER 6 LOGOUT 95

APPENDIX A – SPECIFICATIONS 96

APPENDIX B - SSH CLIENT 98

Chapter 1 Introduction

VR-3053 is a Multi-DSL router using the Intel solution. It not only provides both ADSL and 35b VDSL but also integrated 5 Giga Ethernet ports and WLAN 802.11n 2.4GHz frequency band and 802.11ac 5GHz Frequency band. Therefore, VR-3053 is designed for high speed applications. VR-3053 also follows TR-069 making central management (ACS) very easy.

Chapter 2 Installation

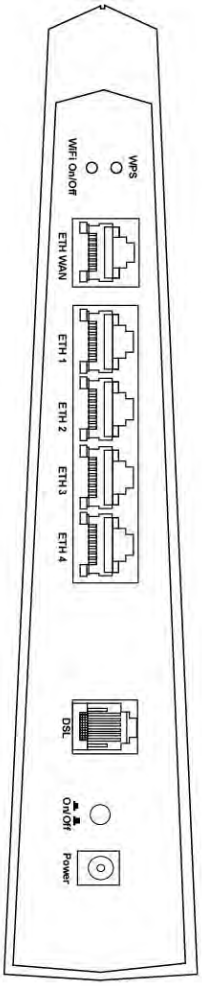
2.1 Hardware Setup

Non-stackable
This device is not stackable – do not place units on top of each other, otherwise damage could occur.

Follow the instructions below to complete the hardware setup.

2.1.1 Back Panel

The figure below shows the back panel of the device.



WiFi On/Off
Press and release the WiFi button to enable the WiFi function. To disable WiFi, press and release the WiFi button.

WPS Button
Press the WPS button less than 2 seconds to enable WPS which will allow 2 minutes for WiFi connection.

ETH WAN PORT
This port is designated to be used for Ethernet WAN functionality only. Use 1000-BASE-T RJ-45 cables to connect to Gigabit WAN server, or 10/100BASE-T RJ-45 cables for standard network usage. This ports is auto-sensing MDI/X; so either straight-through or crossover cable can be used.

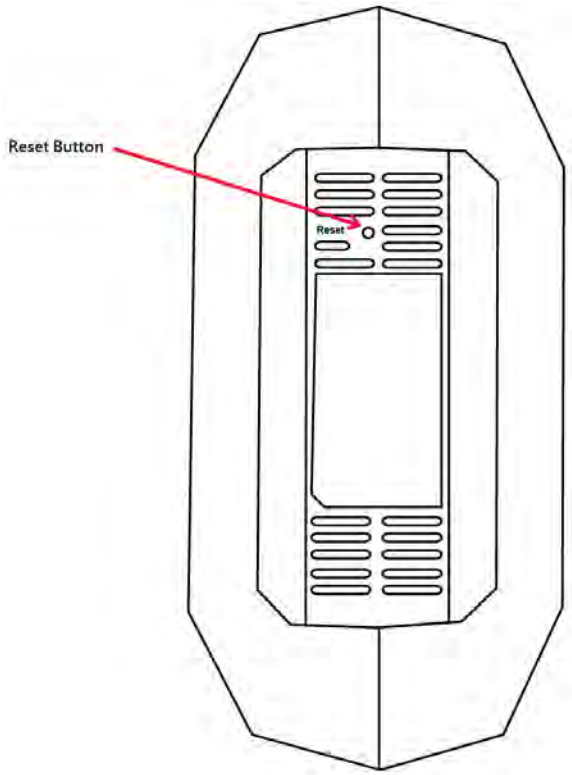
LAN (Ethernet) Ports
You can connect the router to up to four LAN devices using RJ45 cables. The ports are auto-sensing MDI/X and either straight-through or crossover cable can be used.

DSL
Connect to the DSL port with the DSL RJ11 cable.

Power ON
Press the power button to the OFF position (OUT). Connect the power adapter to the power port. Attach the power adapter to a wall outlet or other AC source. Press the power button to the ON position (IN). If the Power LED displays as expected then the device is ready for setup (see section – LED Indicators).

Caution 1:	If the device fails to power up, or it malfunctions, first verify that the power cords are connected securely and then power it on again. If the problem persists, contact technical support.
Caution 2:	Before servicing or disassembling this equipment, disconnect all power cords and telephone lines from their outlets.

2.1.2 Bottom Panel

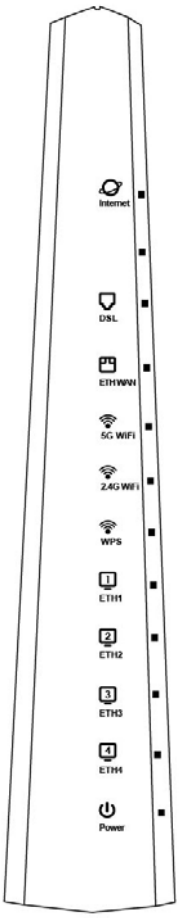


Reset Button
Restore the default parameters of the device by pressing the Reset button for 10 seconds. After the device has rebooted successfully, the front panel should display as expected (see section 2.1.3 Front Panel for details).

NOTE:	If pressed down for more than 60 seconds, the VR-3053 will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

2.1.3 Front Panel

The front panel LED indicators are shown below and explained in the following table. This information can be used to check the status of the device and its connections.



LED	Color	Mode	Function
INTERNET	Green	On	IP connected and no traffic detected. If an IP or PPPoE session is dropped due to an idle timeout, the light will remain blue. The light will turn red when it attempts to reconnect and DHCP or PPPoE fails.
		Off	Modem power off, modem in bridged mode or WAN connection not present.
		Blink	IP connected and IP Traffic is passing through the device (either direction)
	Red	On	Device attempted to become IP connected and failed (no DHCP response, no PPPoE response, PPPoE authentication failed, no IP address from IPCP, etc.)
DSL	Green	On	xDSL Link is established.
		Off	xDSL Link is not established.
		Blink	xDSL Link is training or data transmitting.

ETH WAN	Green	On	Ethernet WAN is connected.
		Off	Ethernet WAN is not connected.
		Blink	Ethernet WAN is transmitting/ receiving.
5G WiFi	Green	On	Wi-Fi enabled.
		Off	Wi-Fi disabled.
		Blink	Data transmitting or receiving over WLAN.
2.4G WiFi	Green	On	Wi-Fi enabled.
		Off	Wi-Fi disabled.
		Blink	Data transmitting or receiving over WLAN.
WPS	Green	On	WPS connection successful. The LED will stay on for 3 minutes.
		Off	No WPS association process ongoing.
		Slow Blink	WPS connection in progress.
		Fast Blink	WPS connection unsuccessful. The LED will keep blinking for 30 seconds.
ETH 1X-4X	Green	On	An Ethernet Link is established.
		Off	An Ethernet Link is not established.
		Blink	Data transmitting or receiving over Ethernet.
POWER	Green	On	The device is powered up.
		Off	The device is powered down.
	Red	On	POST (Power On Self Test) failure or other malfunction. A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data.

Note:

A malfunction is any error of internal sequence or state that will prevent the device from connecting to the DSLAM or passing customer data. This may be identified at various times such after power on or during operation through the use of self testing or in operations which result in a unit state that is not expected or should not occur.

IP connected (the device has a WAN IP address from IPCP or DHCP and DSL is up or a static IP address is configured, PPP negotiation has successfully complete – if used – and DSL is up) and no traffic detected. If the IP or PPPoE session is dropped for any other reason, the light is turned off. The light will turn red when it attempts to reconnect and DHCP or PPPoE fails.

Chapter 3 Web User Interface

This section describes how to access the device via the web user interface (WUI) using an Internet browser such as Internet Explorer (version 5.0 and later).

3.1 Default Settings

The factory default settings of this device are summarized below.

- LAN IP address: 192.168.1.1
- LAN subnet mask: 255.255.255.0
- Administrative access (username: **root**, password: **12345**)
- User access (username: **user**, password: **user**)
- Remote (WAN) access (username: **support**, password: **support**)
- WLAN access: **enabled**

Technical Note

During power on, the device initializes all settings to default values. It will then read the configuration profile from the permanent storage section of flash memory. The default attributes are overwritten when identical attributes with different values are configured. The configuration profile in permanent storage can be created via the web user interface or telnet user interface, or other management protocols. The factory default configuration can be restored either by pushing the reset button for more than ten seconds until the power indicates LED blinking or by clicking the Restore Default Configuration option in the Restore Settings screen.

3.2 IP Configuration

DHCP MODE

When the VR-3053 powers up, the onboard DHCP server will switch on. Basically, the DHCP server issues and reserves IP addresses for LAN devices, such as your PC.

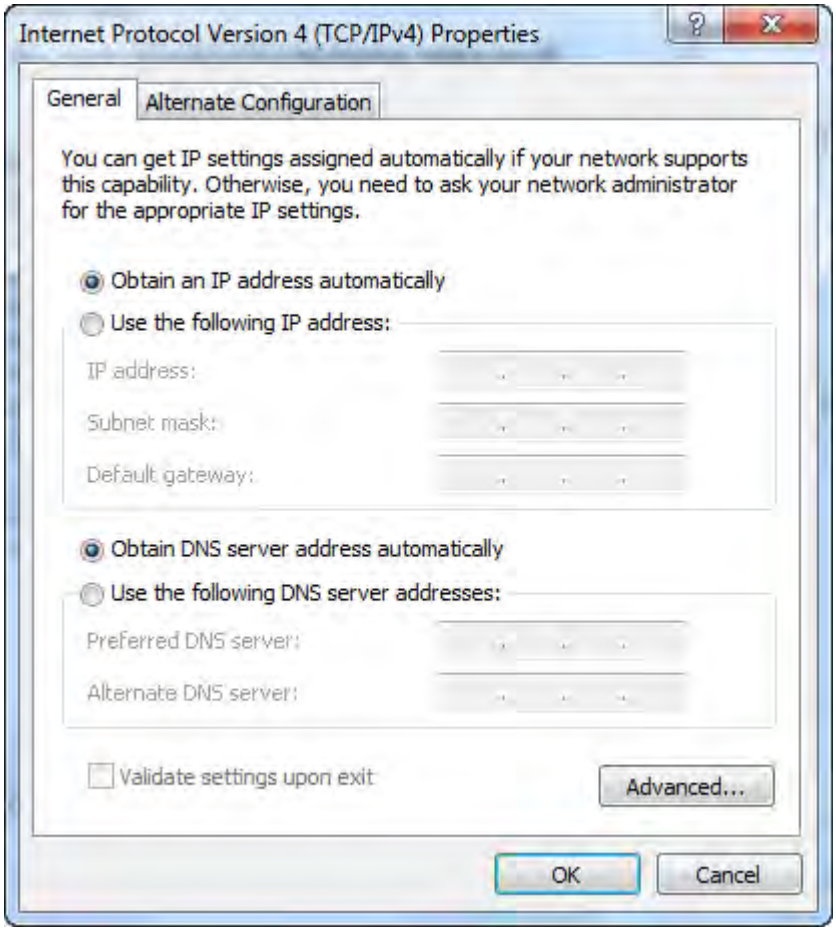
To obtain an IP address from the DCHP server, follow the steps provided below.

NOTE:	The following procedure assumes you are running Windows. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

STEP 1: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.

STEP 2: Select Internet Protocol (TCP/IP) **and click the** Properties button.

STEP 3: Select Obtain an IP address automatically as shown below.



STEP 4: Click **OK** to submit these settings.

If you experience difficulty with DHCP mode, you can try static IP mode instead.

STATIC IP MODE

In static IP mode, you assign IP settings to your PC manually.

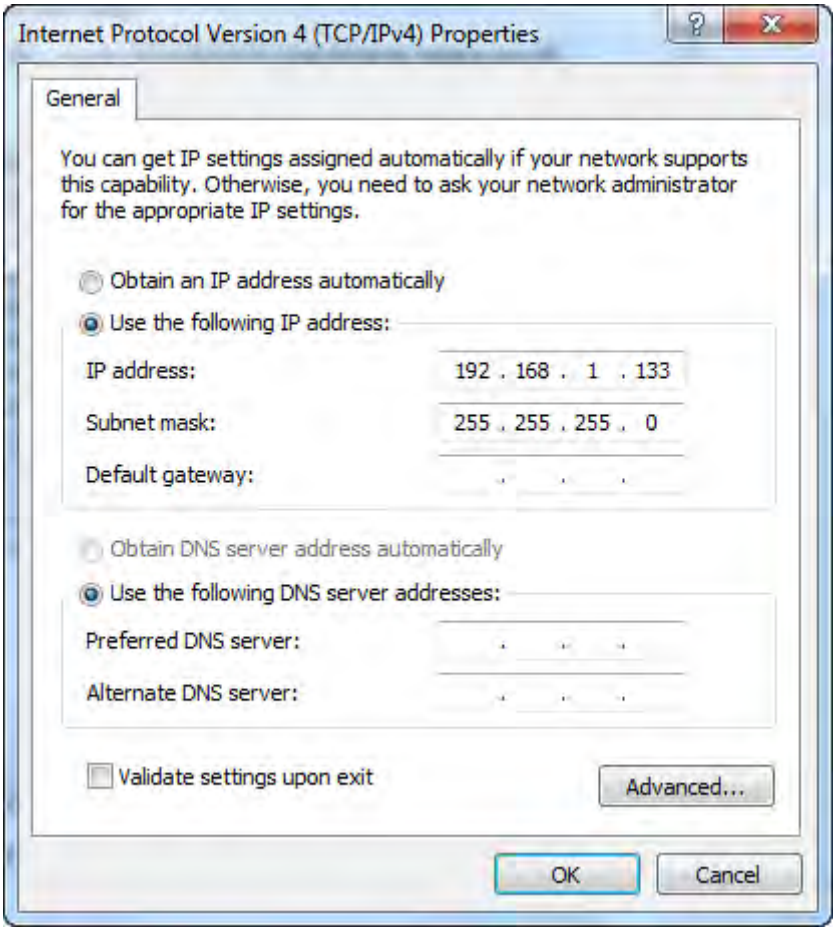
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

NOTE:	The following procedure assumes you are running Windows. However, the general steps involved are similar for most operating systems (OS). Check your OS support documentation for further details.

STEP 1: From the Network Connections window, open Local Area Connection (*You may also access this screen by double-clicking the Local Area Connection icon on your taskbar*). Click the **Properties** button.

STEP 2: Select Internet Protocol (TCP/IP) **and click the** Properties button.

STEP 3: Change the IP address to the 192.168.1.x (1<x<255) subnet with subnet mask of 255.255.255.0. The screen should now display as shown below.



STEP 4: Click **OK** to submit these settings.

3.3 Login Procedure

Perform the following steps to login to the web user interface.

NOTE:	The default settings can be found in 3.1 Default Settings.

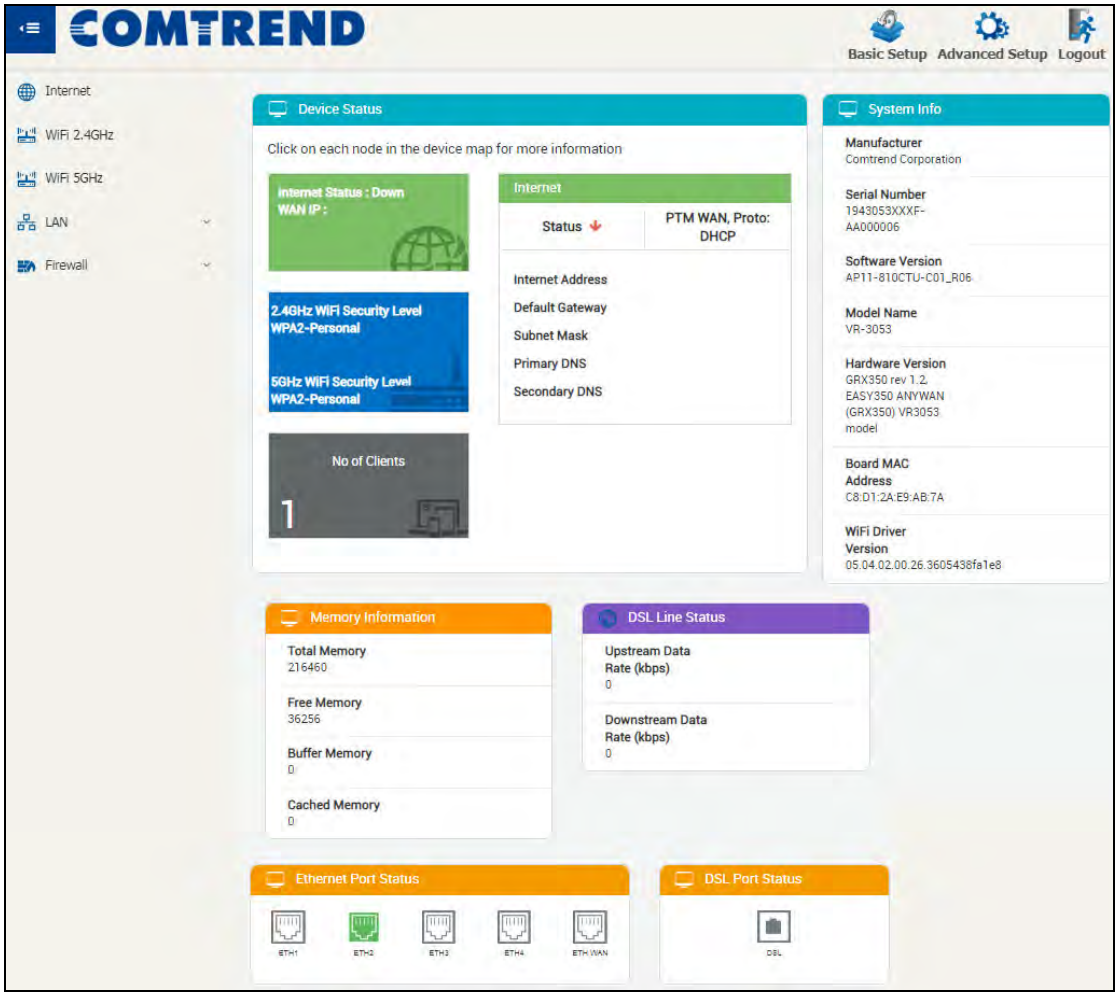
STEP 1: Start the Internet browser and enter the default IP address for the device in the Web address field. For example, if the default IP address is 192.168.1.1, type http://192.168.1.1.

NOTE:	For local administration (i.e. LAN access), the PC running the browser must be attached to the Ethernet, and not necessarily to the device.

STEP 2: A dialog box will appear, such as the one below. Enter the default username and password, as defined in section 3.1 Default Settings.

Click **OK** to continue.

STEP 3: After successfully logging in for the first time, you will reach this screen.



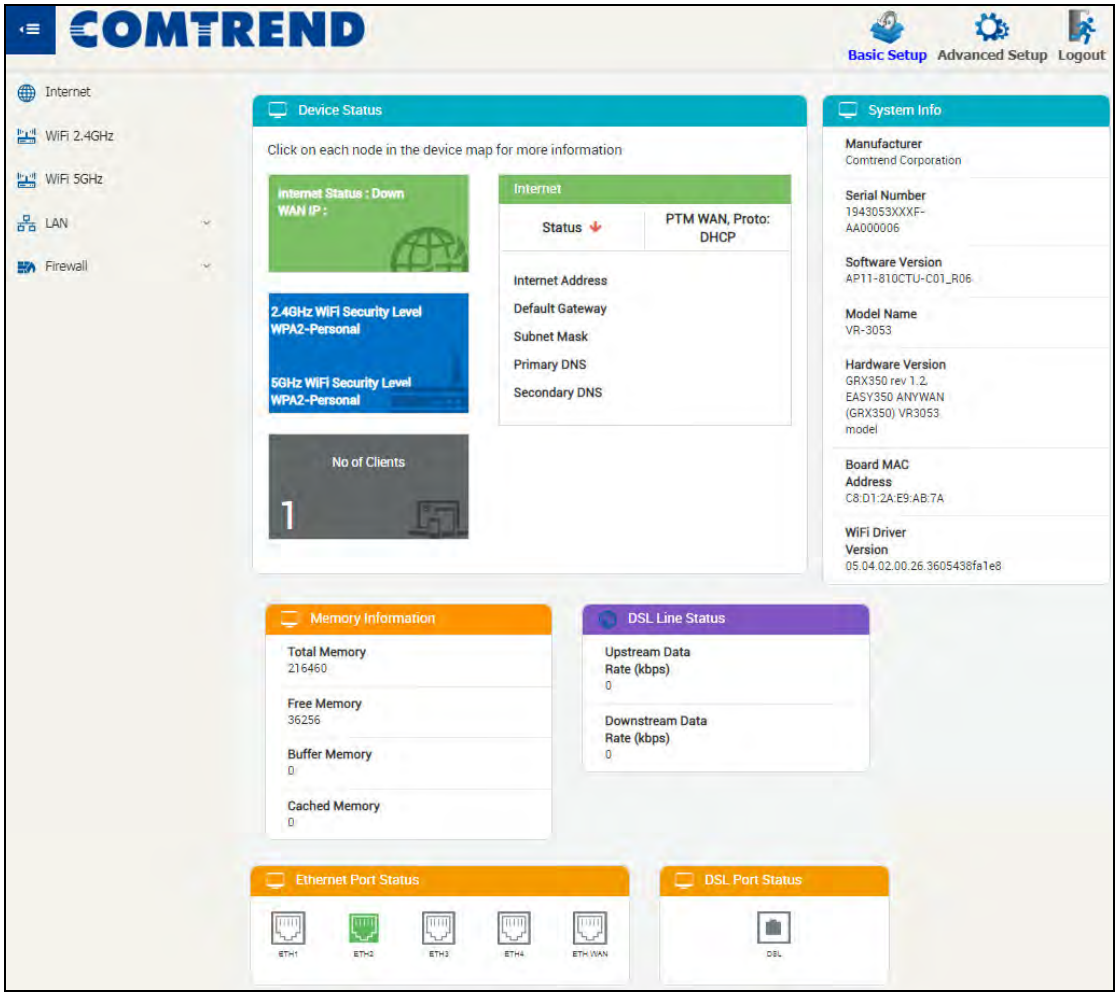
You can also reach this page by clicking on the following icon located at the top of the screen.

Chapter 4 Basic Setup

You can reach this page by clicking on the following icon located at the top of the screen.

The web user interface window is divided into two frames, the main menu (at left) and the display screen (on the right). The main menu has several options and selecting each of these options opens a submenu with more selections.

NOTE:	The menu items shown are based upon the configured connection(s) and user account privileges. For example, if NAT and Firewall are enabled, the main menu will display the NAT and Security submenus. If either is disabled, their corresponding menu(s) will also be disabled.



This screen shows hardware, software, IP settings and other related information.

4.1 Internet

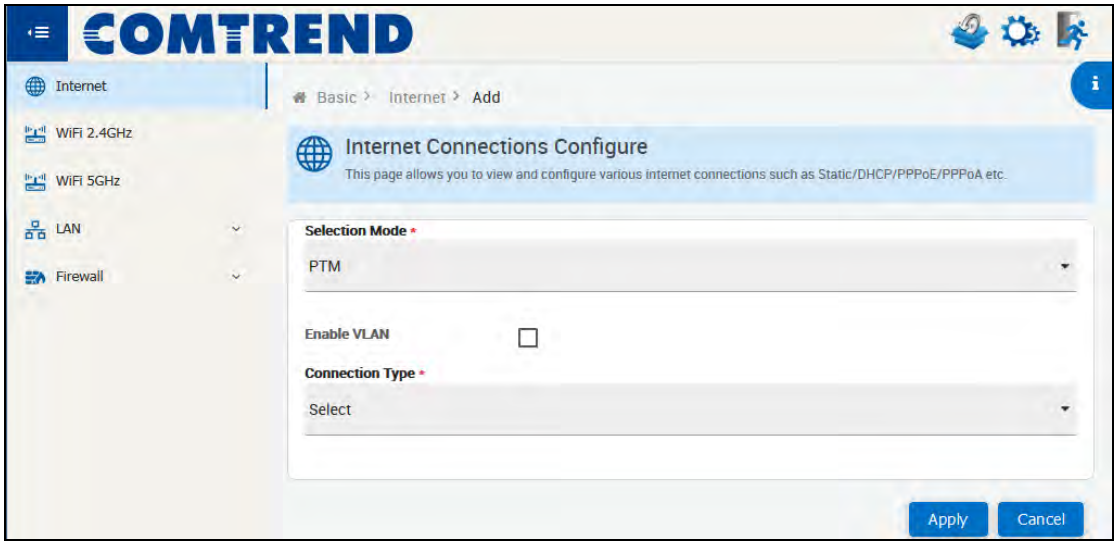
Click on the internet tab

to display the following.

For a tour of the page, please click the question mark icon on the upper right-hand side of this screen.

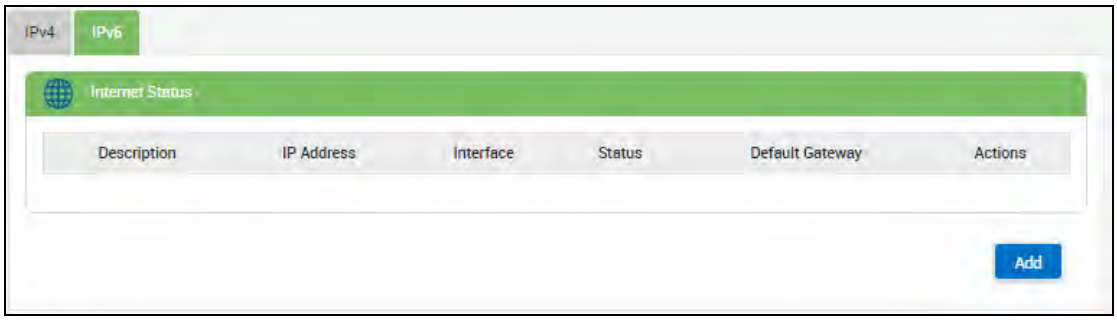
To add aconnection, click the

button to display the following.



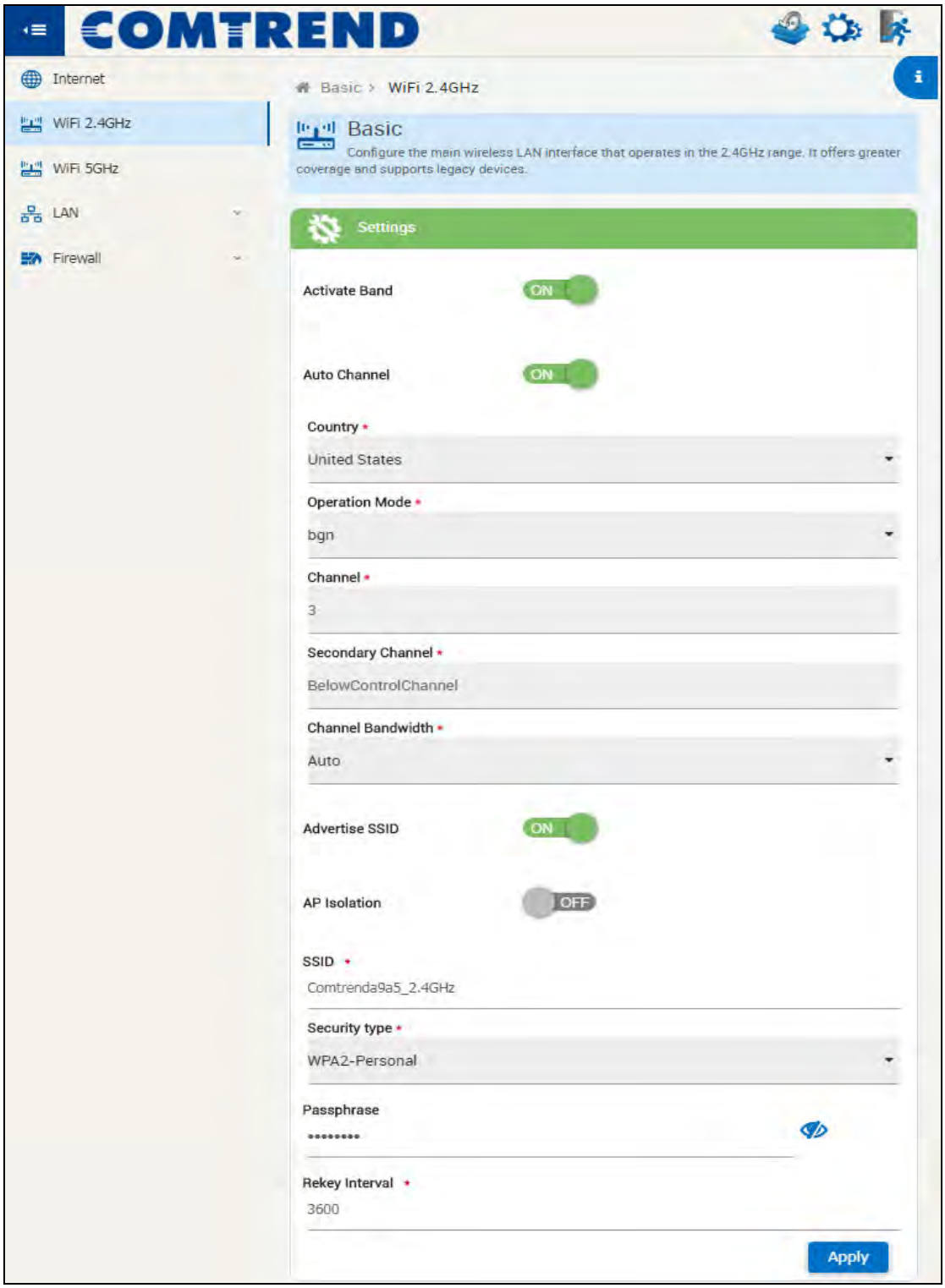
Click the Information icon on the upper right-hand side of this screen for information on Internet Connections.

IPv6 for your reference.



4.2 WiFi 2.4GHz

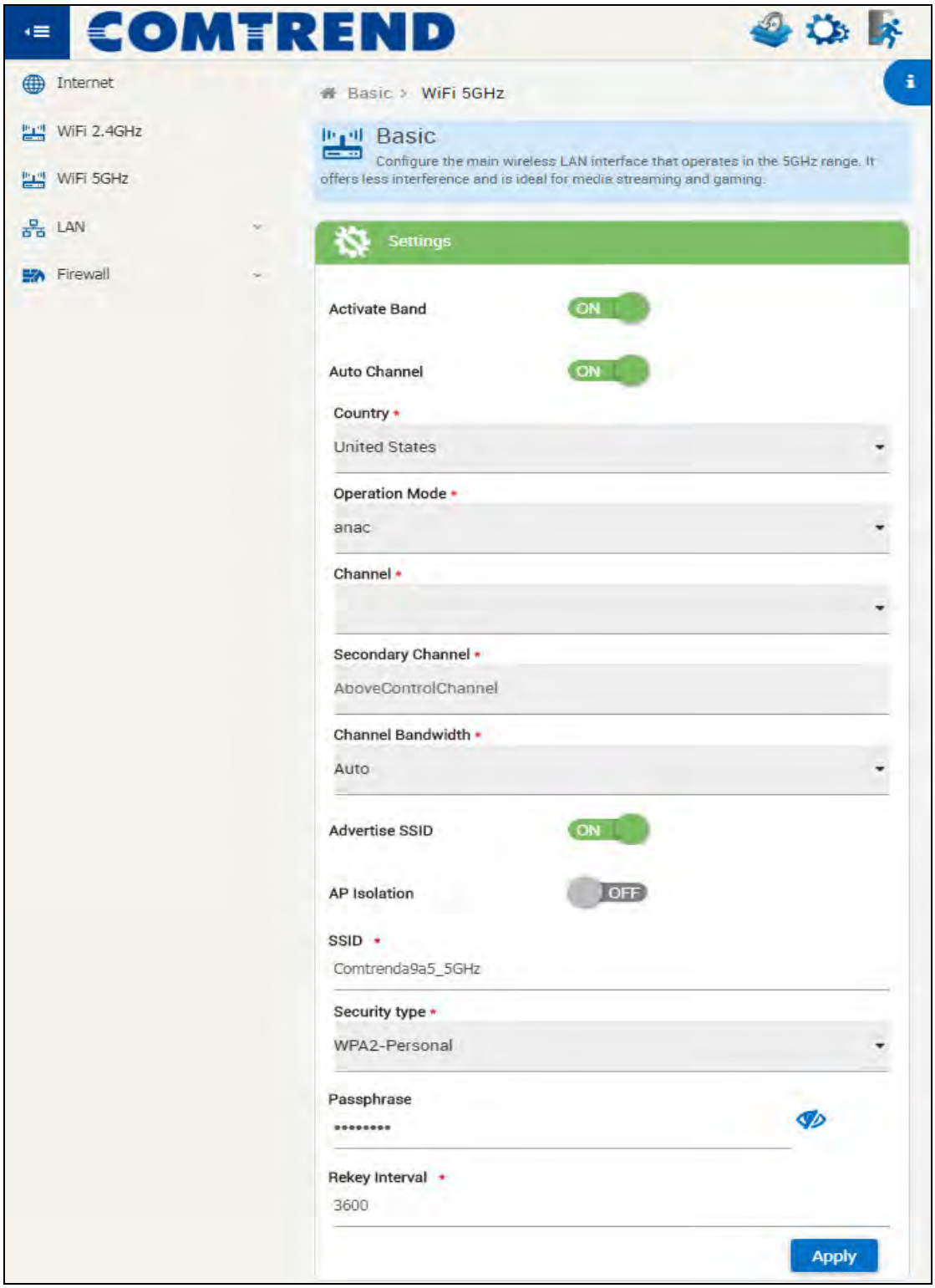
Configure the main wireless LAN interface that operates in the 2.4GHz range. It offers greater coverage and supports legacy devices.



Click the Information icon on the upper right-hand side of this screen for information on 2.4GHZ WiFi Settings.

4.3 WiFi 5GHz

Configure the main wireless LAN interface that operates in the 5GHz range. It offers less interference and is ideal for media streaming and gaming.

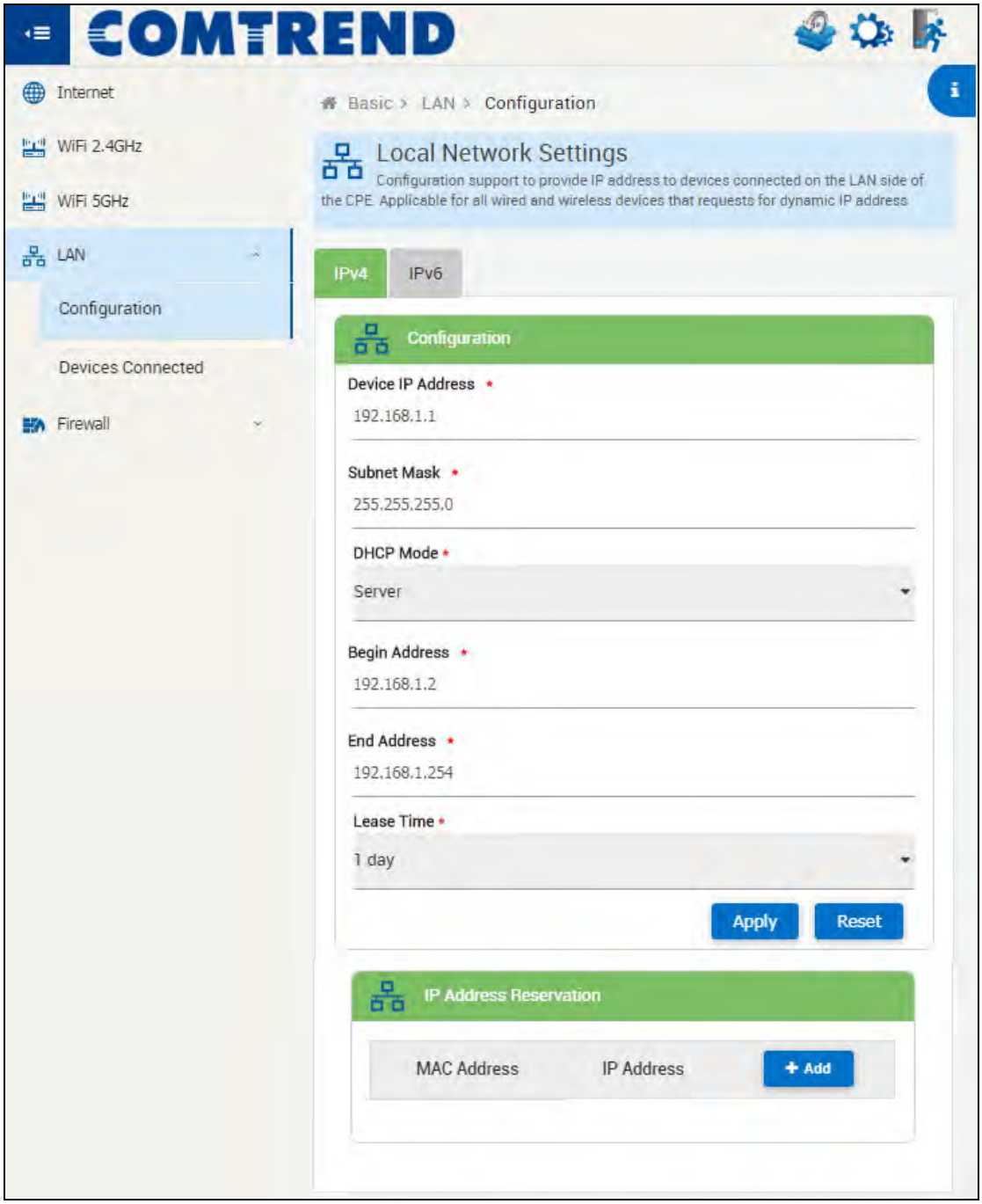


Click the Information icon on the upper right-hand side of this screen for information on 5GHZ WiFi Settings.

4.4 LAN

4.4.1 Configuration

Configuration support to provide IP address to devices connected on the LAN side of the CPE. Applicable for all wired and wireless devices that requests a dynamic IP address.



Click the Information icon on the upper right-hand side of this screen for information on Local Network Settings.

4.4.2 Devices Connected

This displays the List of Clients Connected on the LAN Side of the CPE.

MAC Address

MAC address of the device that is connected to the LAN port.

Host Name

Host Name of the device that is connected to the LAN port.

IP Address

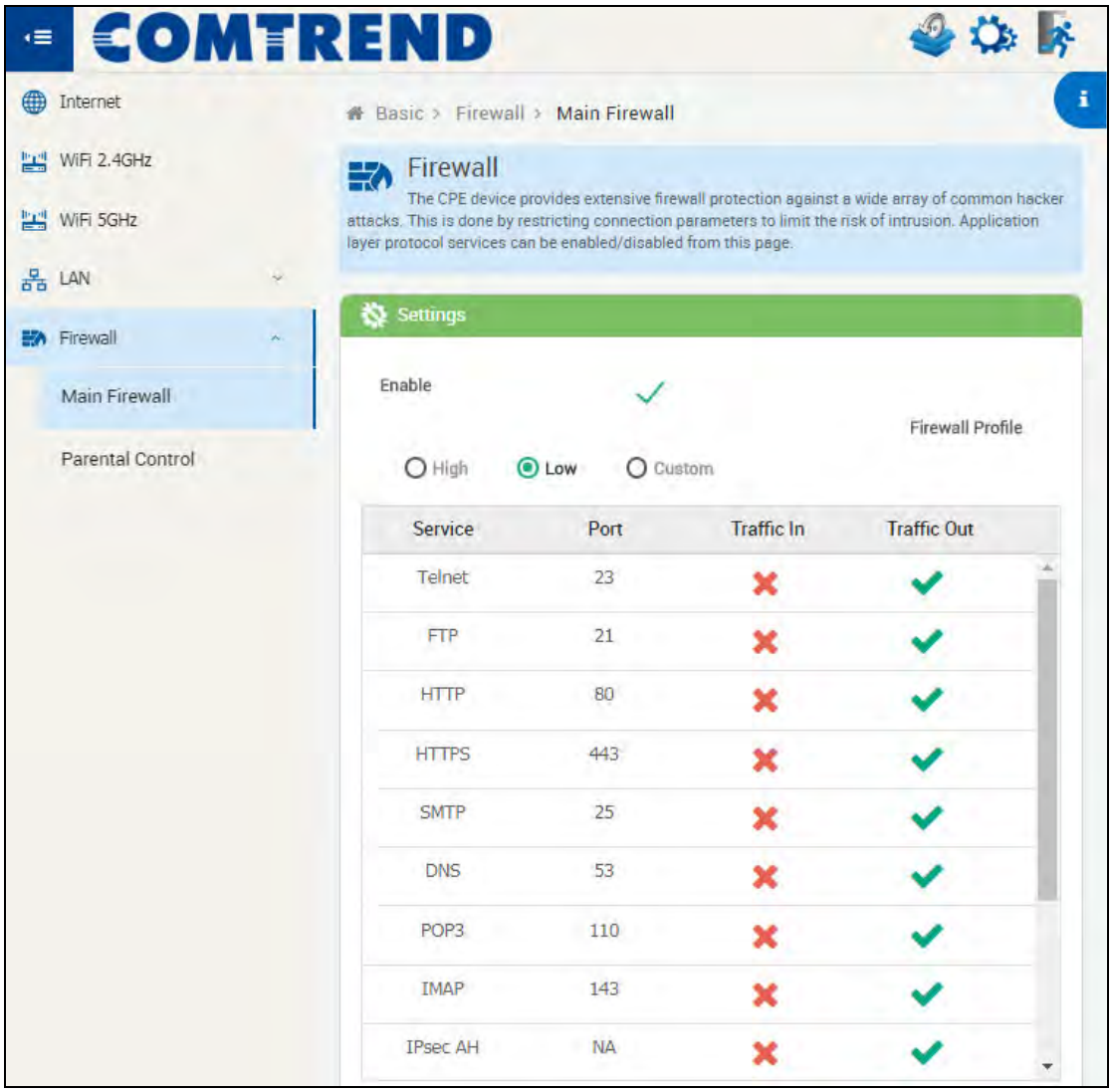
IP Address of the device that is connected to the LAN port.

Click the Refresh button to refresh the screen.

4.5 Firewall

4.5.1 Main Firewall

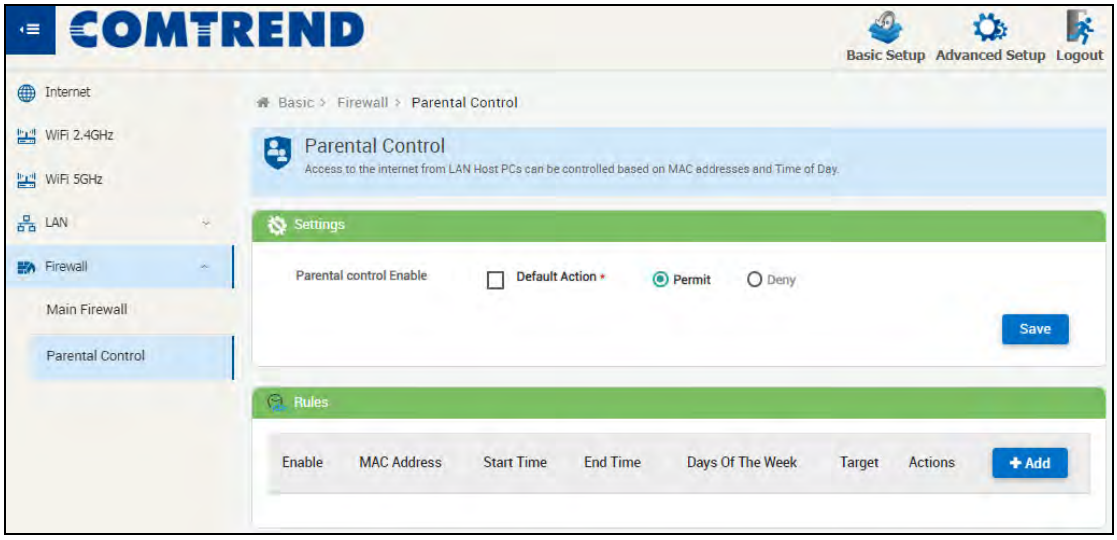
The CPE device provides extensive firewall protection against a wide array of common hacker attacks. This is done by restricting connection parameters to limit the risk of intrusion. Application layer protocol services can be enabled/disabled from this page.



Click the Information icon on the upper right-hand side of this screen for information on Main Firewall Settings.

4.5.2 Parental Control

Access to the internet from LAN Host PCs can be controlled based on MAC addresses and Time of Day.

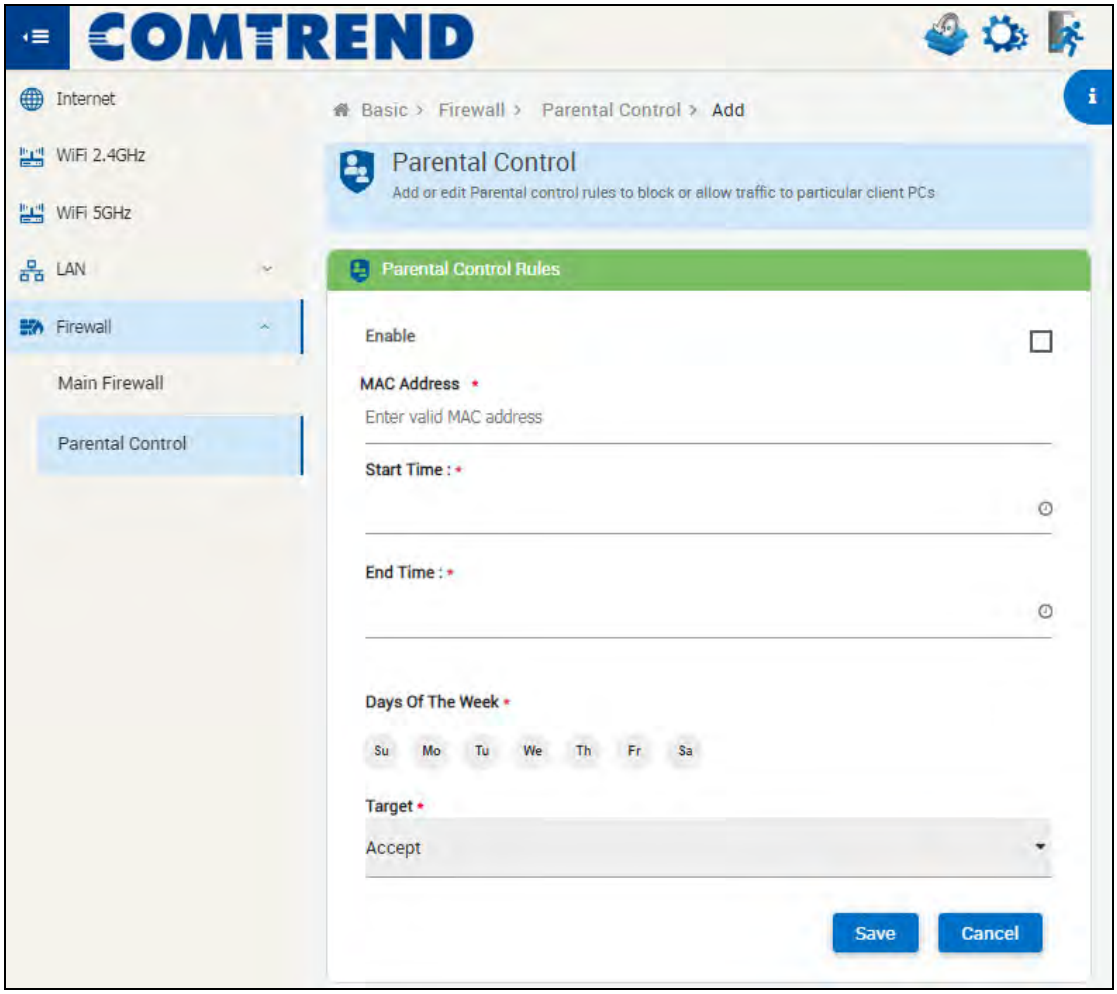


Select the default action Permit or Deny and click the

button.

Click the

button to display the following.



Click the Information icon on the upper right-hand side of this screen for information on Parental Control Rules.

Click the button to save your Parental Control Rules.

Chapter 5 Advanced Setup

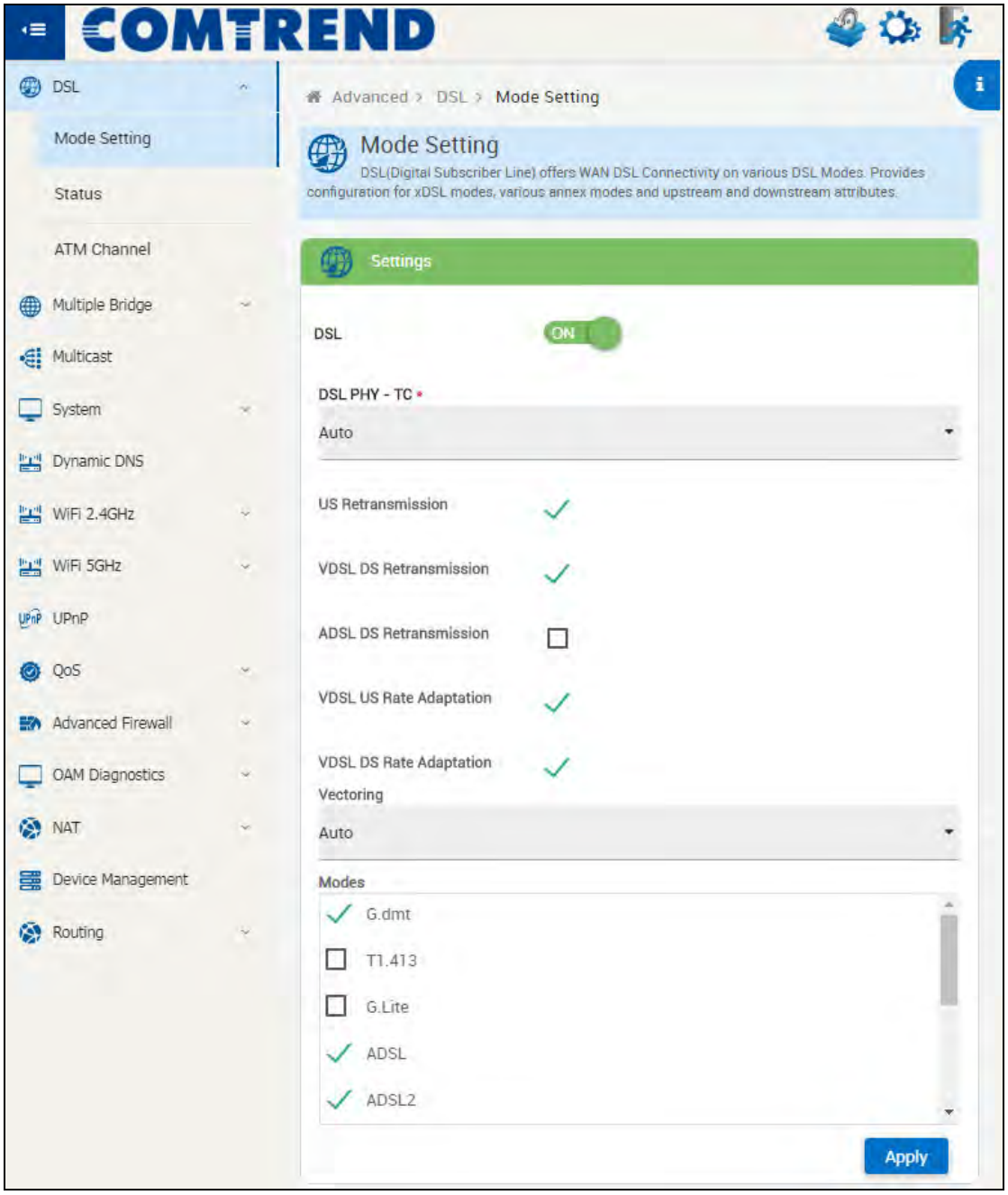
You can reach this page by clicking on the following icon located at the top of the screen.

The web user interface window is divided into two frames, the main menu (at left) and the display screen (on the right). The main menu has several options and selecting each of these options opens a submenu with more selections.

5.1 DSL

5.1.1 Mode Setting

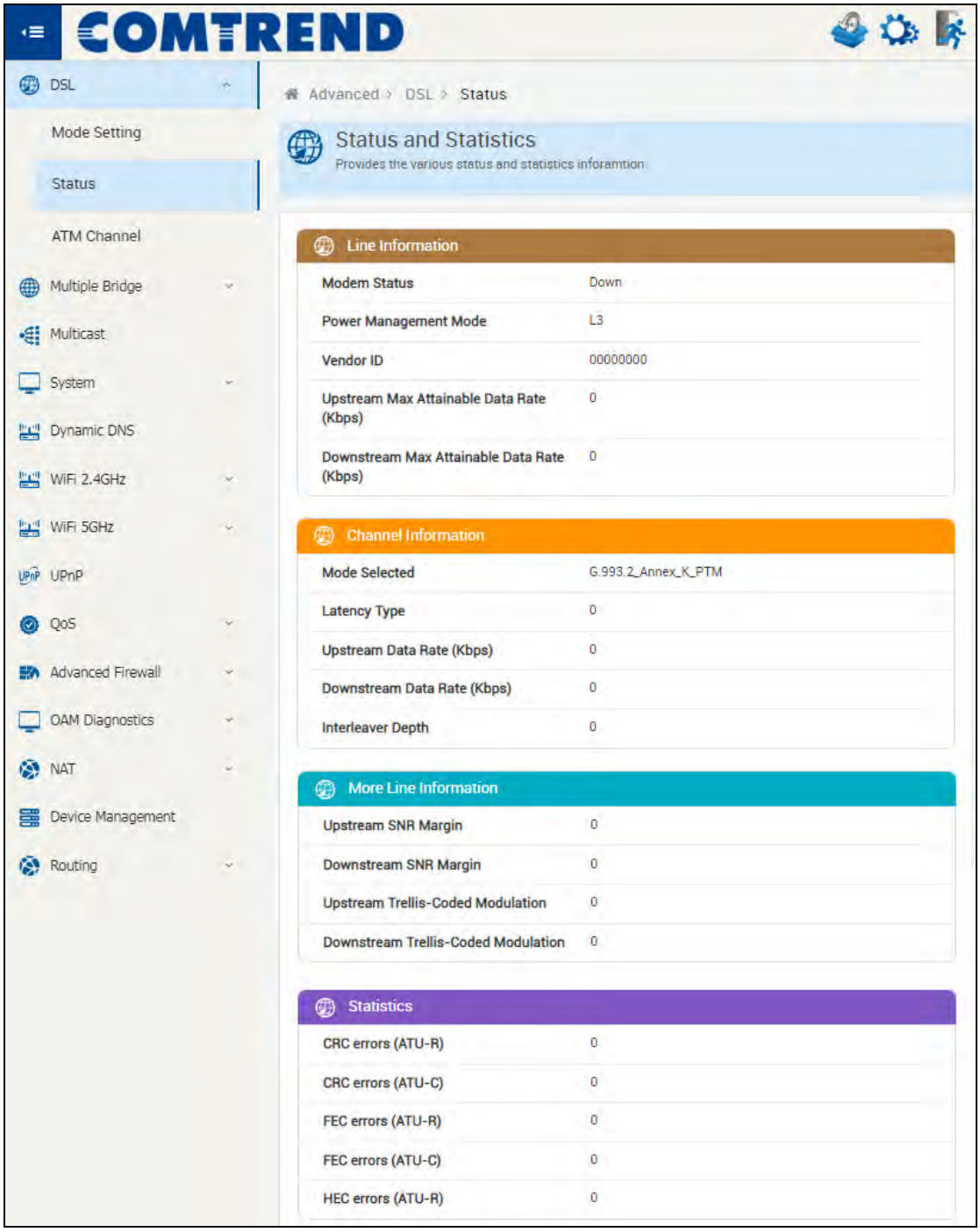
DSL(Digital Subscriber Line) offers WAN DSL Connectivity on various DSL Modes. Provides configuration for xDSL modes, various annex modes and upstream and downstream attributes.



Click the Information icon on the upper right-hand side of this screen for information on Mode Setting.

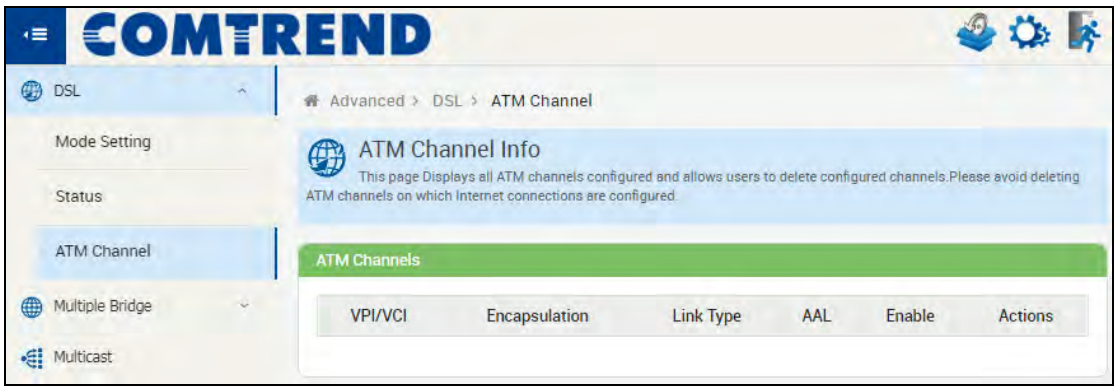
5.1.2 Status

Provides the various status and statistics information.



5.1.3 ATM Channel

This page Displays all ATM channels configured, and allows users to delete configured channels. Please avoid deleting ATM channels on which Internet connections are configured.



VPI / VCI

The Identifier of the Virtual Path and the Virtual Channel for the ATM.

Encapsulation

The encapsulation types are LLC and VCMUX.

Link Type

The link type of the ATM.

AAL

For Types of service: AAL1, AAL2, AAL3 AAL4 and AAL5.

Enable

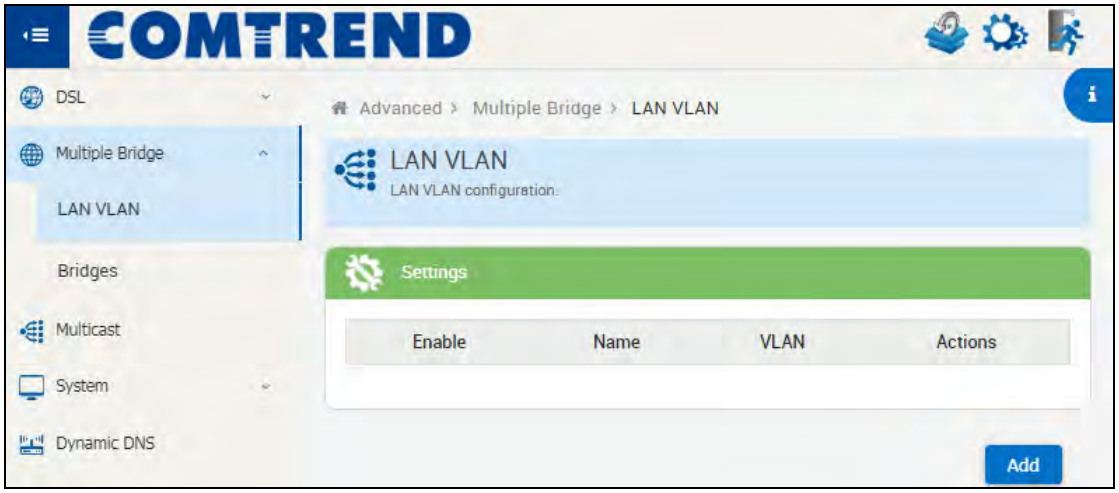
Displays the status.

Actions

Displays details of actions.

5.2 Multiple Bridge

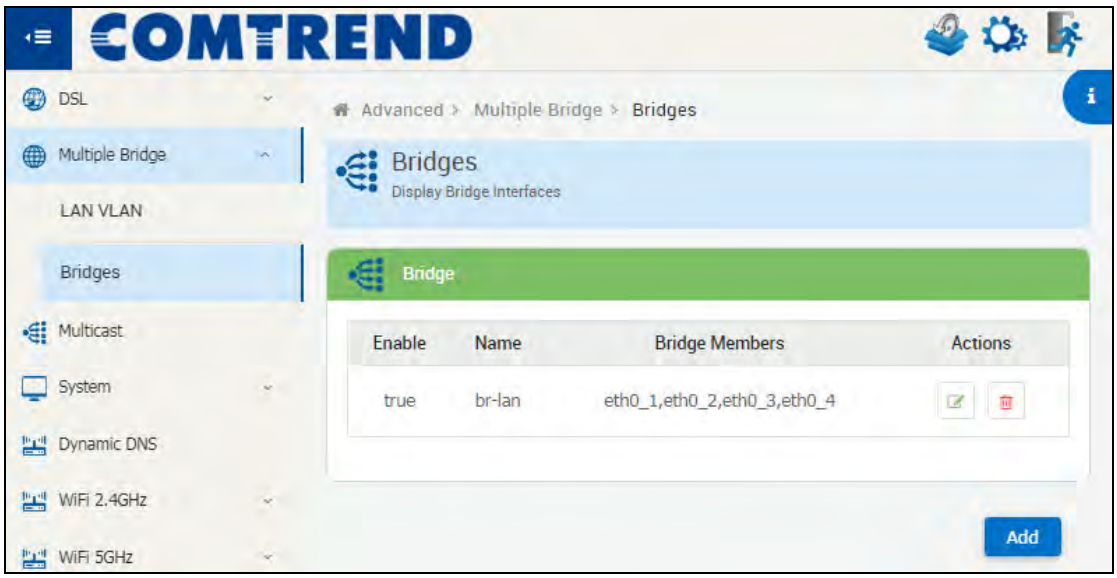
5.2.1 LAN VLAN



Click the Information icon on the upper right-hand side of this screen for information on the LAN VLAN Settings.

5.2.2 Bridges

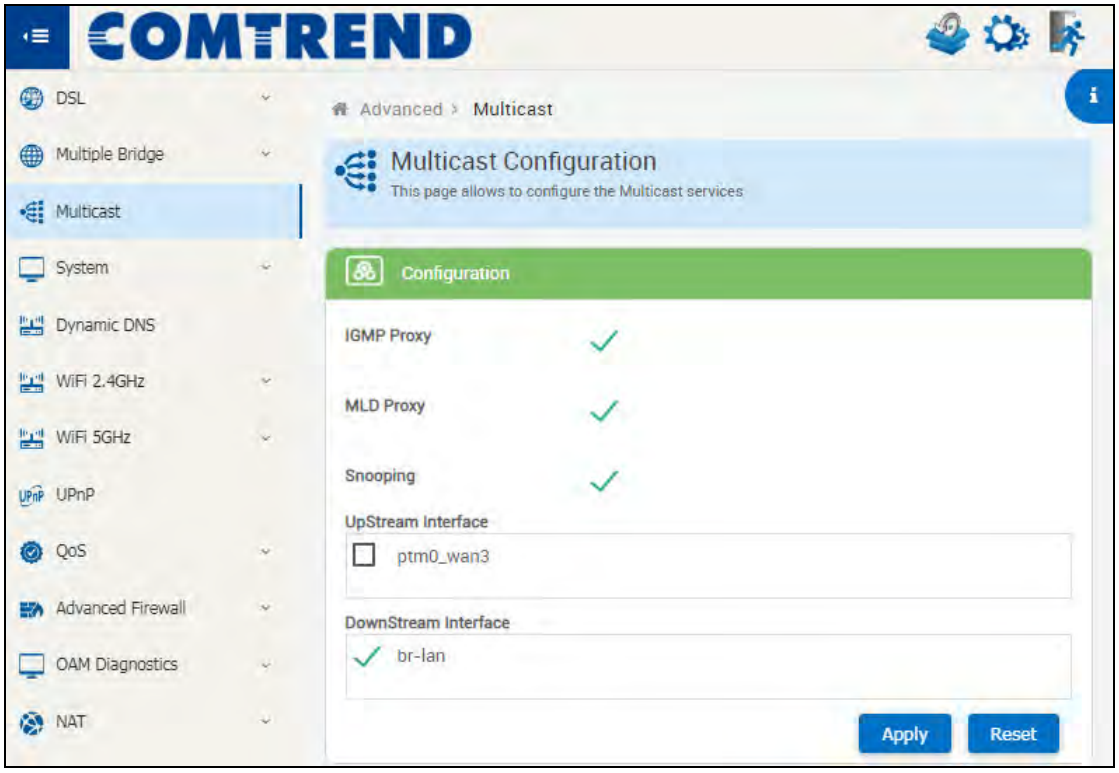
Displays Bridge Interfaces.



Click the Information icon on the upper right-hand side of this screen for information on Bridges Settings.

5.3 Multicast

This page allows you to configure the Multicast services.

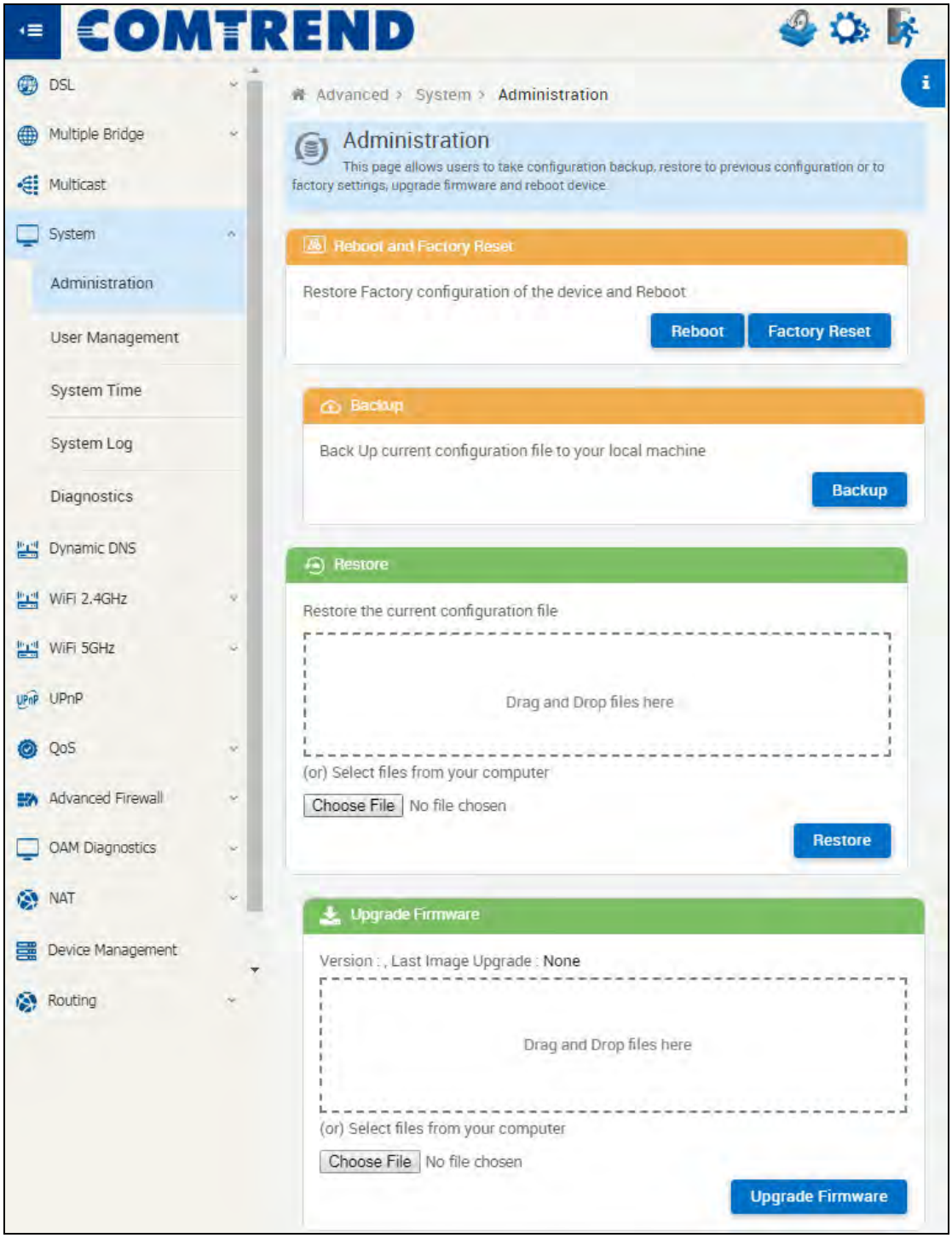


Click the Information icon on the upper right-hand side of this screen for information on Multicast Settings.

5.4 System

5.4.1 Administration

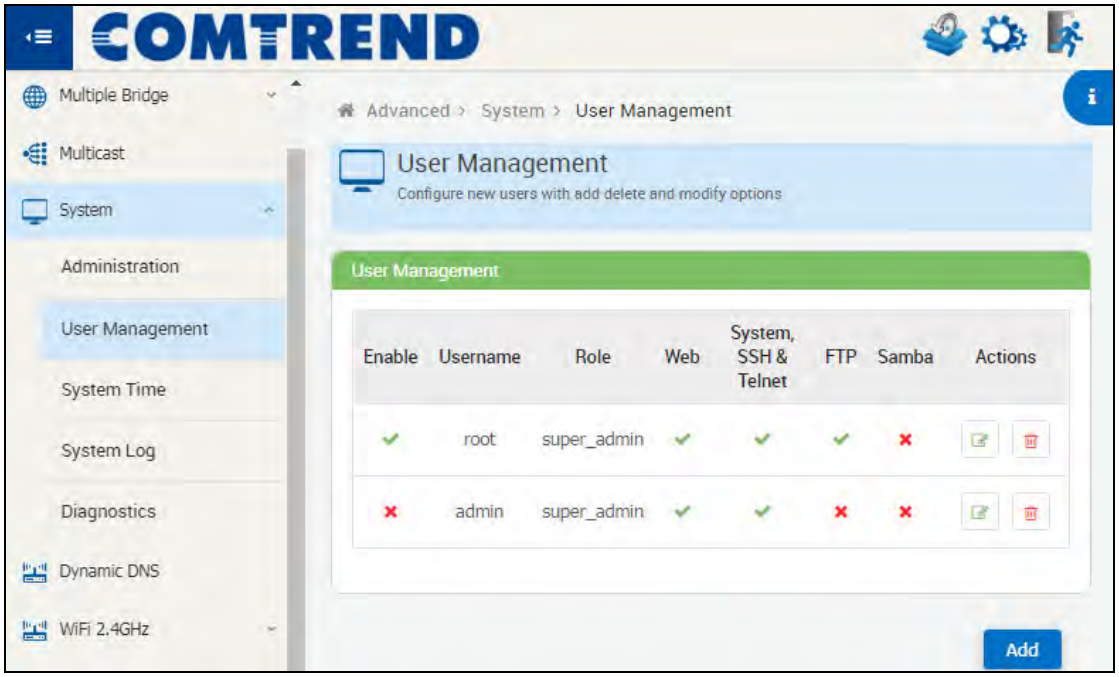
This page allows users to take configuration backup, restore to previous configuration or to factory settings, upgrade firmware and reboot device.



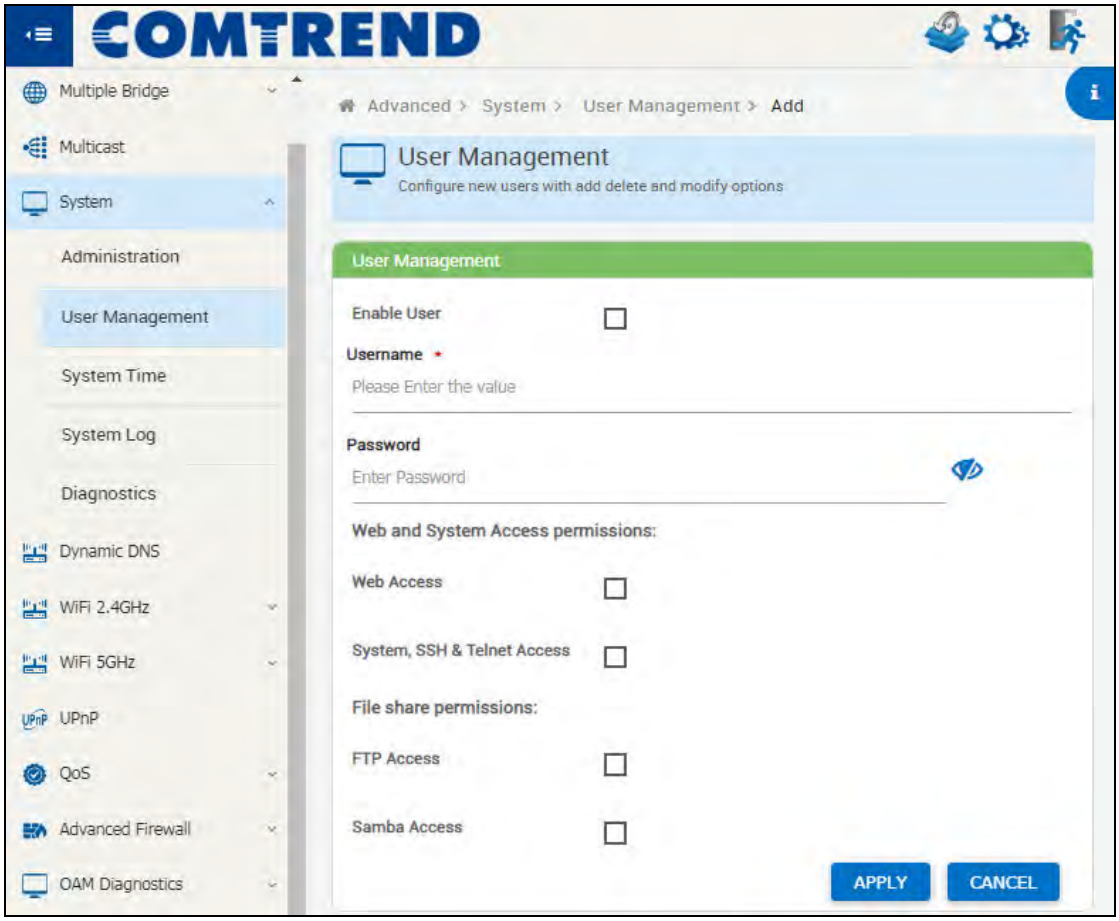
Click the Information icon on the upper right-hand side of this screen for information on Administration Settings.

5.4.2 User Management

Configure new users with add delete and modify options.



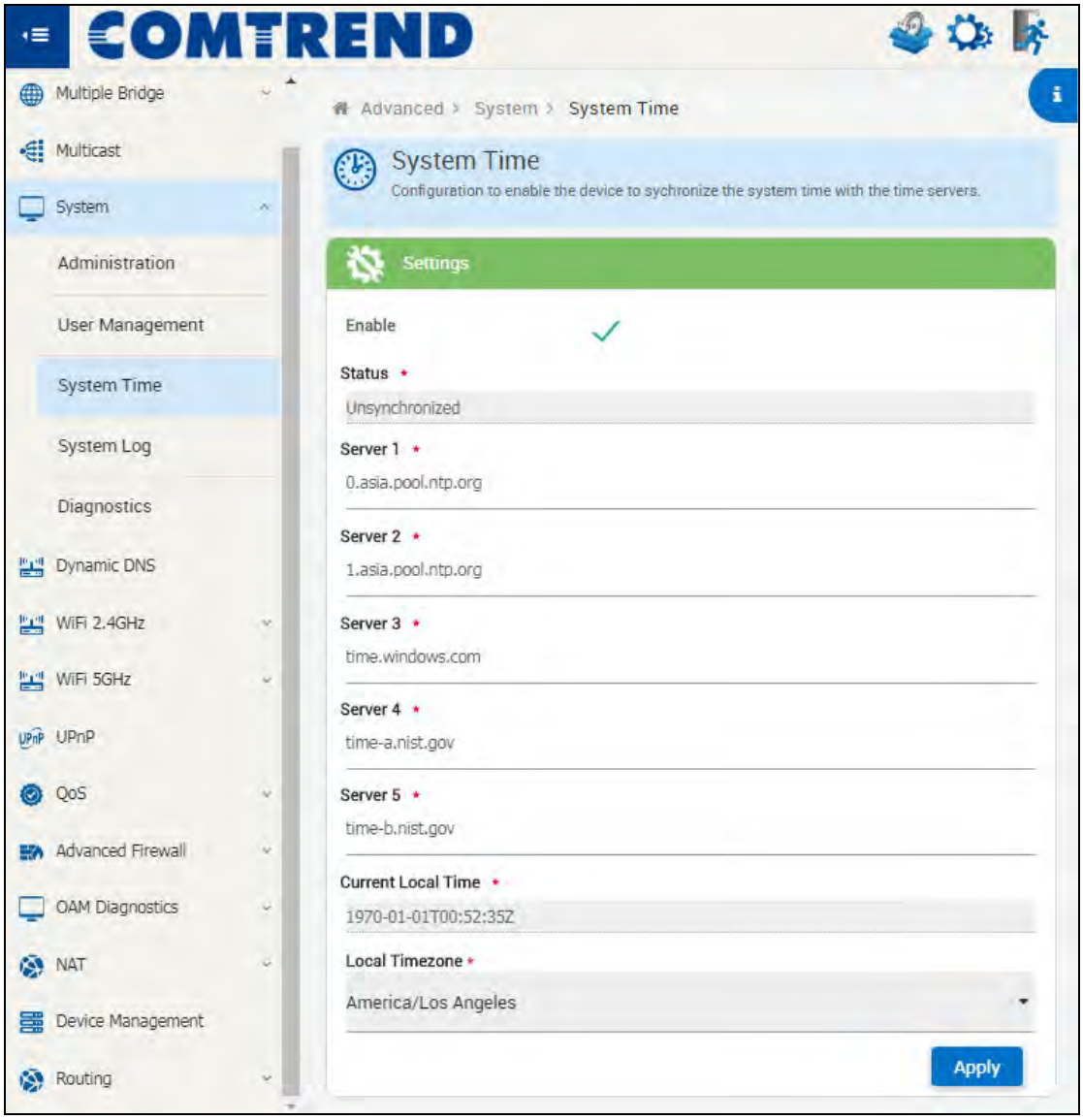
Click the Add button to display the following.



Click the Information icon on the upper right-hand side of this screen for information on User Management Settings.

5.4.3 System Time

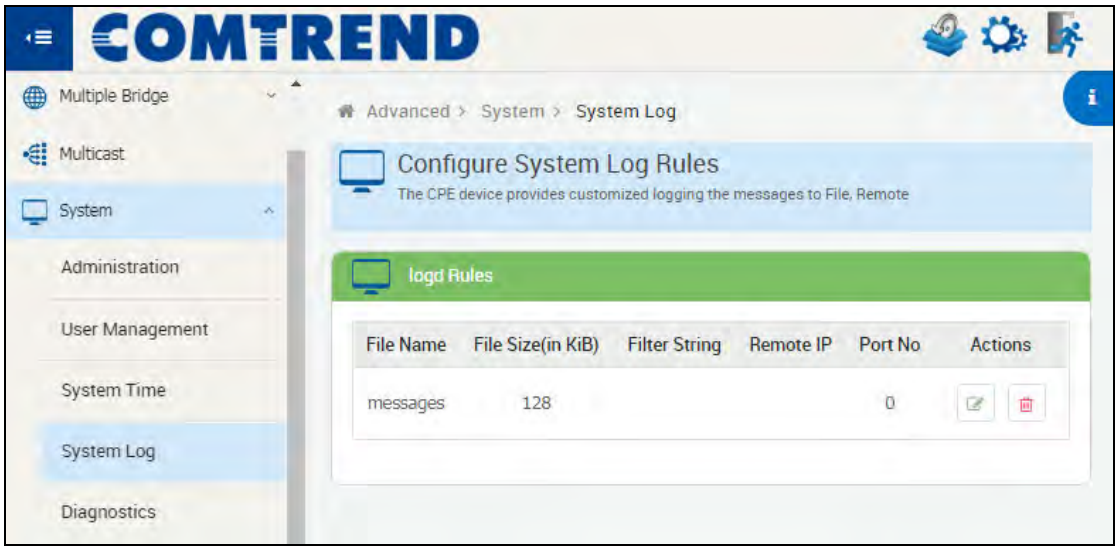
Configuration to enable the device to synchronize the system time with the time servers.



Click the Information icon on the upper right-hand side of this screen for information on System Time Settings.

5.4.4 System Log

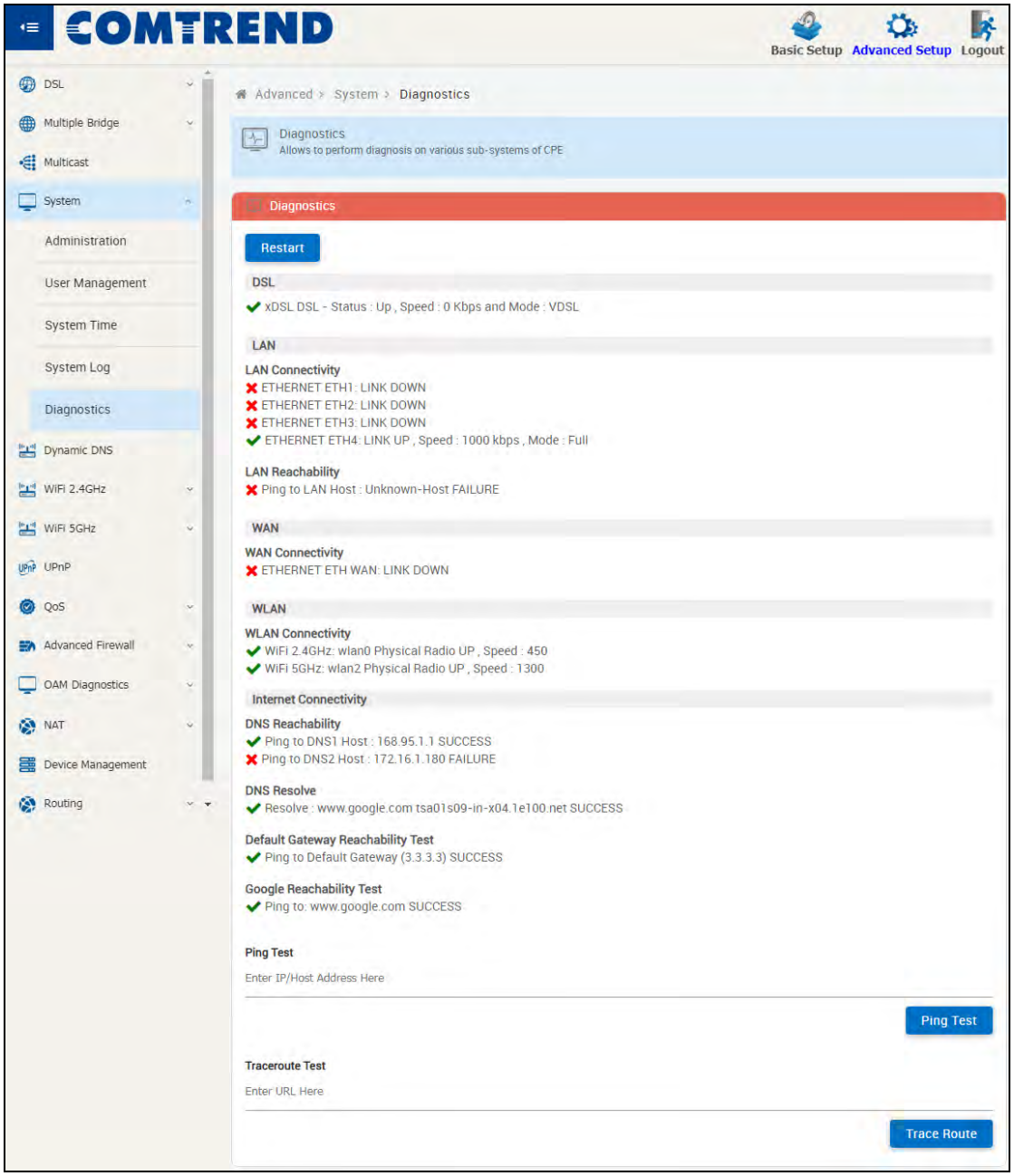
The CPE device provides customized logging the messages to File, Remote.



Click the Information icon on the upper right-hand side of this screen for information on System Log Settings.

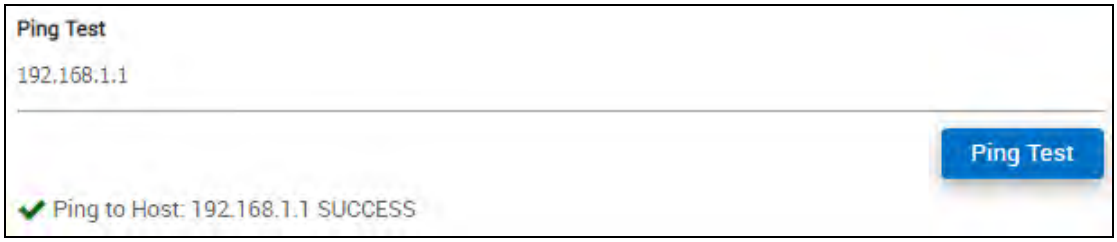
5.4.5 Diagnostics

Allows diagnosis to be performed on various sub-systems of the CPE.

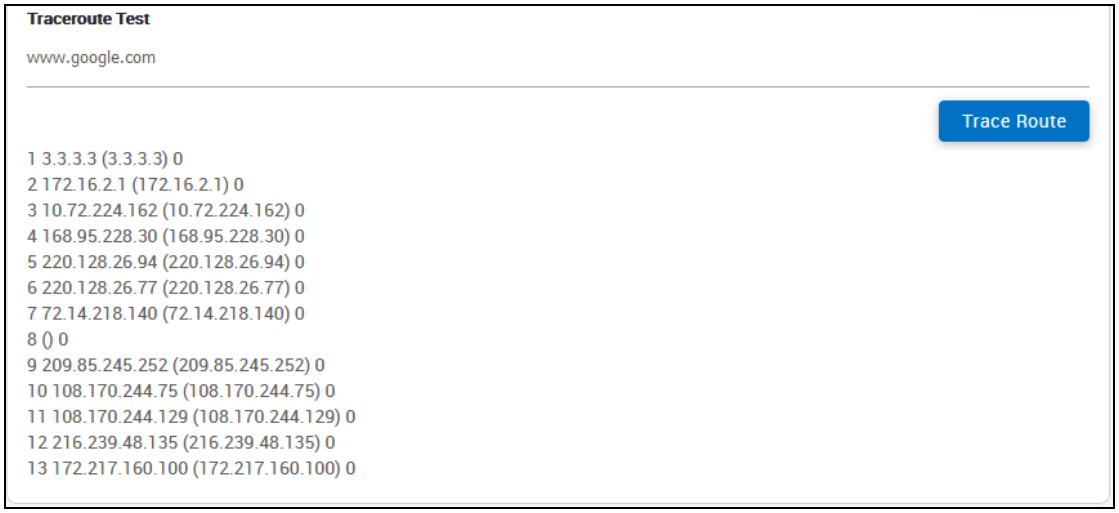


Click the **Restart** button to restart the diagnostic tests.

Input the IP/Host address and click the **Ping Test** button start the test. See below for ping test result.

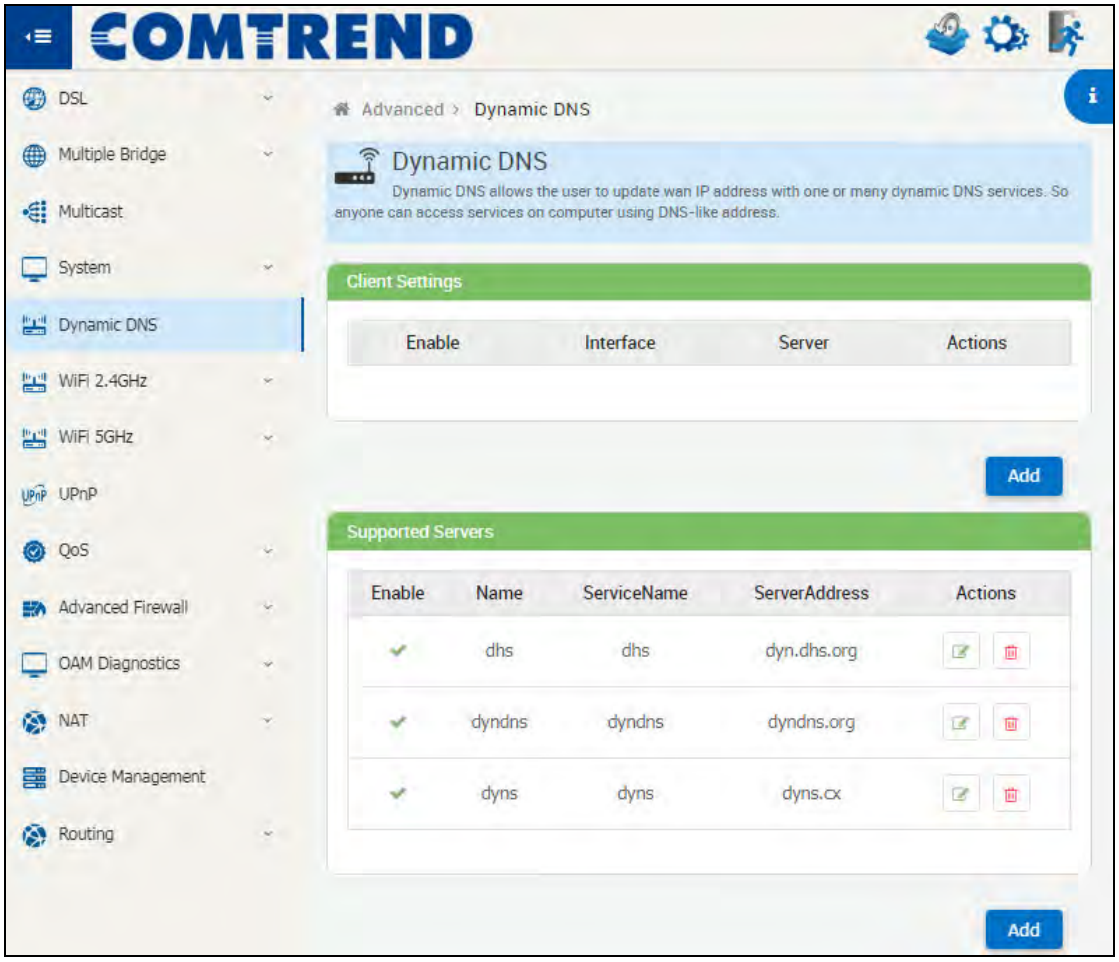


Input the url and click the Trace Route button start the test. See below for trace route result.



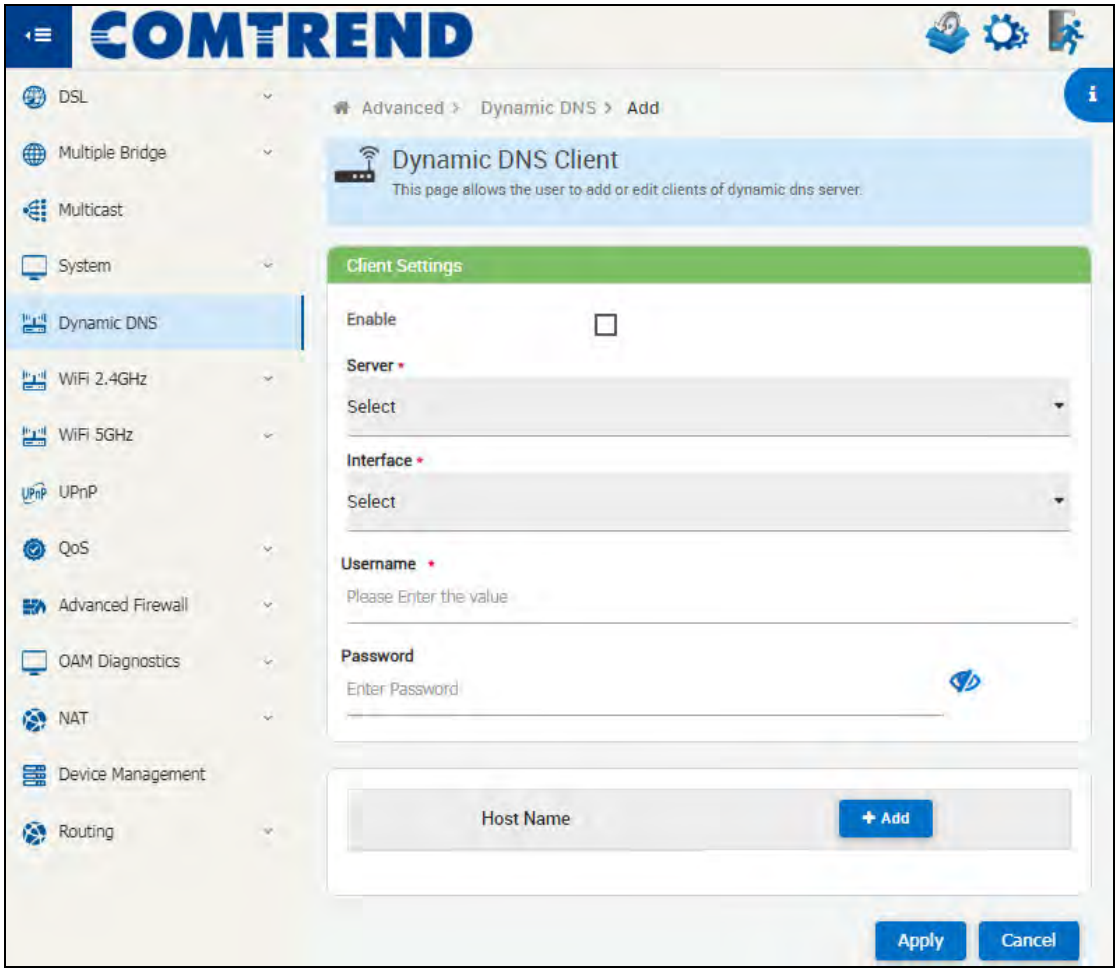
5.5 Dynamic DNS

Dynamic DNS allows the user to update wan IP address with one or many dynamic DNS services. So anyone can access services on computer using DNS-like address.



Client Settings

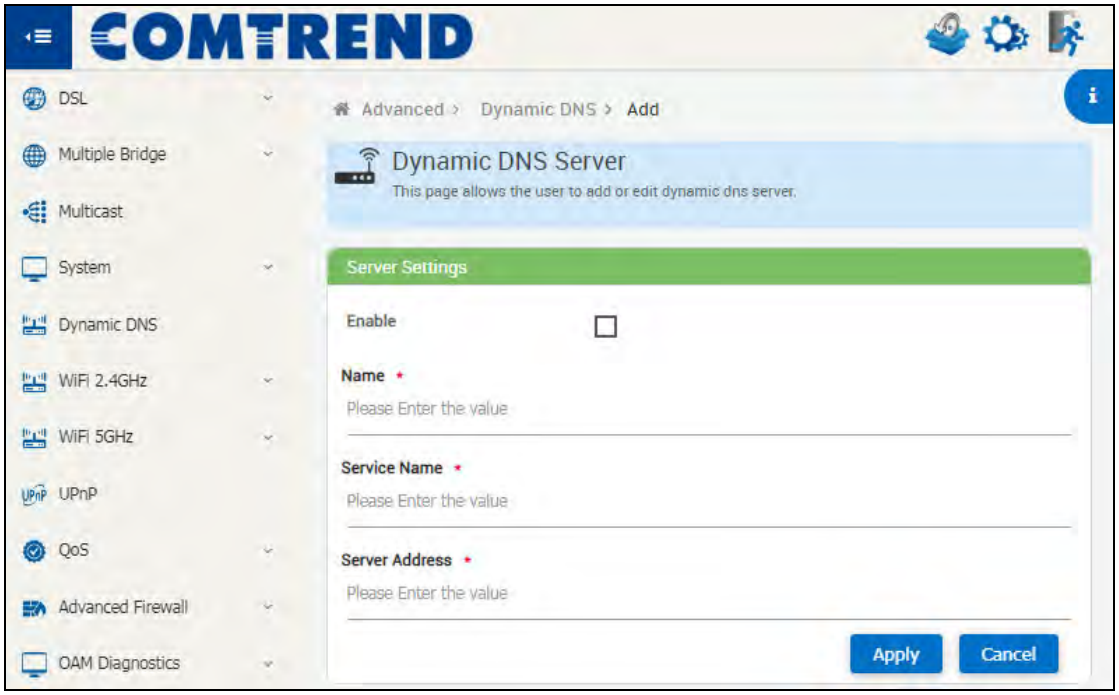
Click the Add button to display the following.



Click the Information icon on the upper right-hand side of this screen for information on Client Settings.

Supported Servers

Click the Add button to display the following.

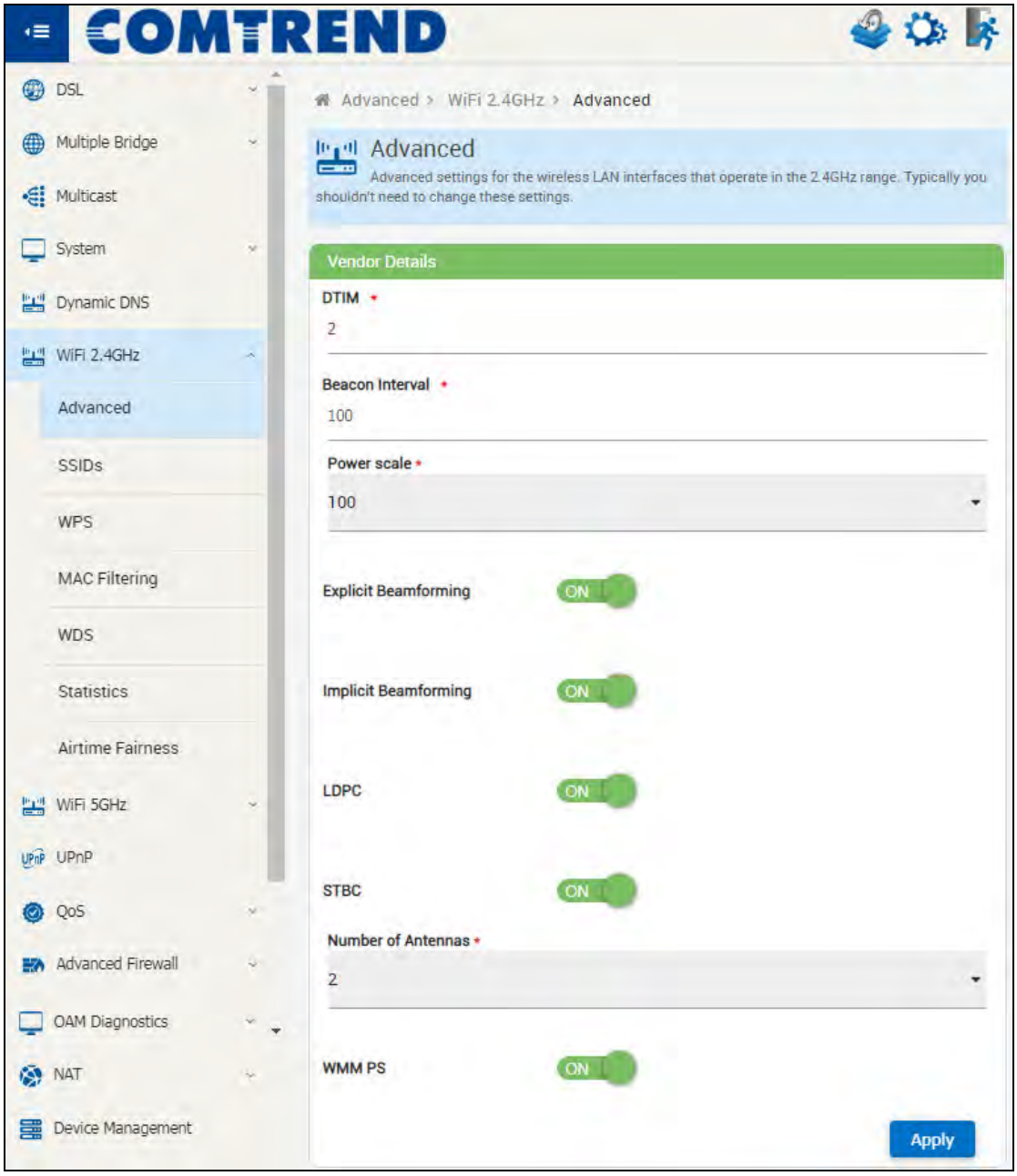


Click the Information icon on the upper right-hand side of this screen for information on Server Settings.

5.6 WiFi 2.4GHz

5.6.1 Advanced

Advanced settings for the wireless LAN interfaces that operate in the 2.4GHz range. Typically you shouldn't need to change these settings.



The settings shown above are described below.

DTIM

A value between 1~255.

Beacon Interval

100 ms by default.

Power Scale

12/25/50/100 and 100 by default.

Explicit Beamforming

Turned on by default.

Implicit Beamforming

Turned on by default.

LDPC

Turned on by default.

STBC

Turned on by default.

Number of Antennas

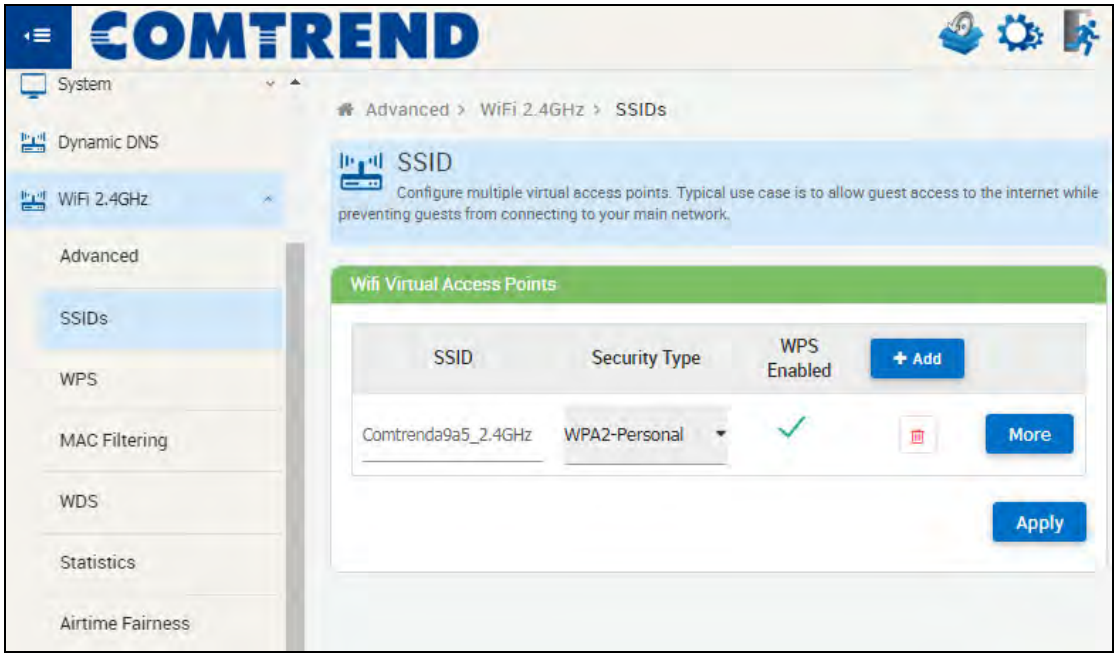
Select number of antennas; 1 or 2.

WMM PS

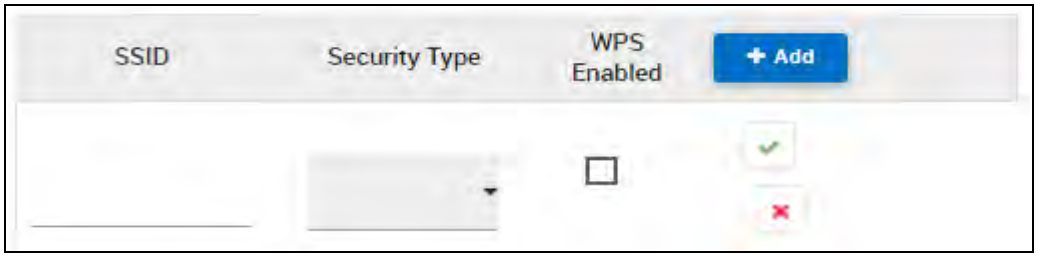
Enabled by default.

5.6.2 SSIDs

Configure multiple virtual access points. Typical use is to allow guest access to the internet while preventing guests from connecting to your main network.



Click the **button to display the following.**



The settings shown above are described below.

SSID

2.4G SSID.

Security Type

Select the security type from the drop-down menu; WEP, WPA1 or WPA2.

WPS Enabled

Tick the box to enable.

Click the More button to display the following.

The settings shown above are described below.

Rekey Interval

3600 seconds by default.

Passphrase

The password.

AP Isolation

Enable/Disable AP isolation.

Max Connected STAs

The maximum number of STAs that can be connected.

WMM-PS

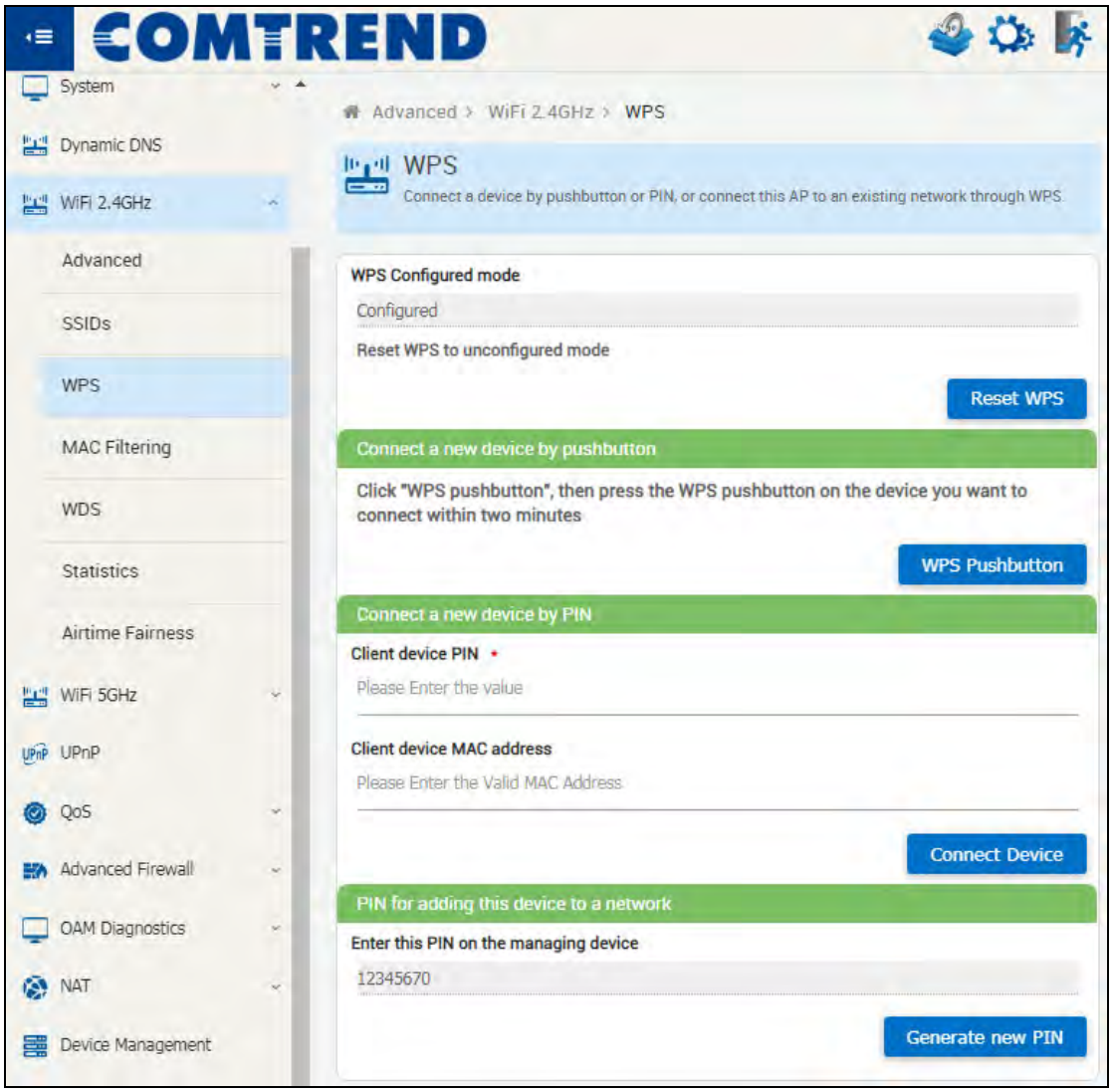
Enable/disable WMM power save.

Bridge Name

WiFi Bridge Interface Name.

5.6.3 WPS

Connect a device by pushbutton or PIN, or connect this AP to an existing network through WPS.



Click the **Reset WPS** button to reset WPS to Unconfigured mode.

Click the **WPS Pushbutton** button, then press the WPS pushbutton on the device you want to connect within two minutes.

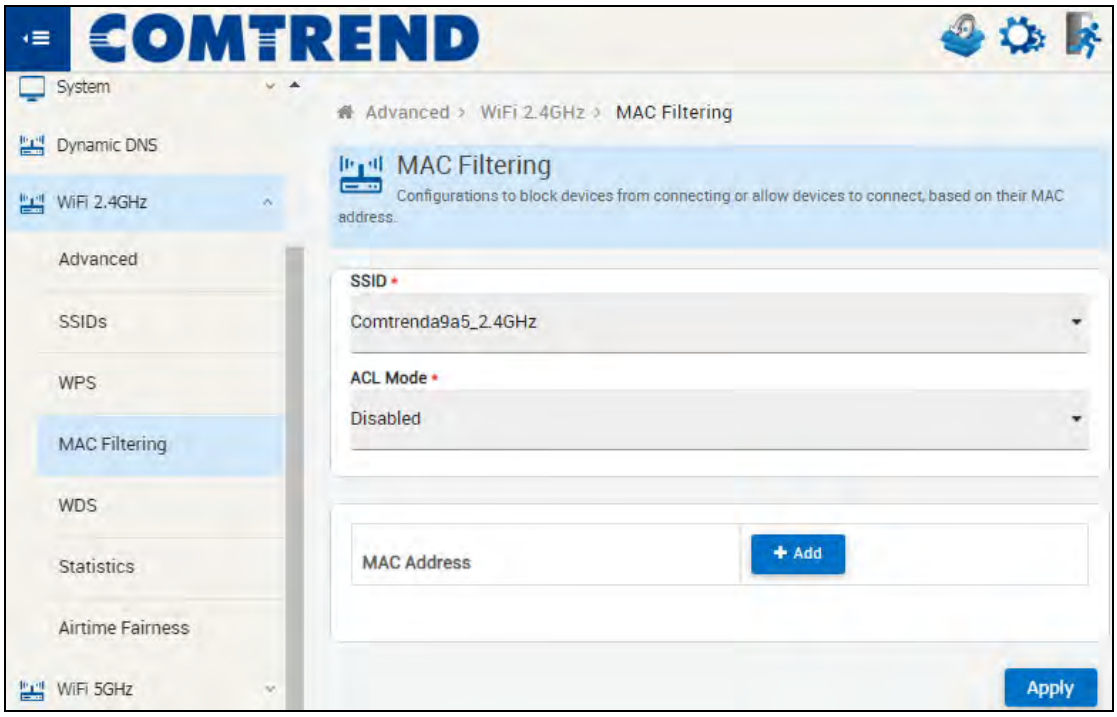
To connect a new device by PIN (Personal Identification Number), input the Client device PIN and Client device MAC address, then click the **Connect Device** button.

To add this device to a network, enter the PIN in the box on the managing device.

To create a new PIN, Click the Generate new PIN button.

5.6.4 MAC Filtering

Configurations to block devices from connecting or allow devices to connect, based on their MAC address.



The settings shown above are described below.

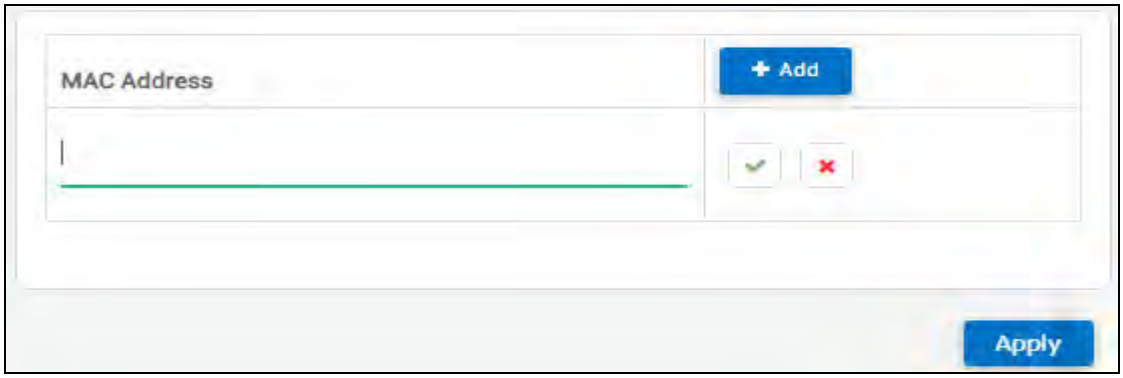
SSID

2.4G SSID.

ACL Mode

Select the access control list mode from the drop-down menu.

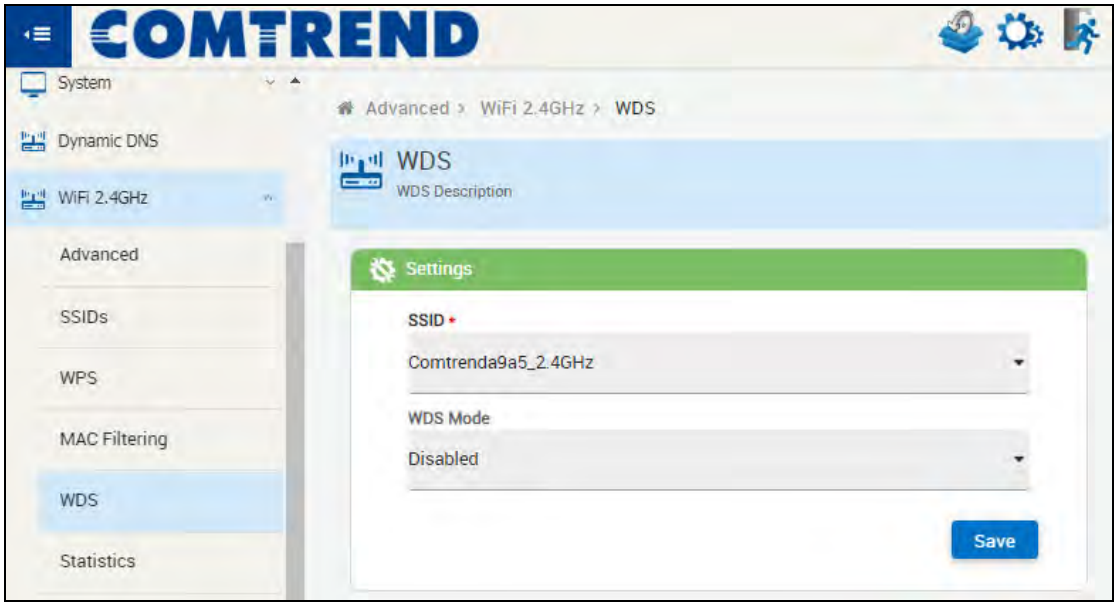
To add a filter, click the + Add button to display the following.



Input the MAC address and click the ✓ or ✗ box to allow or deny.

5.6.5 WDS

Wireless Distribution System.



The settings shown above are described below.

SSID

2.4G Wi-Fi SSID.

WDS Mode

WDS mode setting:

Disabled

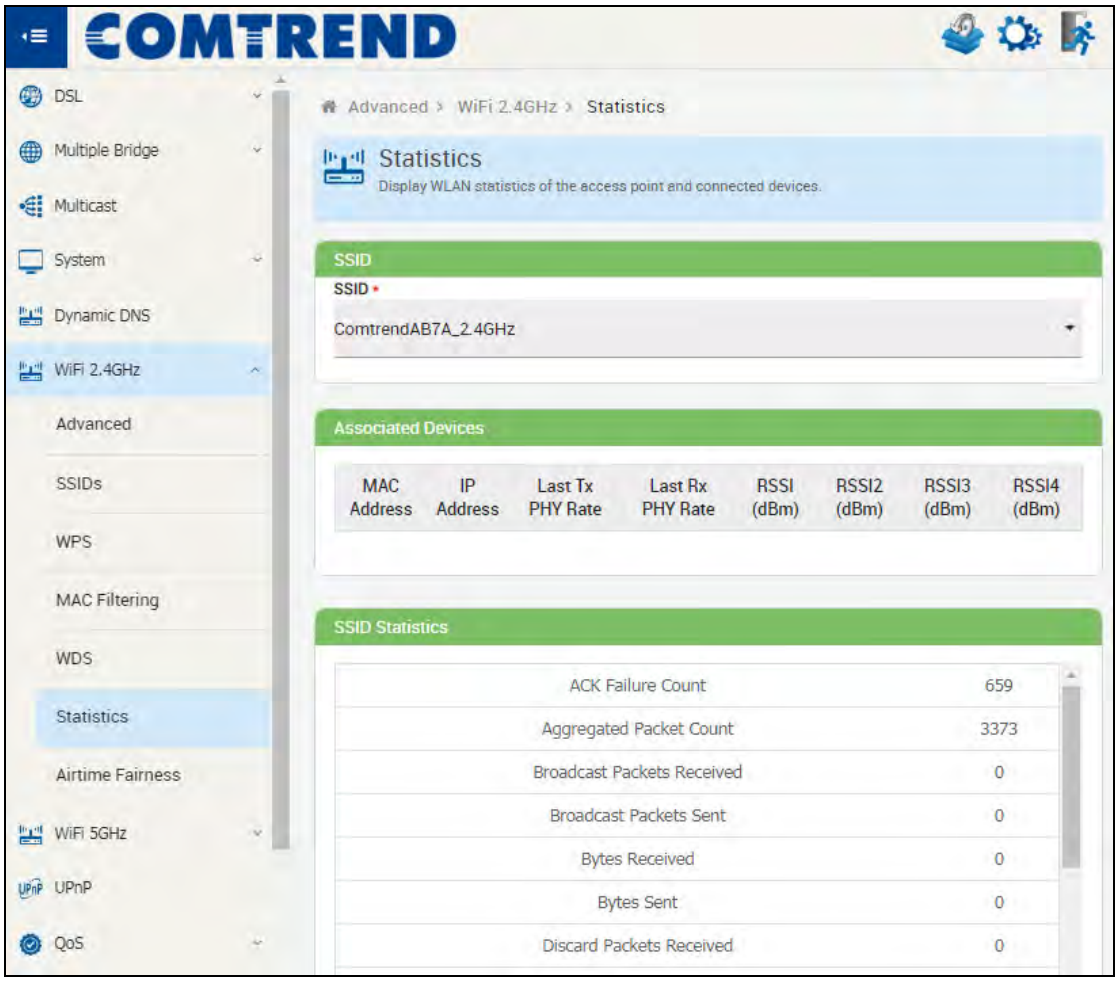
Legacy (Just support 802.11g with WEP)

Hybrid (Support both AP and WDS functions.)

Click the Save button to save the entry.

5.6.6 Statistics

Displays WLAN statistics of the access point and connected devices.



The settings shown above are described below.

SSID

2.4G Wi-Fi SSID.

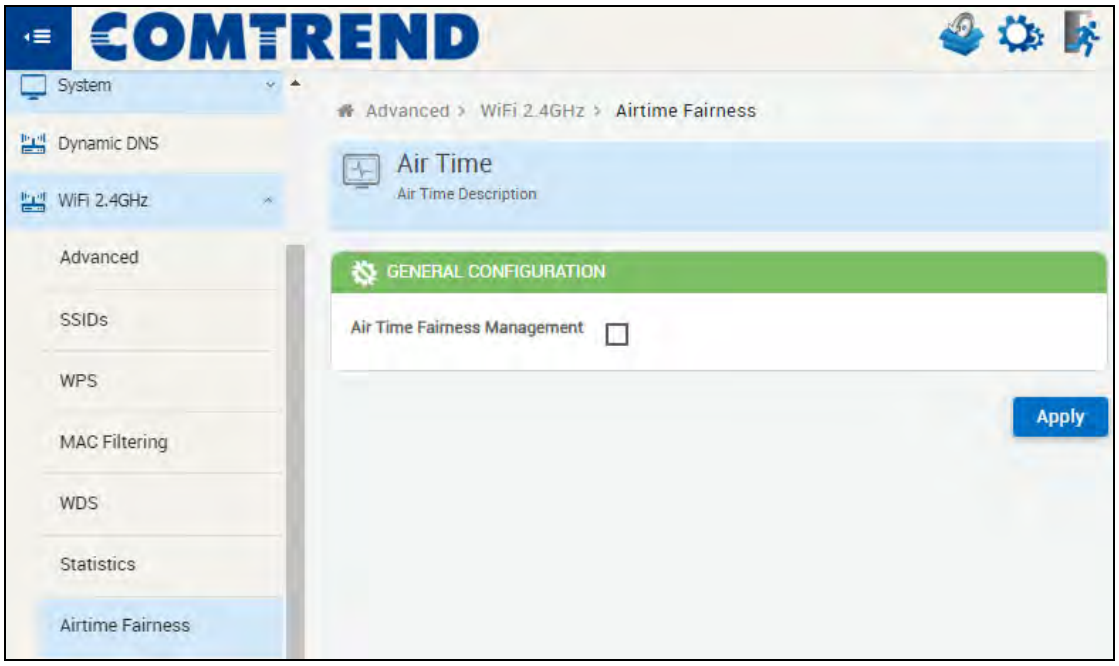
Associated Devices

Heading	Description
MAC Address	MAC address of the STA
IP Address	IP address of the STA
Last Tx PHY Rate	Tx PHY Rate of the Wi-Fi connection
Last Rx PHY Rate	Rx PHY Rate of the Wi-Fi connection
RSSI (dBm) RSSI2 (dBm) RSSI3 (dBm) RSSI4 (dBm)	Shows RSSI3 and RSSI4 for two antennas

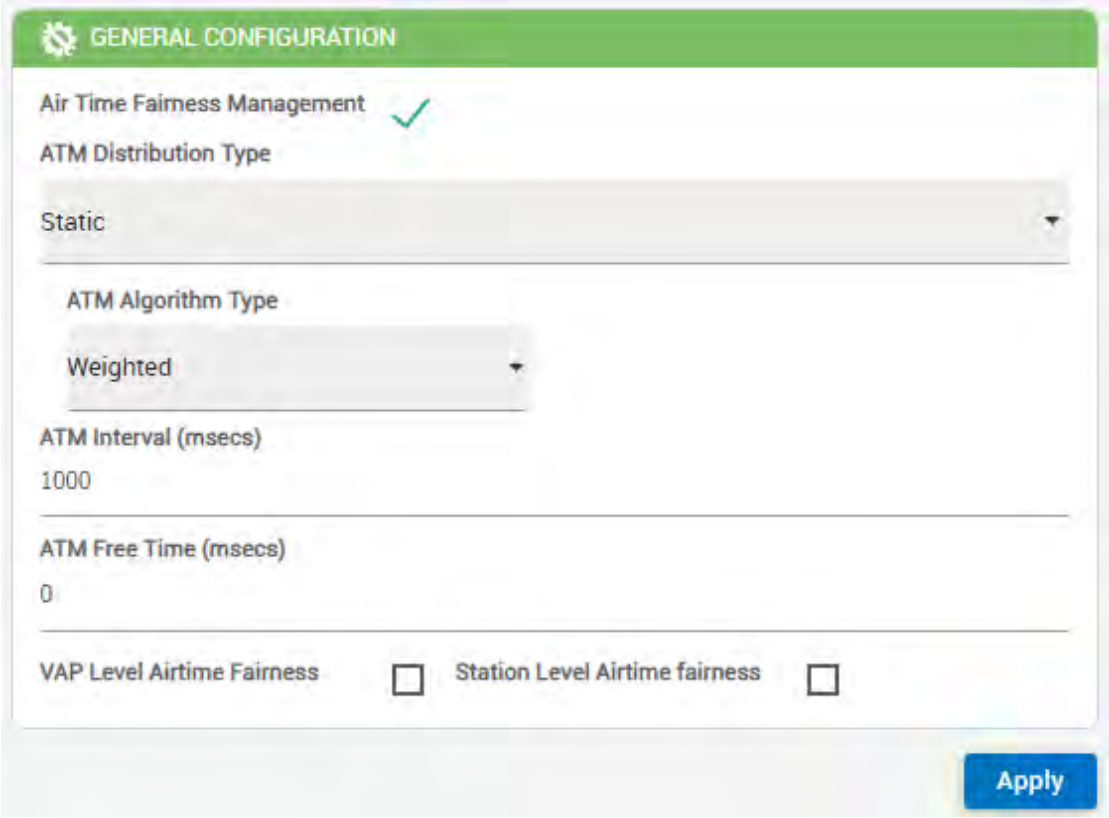
SSID Statistics

Heading	Description
ACK Failure Count	Number of ACK Failure Count
Aggregated Packet Count	Number of Aggregated Packet Count
Broadcast Packets Received	Number of Broadcast Packets Received
Broadcast Packets Sent	Number of Broadcast Packets Sent
Bytes Received	Number of Bytes Received
Bytes Sent	Number of Bytes Sent
Discard Packets Received	Number of Discard Packets Received
Discard Packets Sent	Number of Discard Packets Sent
Errors Received	Number of Errors Received
Packets not transmitted due to error	Number of Packets not transmitted due to error
Failed Retransmission Count	Number of Failed Retransmission Count
Multicast Packets Received	Number of Multicast Packets Received
Multicast Packets Sent	Number of Multicast Packets Sent
Multiple Retry Count	Number of Multiple Retry Count
Packets Received	Number of Packets Received
Packets Sent	Number of Packets Sent
Retransmitted packets	Number of Retransmitted packets
Retry Count	Number of Retry Count
Unicast Packets Received	Number of Unicast Packets Received
Unicast Packets Sent	Number of Unicast Packets Sent

5.6.7 Airtime Fairness



Check the checkbox ☐ to display the following.



Click the **Apply** button to enable airtime fairness for varied wireless clients.

The settings shown above are described below.

ATM Distribution Type

- Static: If an STA does not fully use its grant, do not pass it to other STAs.
- Dynamic: If an STA does not fully use its grant, pass the remaining grant to other STAs.

ATM Algorithm Type

- Global: The grant(weight) allocated to STAs is equally divided between all STAs.
- Weighted: Each STA or SSID (VAP) has a predefined weight in % of the total airtime. Weights can be:
  - Per AC (Access Category)
  - Per STA
  - Per SSID
  - Per SSID, then per STA

ATM Interval (msecs)

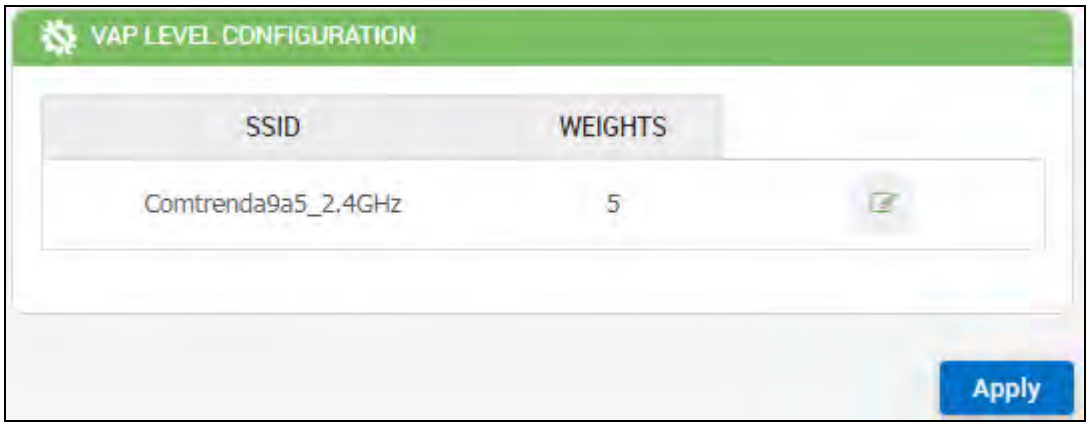
This is basic time frame in milliseconds that is used for ATF calculations.

ATM Free Time (msecs)

This is basic time frame in milliseconds that is subtracted from the ATM Interval. Default free time interval value is 0ms.

VAP Level Airtime Fairness

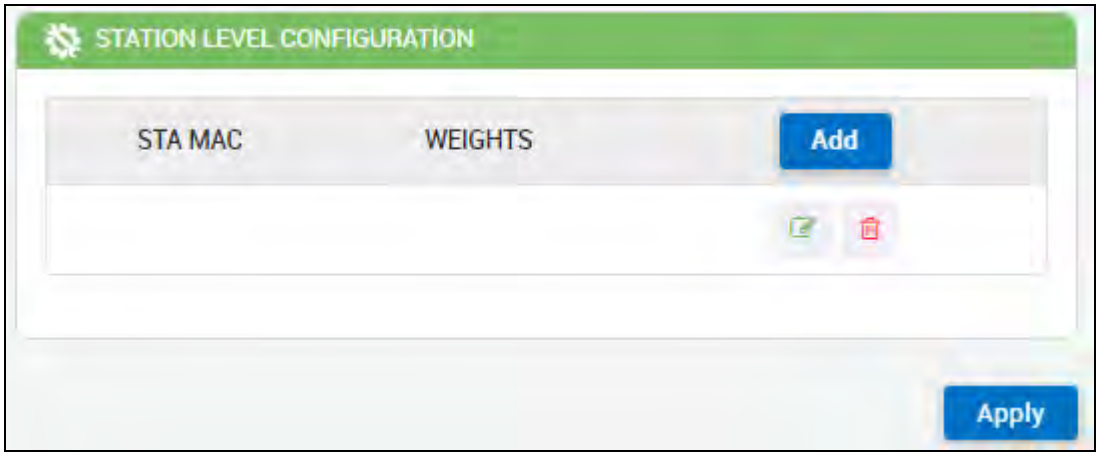
Check the checkbox ☐ to display the following.



Then click the icon to edit the entry. Click the Apply button to apply your changes.

Station Level Airtime Fairness

Check the checkbox ☐ to display the following.



Click the Add button to add an entry.

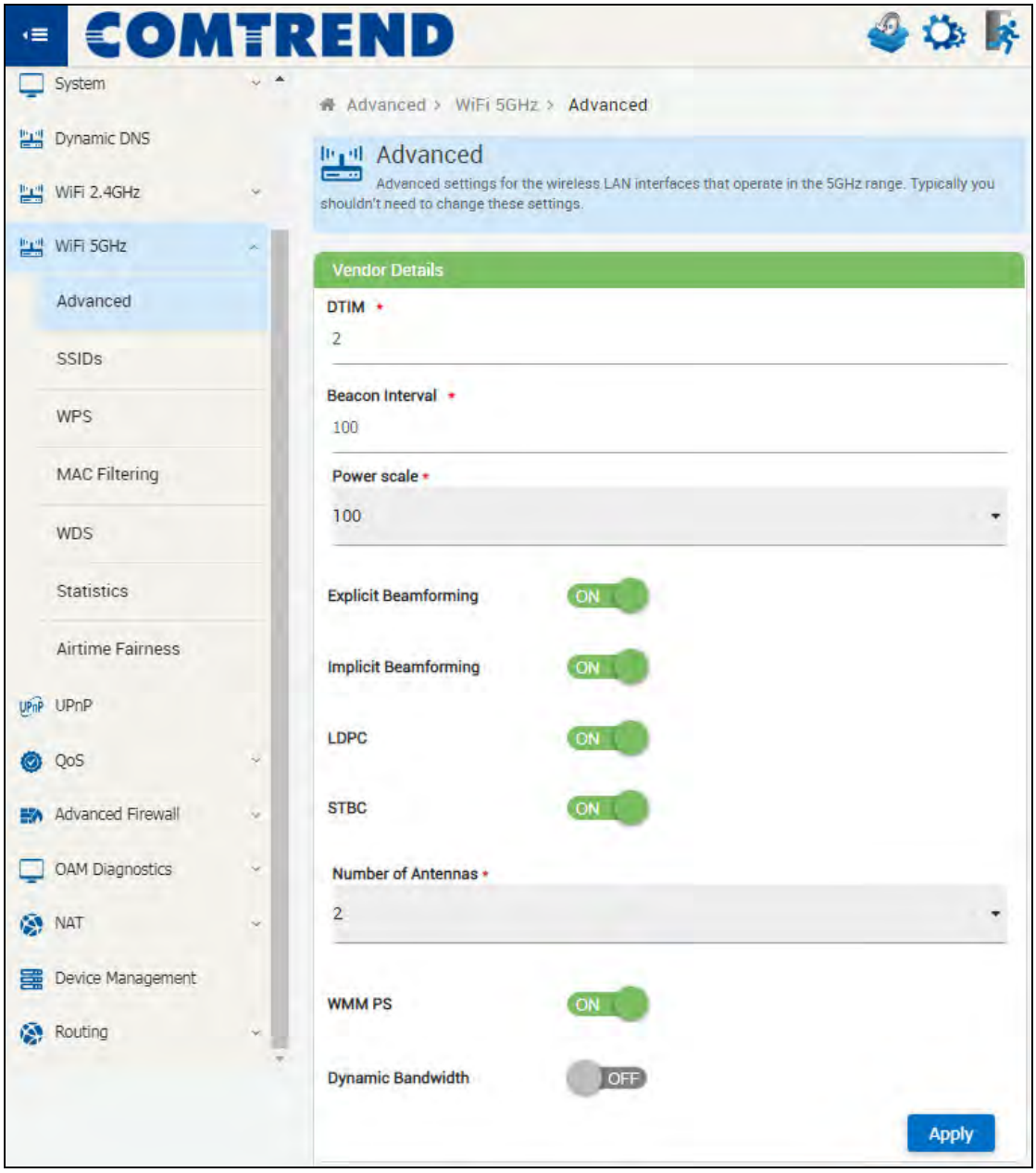
Then click the icon to edit the entry. Click the Apply button to apply your changes.

If required, click the icon to delete an entry.

5.7 WiFi 5GHz

5.7.1 Advanced

Advanced settings for the wireless LAN interfaces that operate in the 2.4GHz range. Typically you shouldn't need to change these settings.



The settings shown above are described below.

DTIM

A value between 1~255.

Beacon Interval

100 ms by default.

Power Scale

12/25/50/100 and 100 by default.

Explicit Beamforming

Turned on by default.

Implicit Beamforming

Turned on by default.

LDPC

Turned on by default.

STBC

Turned on by default.

Number of Antennas

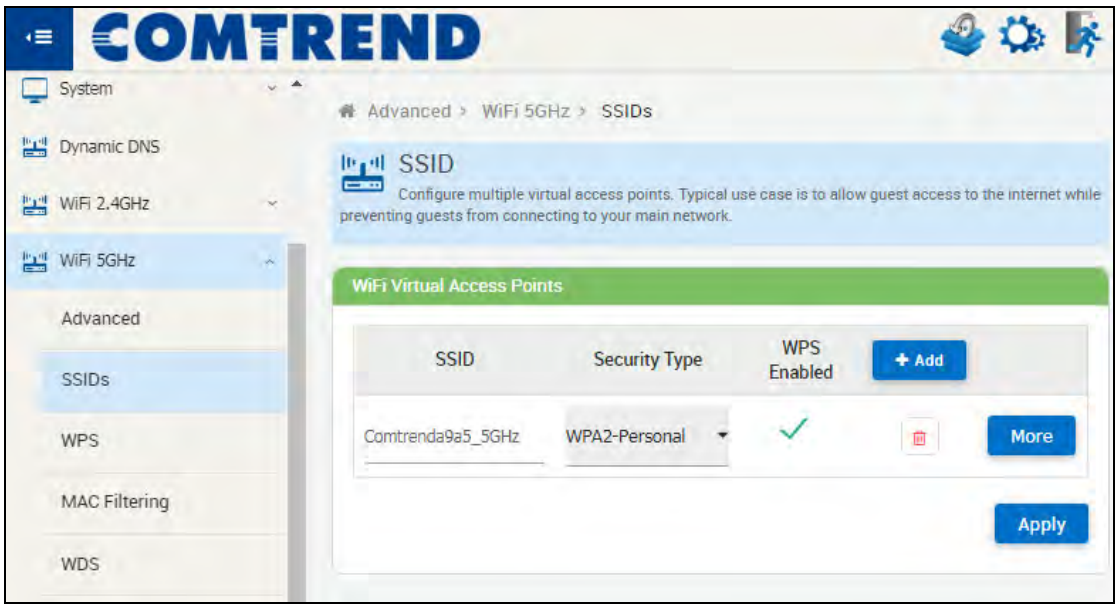
Select number of antennas; 1 or 2.

WMM PS

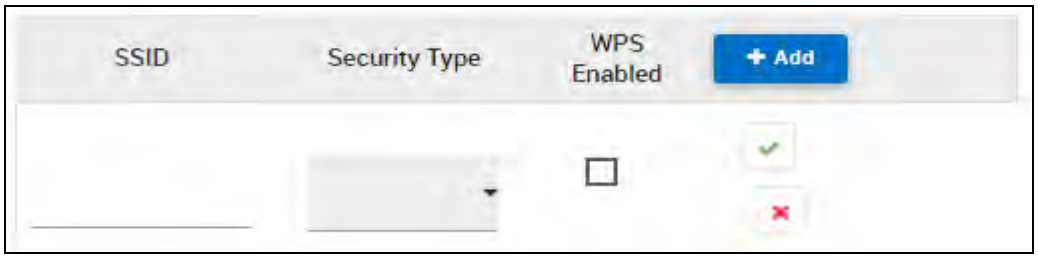
Enabled by default.

5.7.2 SSIDs

Configure multiple virtual access points. Typical use case is to allow guest access to the internet while preventing guests from connecting to your main network.



Click the **button to display the following.**



The settings shown above are described below.

SSID

2.4G SSID.

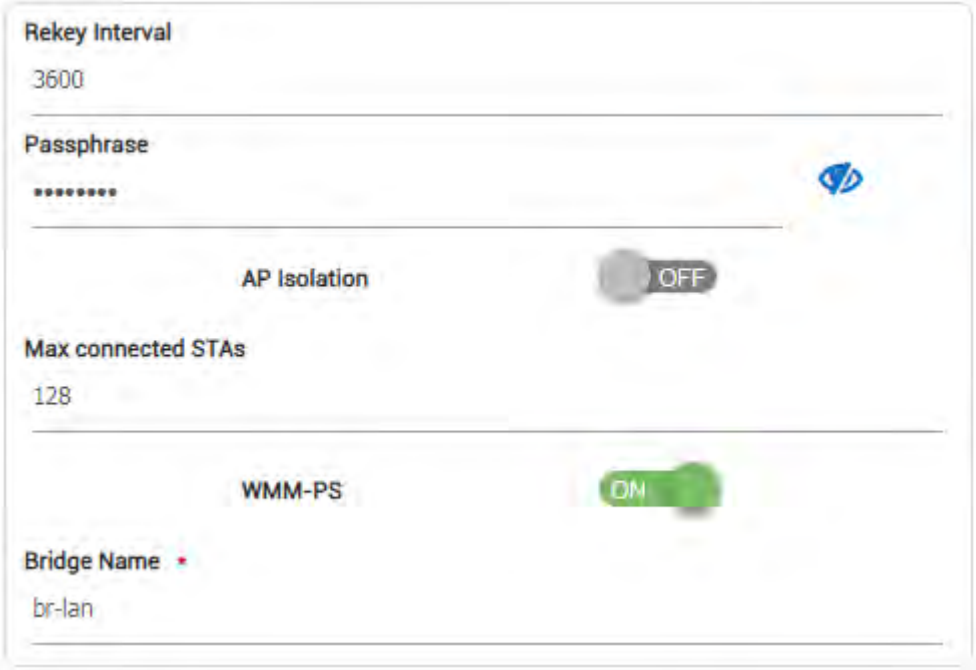
Security Type

Select the security type from the drop-down menu; WEP, WPA1 or WPA2.

WPS Enabled

Tick the box to enable.

Click the More button to display the following.



The settings shown above are described below.

Rekey Interval

3600 seconds by default.

Passphrase

The password.

AP Isolation

Enable/Disable AP isolation.

Max Connected STAs

The maximum number of STAs that can be connected.

WMM-PS

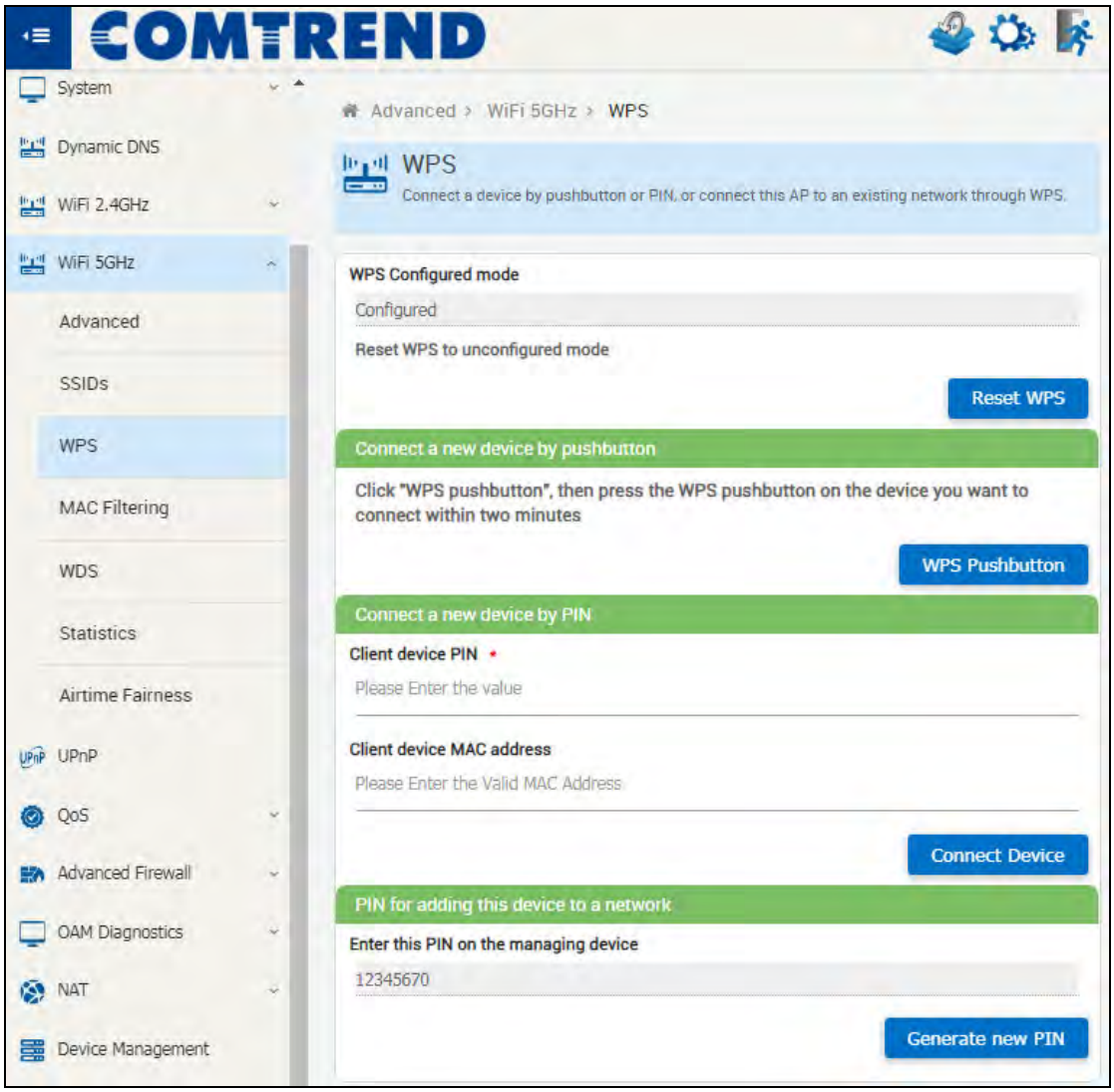
Enable/disable WMM power save.

Bridge Name

WiFi Bridge Interface Name.

5.7.3 WPS

Connect a device by pushbutton or PIN, or connect this AP to an existing network through WPS.



Click the **Reset WPS** button to reset WPS to Unconfigured mode.

Click the **WPS Pushbutton** button, then press the WPS pushbutton on the device you want to connect within two minutes.

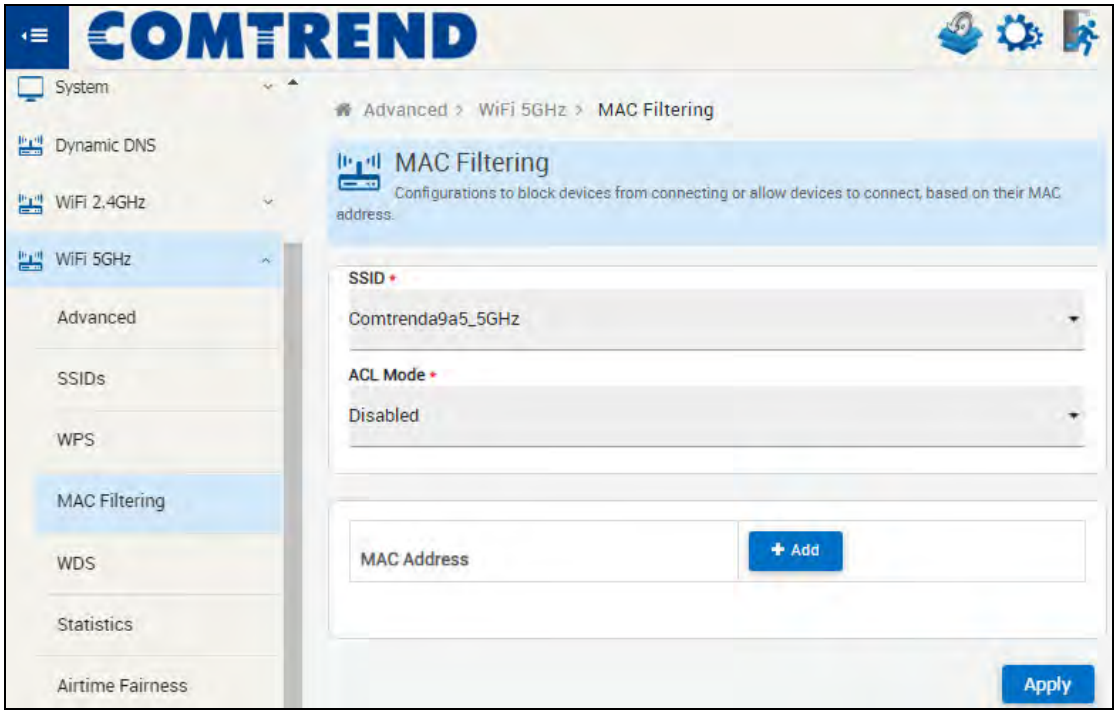
To connect a new device by PIN (Personal Identification Number), input the Client device PIN and Client device MAC address, then click the **Connect Device** button.

To add this device to a network, enter the PIN in the box on the managing device.

To create a new PIN, Click the Generate new PIN button.

5.7.4 MAC Flitering

Configurations to block devices from connecting or allow devices to connect, based on their MAC address.



The settings shown above are described below.

SSID

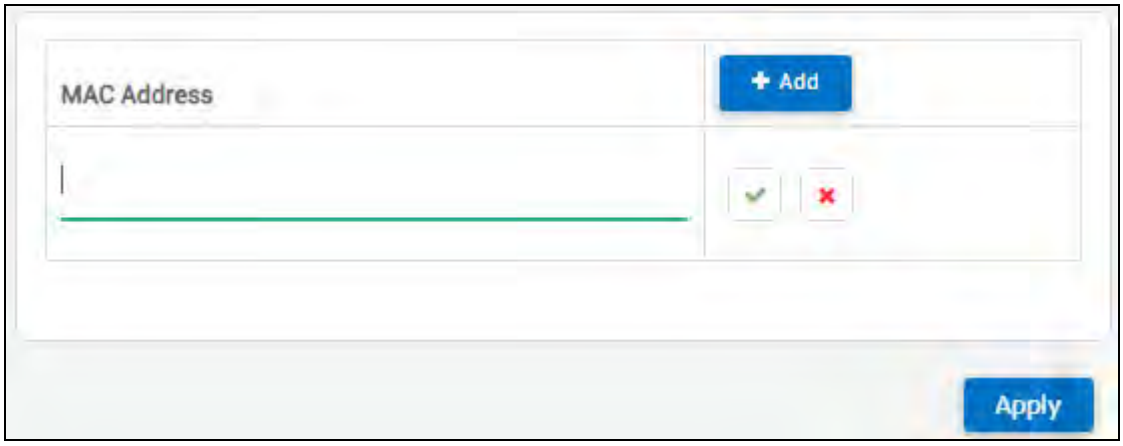
2.4G SSID.

ACL Mode

Select the access control list mode from the drop-down menu.

To add a filter, click the

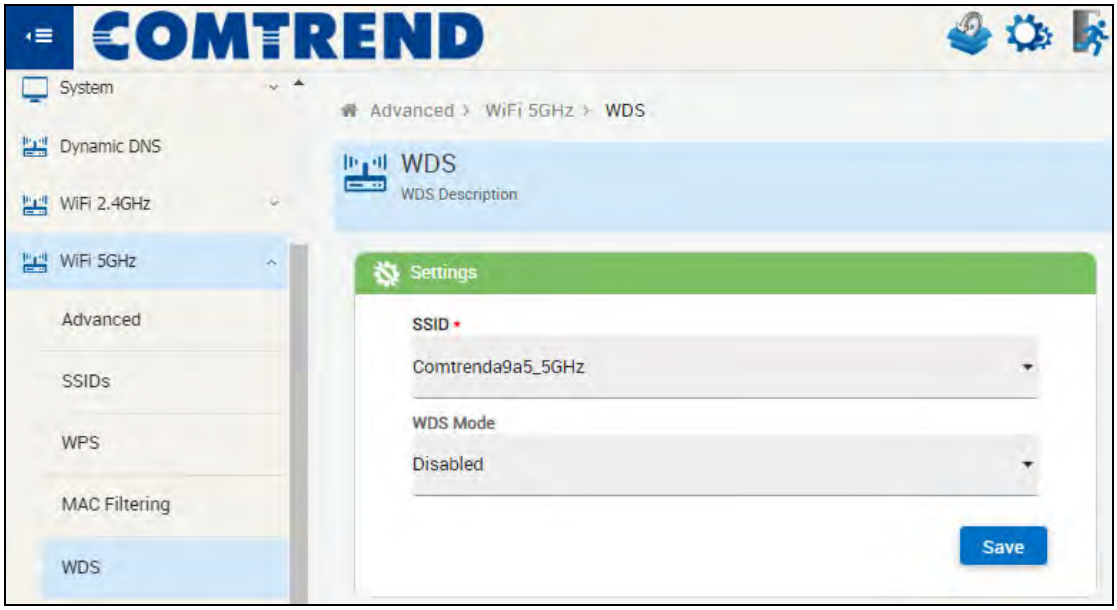
button to display the following.



Input the MAC address and click the or box to allow or deny.

5.7.5 WDS

Wireless Distribution System.



The settings shown above are described below.

SSID

2.4G Wi-Fi SSID.

WDS Mode

WDS mode setting:

Disabled

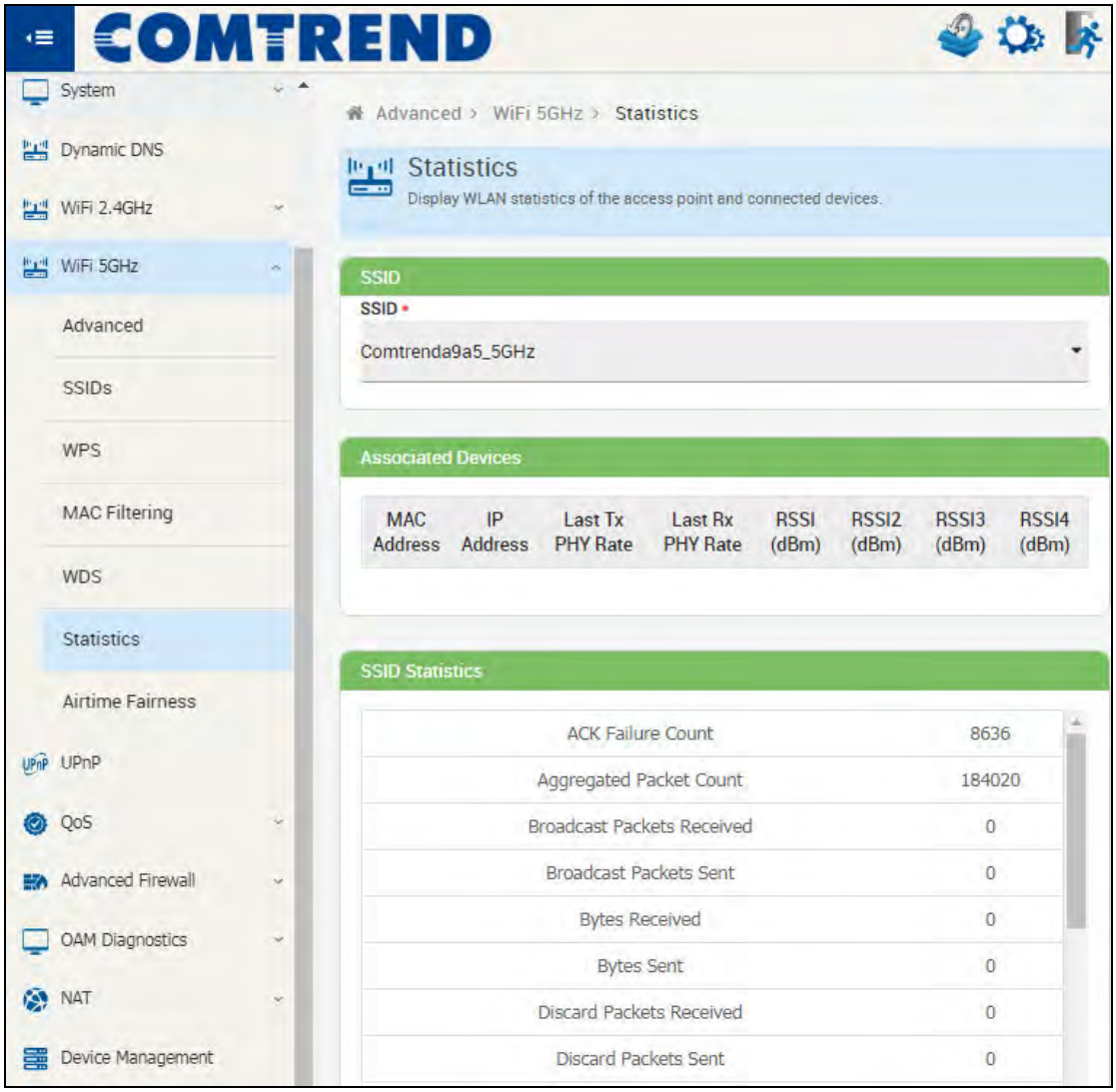
Legacy (Just support 802.11g with WEP)

Hybrid (Support both AP and WDS functions.)

Click the Save button to save the entry.

5.7.6 Statistics

Displays WLAN statistics of the access point and connected devices.



The settings shown above are described below.

SSID

5G Wi-Fi SSID.

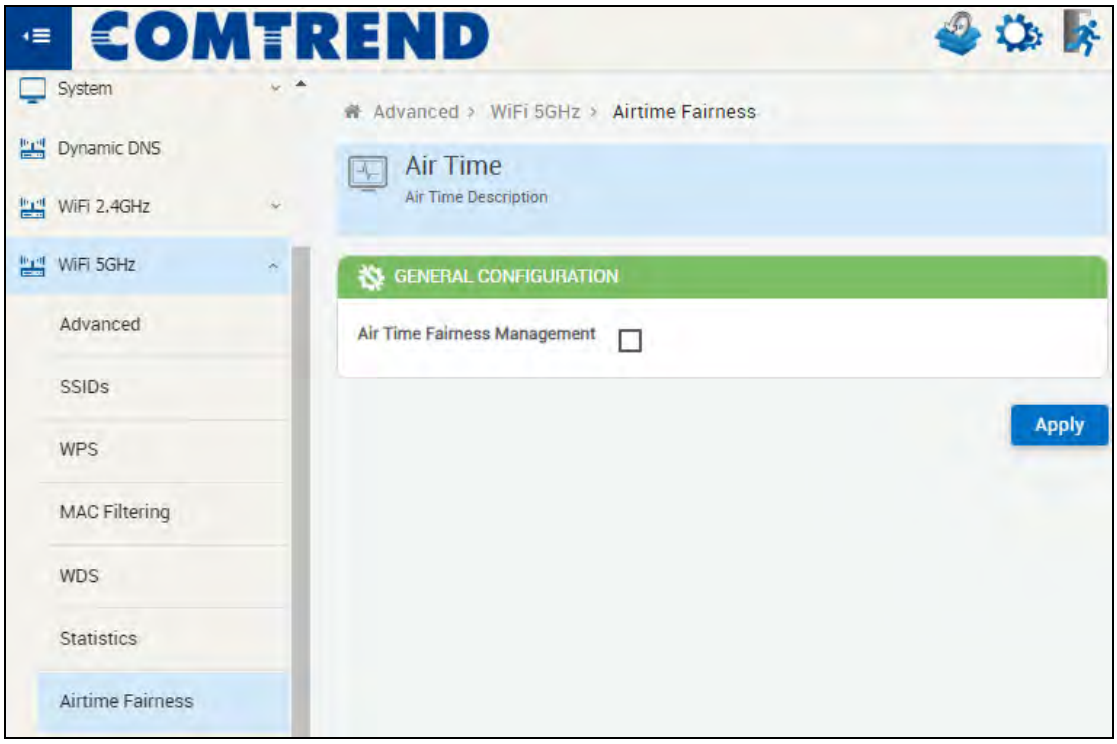
Associated Devices

Heading	Description
MAC Address	MAC address of the STA
IP Address	IP address of the STA
Last Tx PHY Rate	Tx PHY Rate of the Wi-Fi connection.
Last Rx PHY Rate	Rx PHY Rate of the Wi-Fi connection.
RSSI (dBm) RSSI2 (dBm) RSSI3 (dBm) RSSI4 (dBm)	Shows RSSI3 and RSSI4 for two antennas.

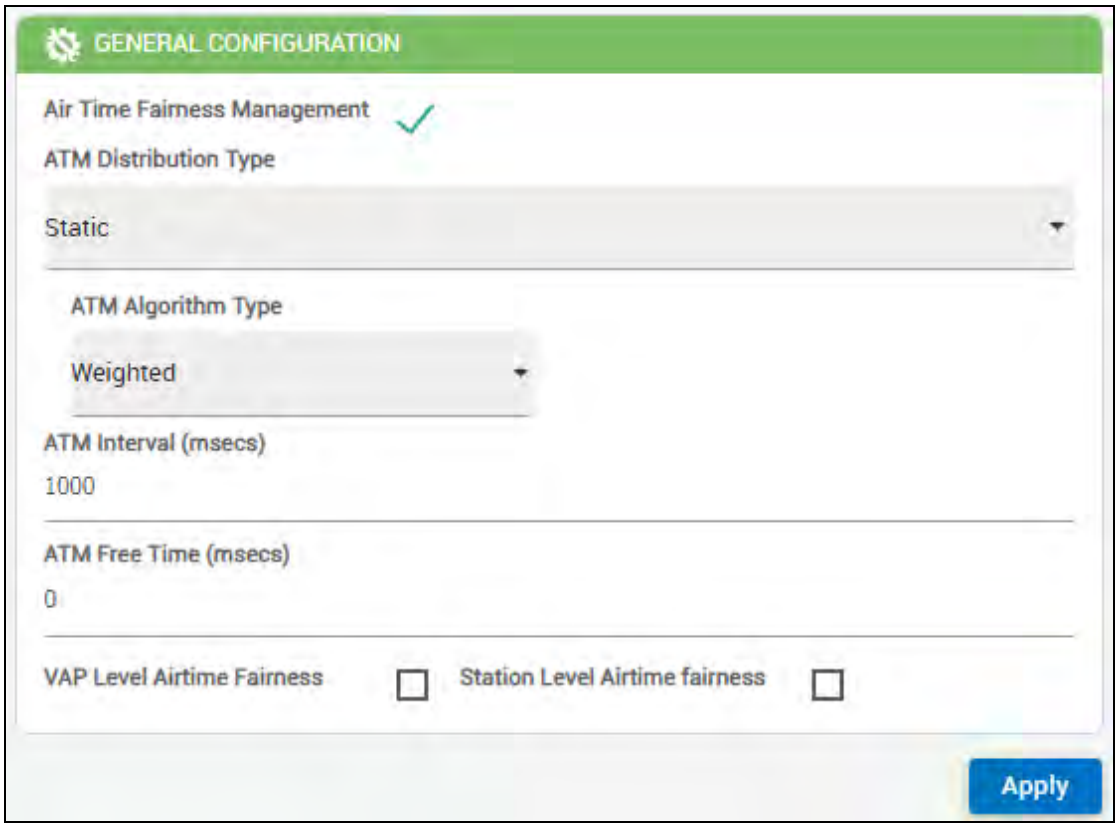
SSID Statistics

Heading	Description
ACK Failure Count	Number of ACK Failure Count
Aggregated Packet Count	Number of Aggregated Packet Count
Broadcast Packets Received	Number of Broadcast Packets Received
Broadcast Packets Sent	Number of Broadcast Packets Sent
Bytes Received	Number of Bytes Received
Bytes Sent	Number of Bytes Sent
Discard Packets Received	Number of Discard Packets Received
Discard Packets Sent	Number of Discard Packets Sent
Errors Received	Number of Errors Received
Packets not transmitted due to error	Number of Packets not transmitted due to error
Failed Retransmission Count	Number of Failed Retransmission Count
Multicast Packets Received	Number of Multicast Packets Received
Multicast Packets Sent	Number of Multicast Packets Sent
Multiple Retry Count	Number of Multiple Retry Count
Packets Received	Number of Packets Received
Packets Sent	Number of Packets Sent
Retransmitted packets	Number of Retransmitted packets
Retry Count	Number of Retry Count
Unicast Packets Received	Number of Unicast Packets Received
Unicast Packets Sent	Number of Unicast Packets Sent

5.7.7 Airtime Fairness



Check the checkbox ☐ to display the following.



Click the Apply button to enable airtime fairness for varied wireless clients.

The settings shown above are described below.

ATM Distribution Type

- Static: If an STA does not fully use its grant, do not pass it to other STAs.
- Dynamic: If an STA does not fully use its grant, pass the remaining grant to other STAs.

ATM Algorithm Type

- Global: The grant(weight) allocated to STAs is equally divided between all STAs.
- Weighted: Each STA or SSID (VAP) has a predefined weight in % of the total airtime. Weights can be:
  - Per AC (Access Category)
  - Per STA
  - Per SSID
  - Per SSID, then per STA

ATM Interval (msecs)
This is basic time frame in milliseconds that is used for ATF calculations.

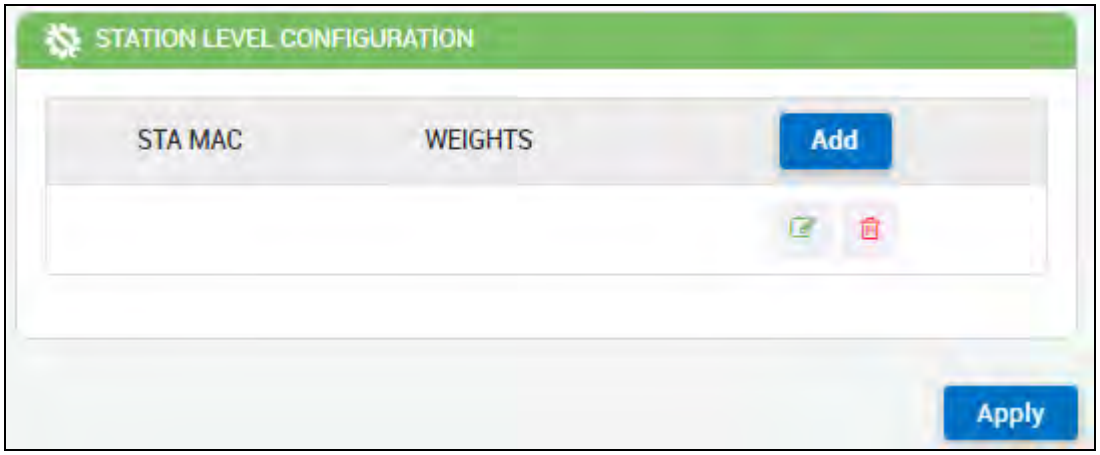
ATM Free Time (msecs)
This is basic time frame in milliseconds that is subtracted from the ATM Interval. Default free time interval value is 0ms.

VAP Level Airtime Fairness
Check the checkbox ☐ to display the following.

Then click the icon to edit the entry. Click the Apply button to apply your changes.

Station Level Airtime Fairness

Check the checkbox ☐ to display the following.

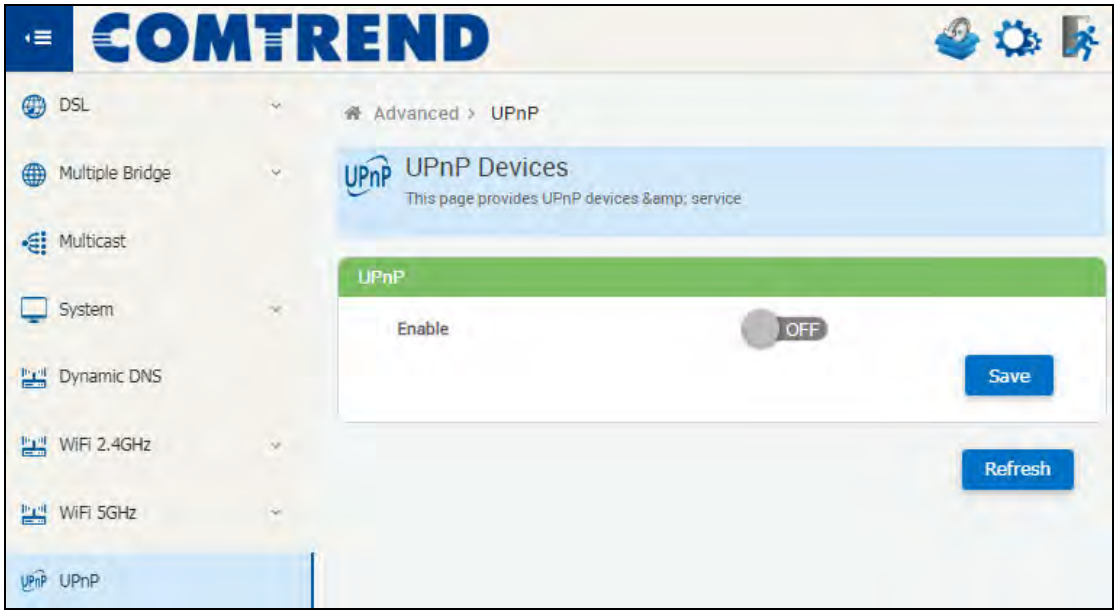


Click the Add button to add an entry.

Then click the icon to edit the entry. Click the Apply button to apply your changes.

If required, click the icon to delete an entry.

5.8 UPnP

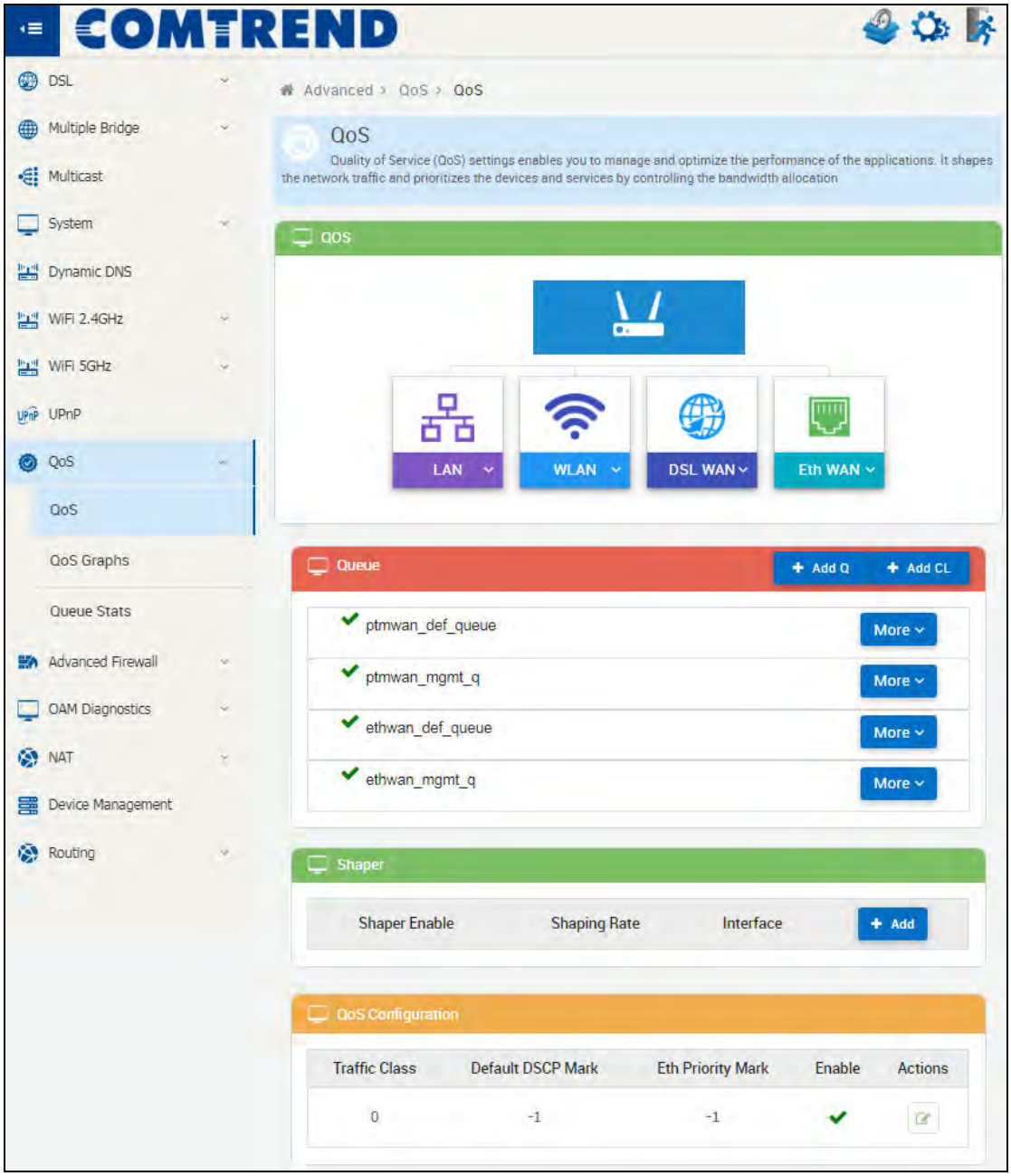


Click the radio button to to enable UPnP protocol and then click the button to save your choice.

Click the button to refresh the screen.

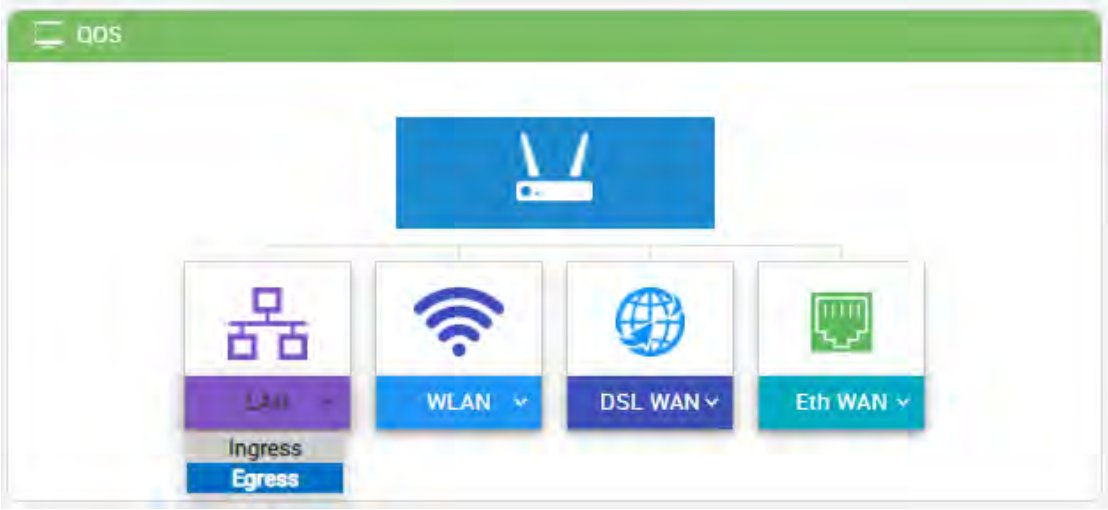
5.9 Quality of Service

Quality of Service (QoS) settings enables you to manage and optimize the performance of the applications. It shapes the network traffic and prioritizes the devices and services by controlling the bandwidth allocation.



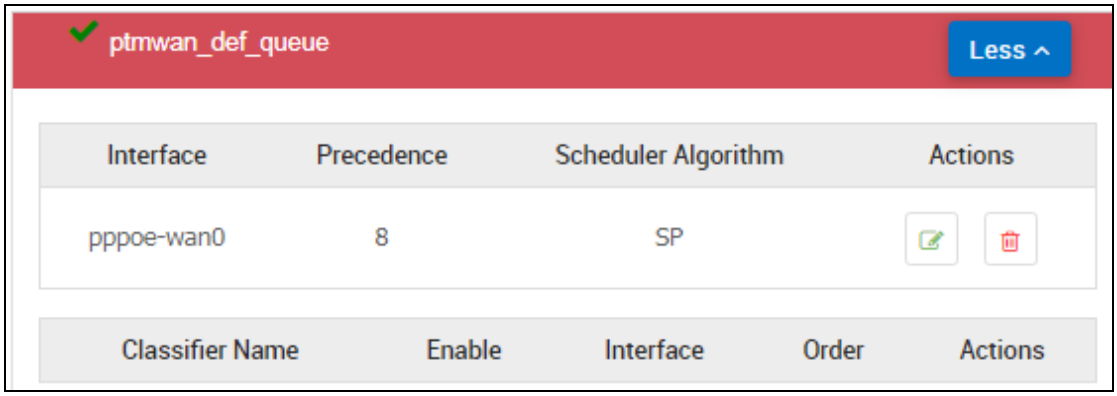
5.9.1 QoS

(QoS) settings enables] you to manage and optimize the performance of the applications. Select Ingress or Egress from each of the drop-down menus – LAN, WLAN, DSL, WAN and Eth WAN.



Click the

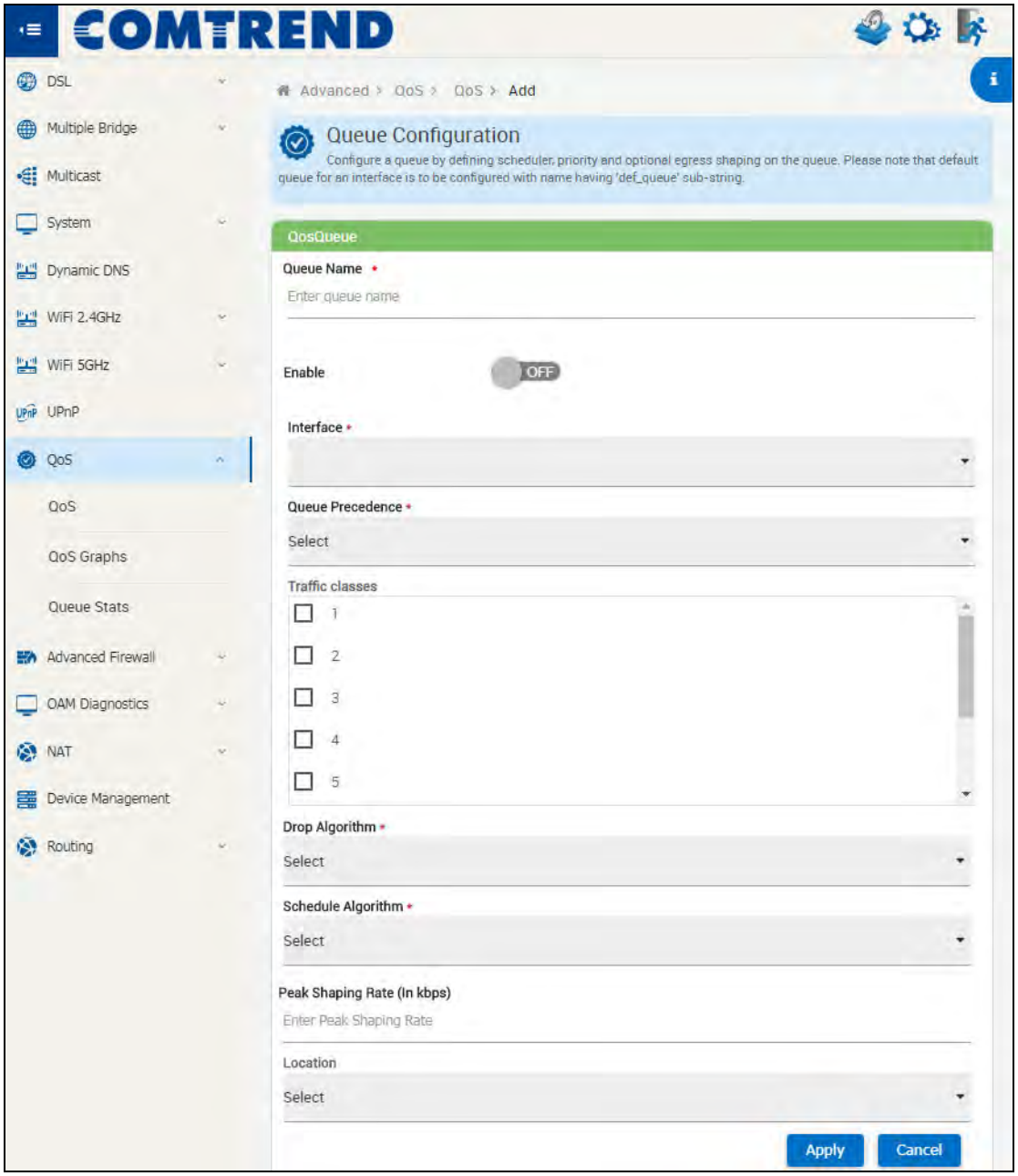
button to see more detail on each entry.



Then click the icon to edit the entry.

If required, click the icon to delete an entry.

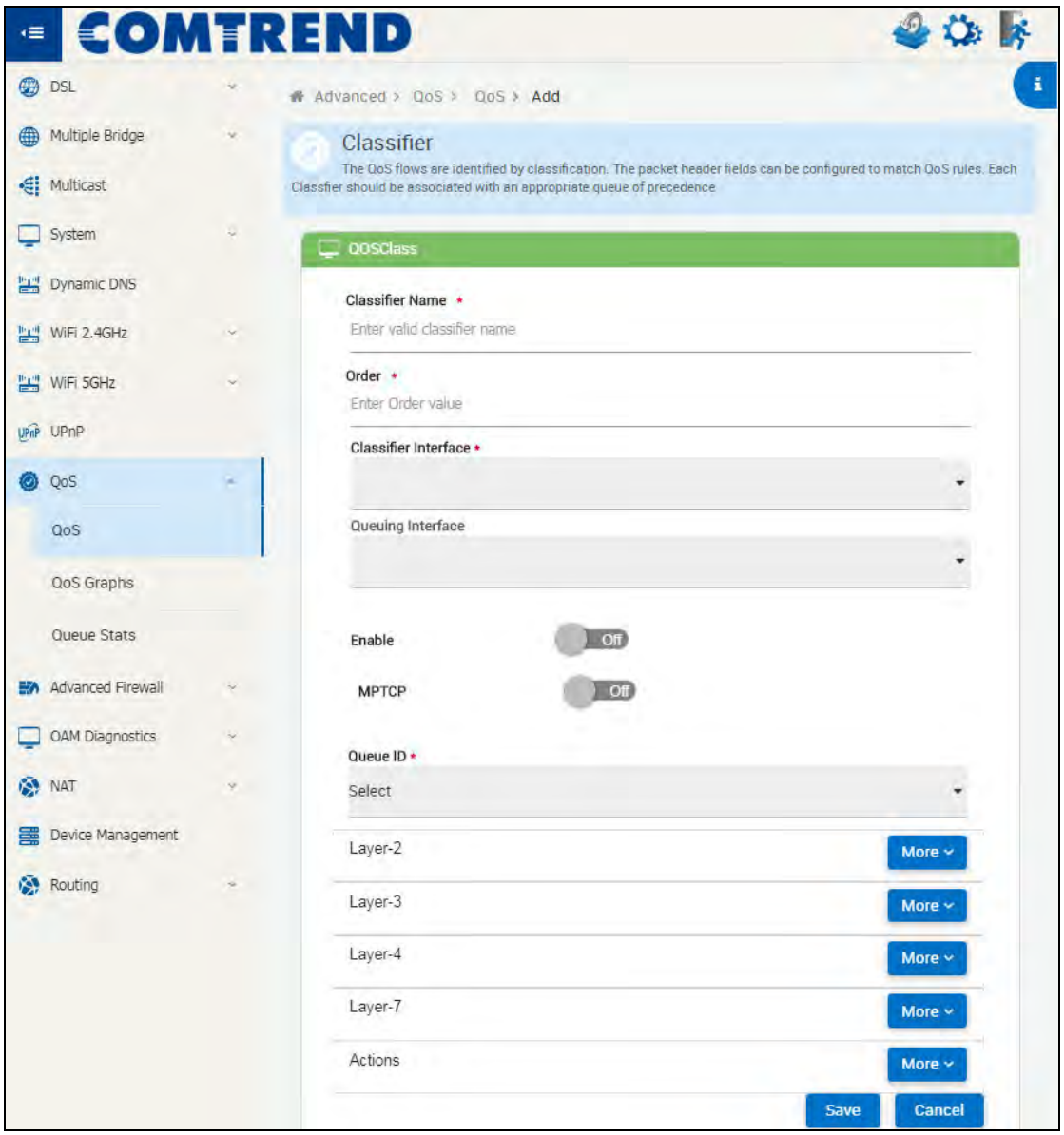
Click the + Add Q button to display the following.



Click the Information icon on the upper right-hand side of this screen for information on Queue Configuration Settings.

Click the

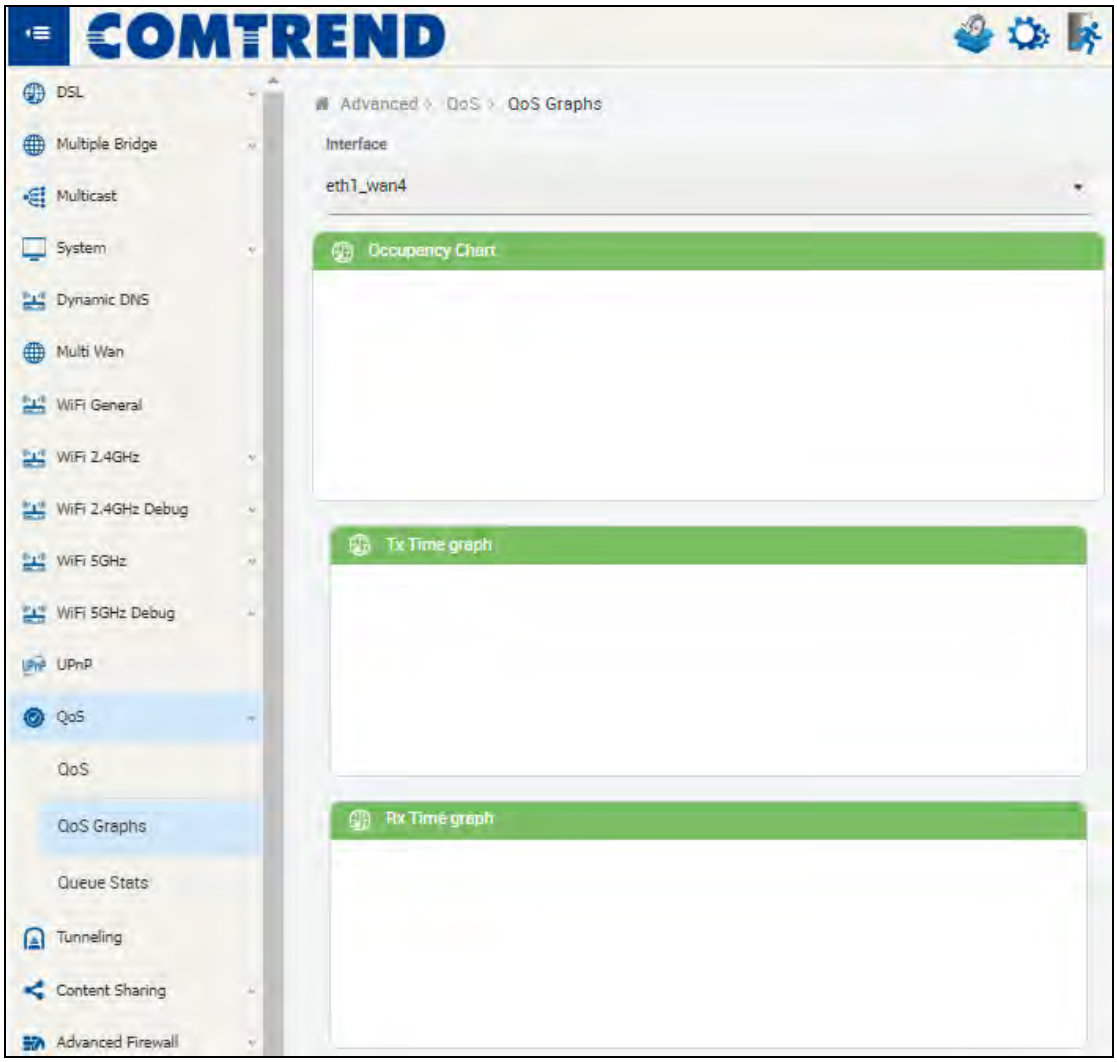
button to display the following.



Click the Information icon on the upper right-hand side of this screen for information on Classifier Settings.

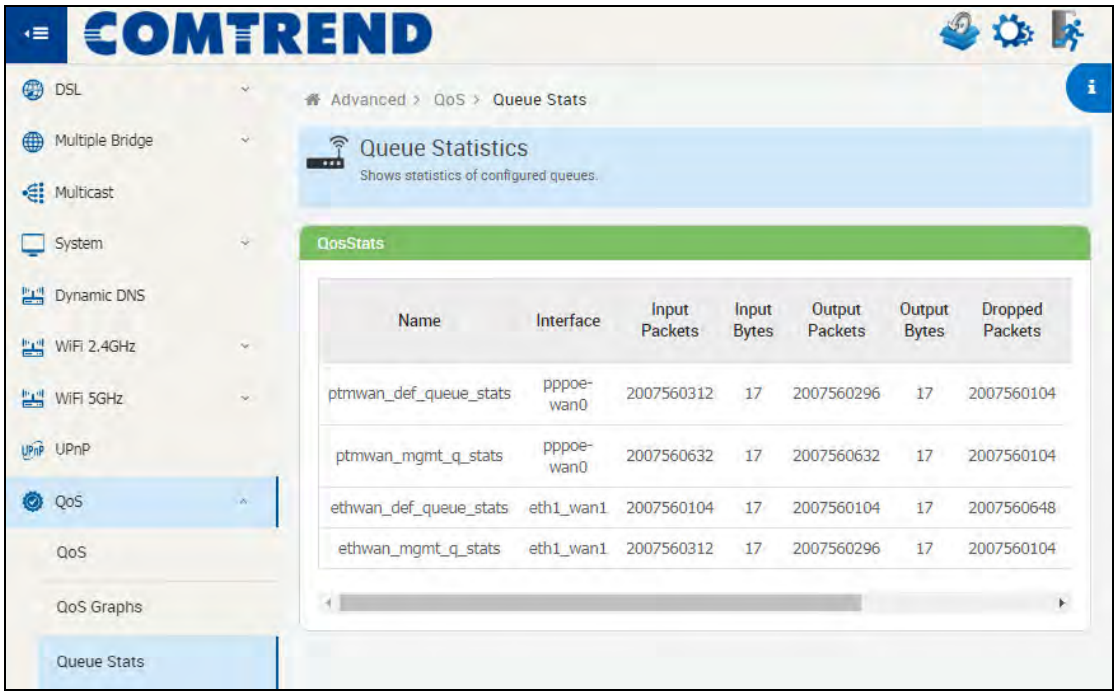
5.9.2 QoS Graphs

This function is not supported on this firmware release.



5.9.3 Queue Stats

Shows the statistics of configured queues.



Click the Information icon on the upper right-hand side of this screen for information on Quque Statistics info.

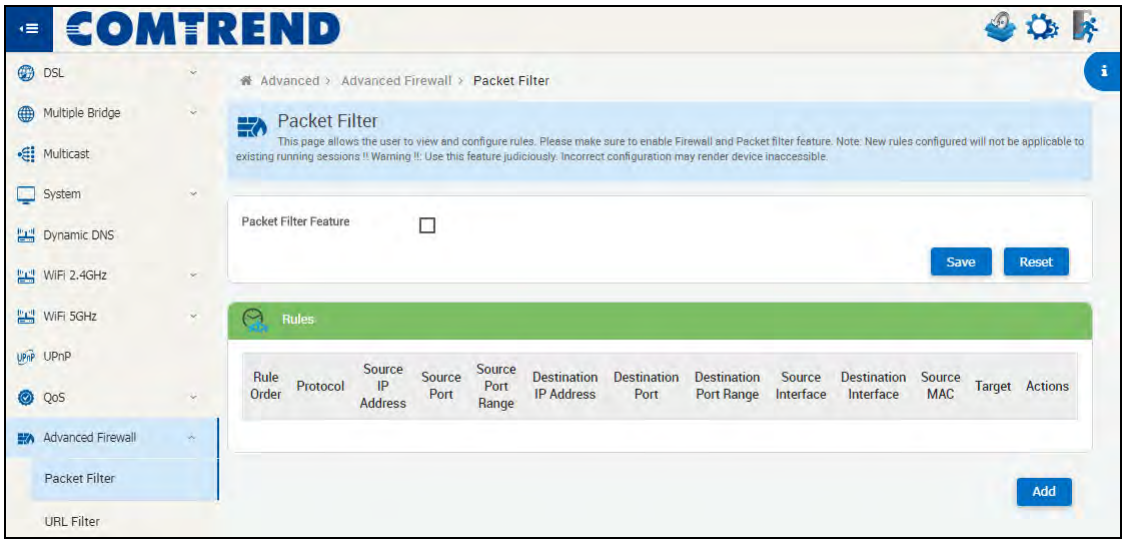
5.10 Advanced Firewall

This page allows the user to view and configure rules. Please make sure to enable Firewall and Packet filter feature.

Note: New rules configured will not be applicable to existing running sessions.

Warning: Use this feature judiciously. Incorrect configuration may render device inaccessible.

5.10.1 Packet Filter

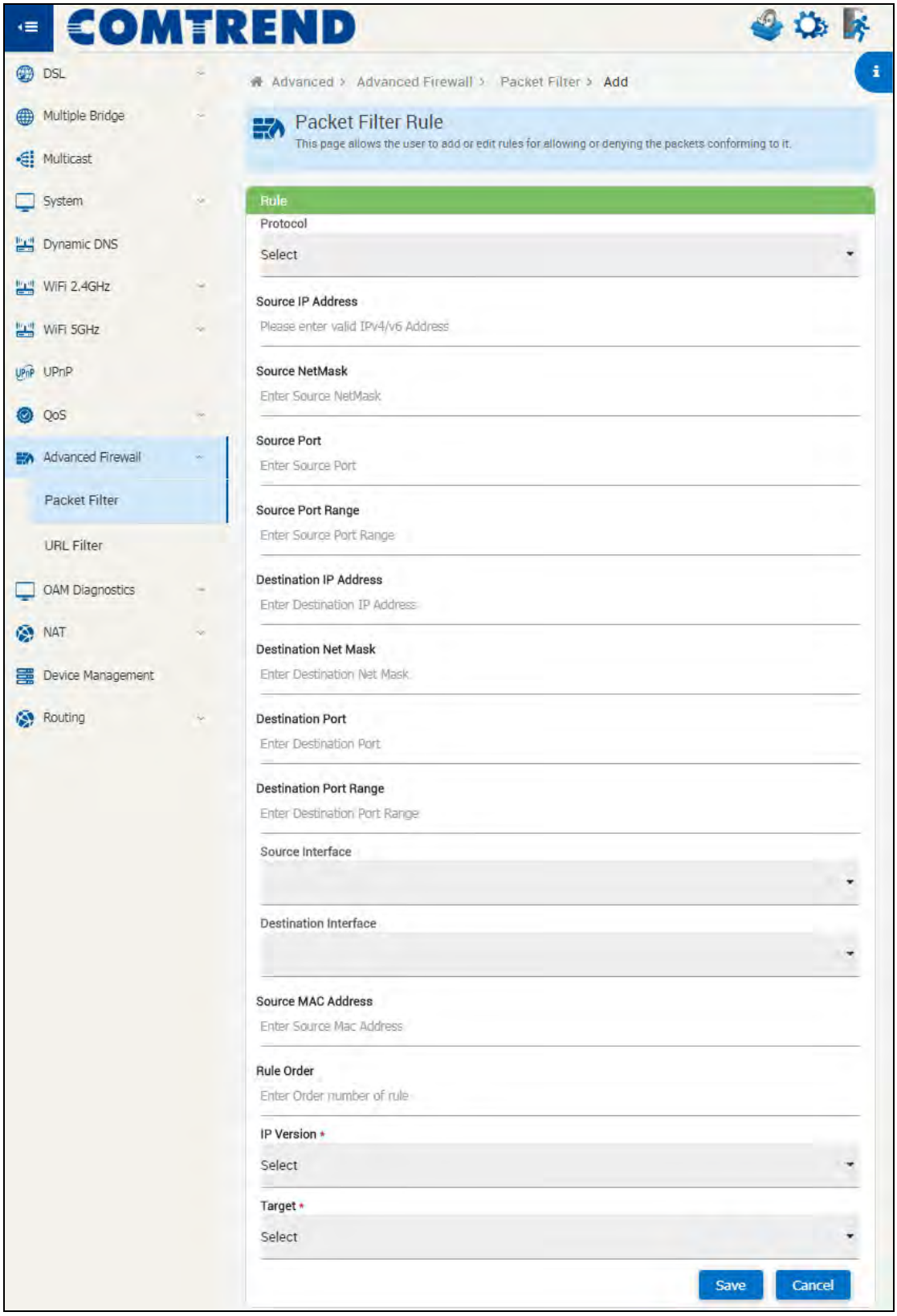


By enabling Packet filter, traffic can be passed or blocked at a network interface based on source and destination addresses, ports, or protocols.

By default packet filter is disabled. To filter the traffic, firewall and packet filter must be enabled and a rule should be added based on source and destination address, ports or protocols.

Click the

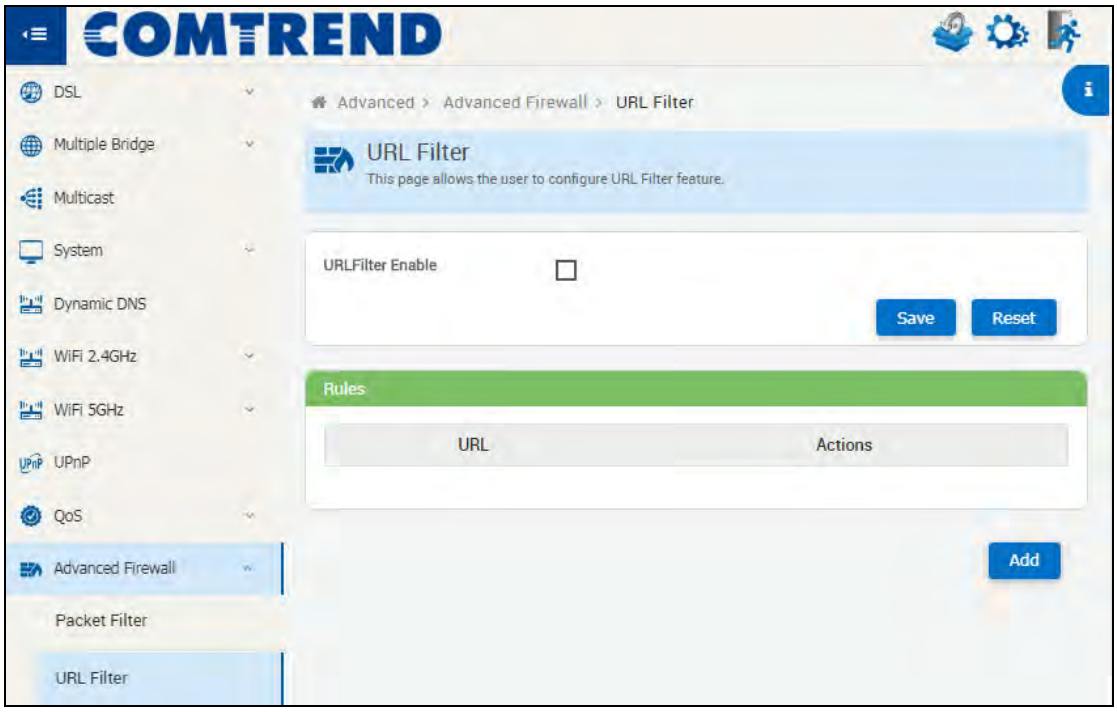
button to display the following.



Click the Information icon on the upper right-hand side of this screen for information on Packet Filter settings.

5.10.2 URL Filter

This page allows the user to configure URL Filter feature.

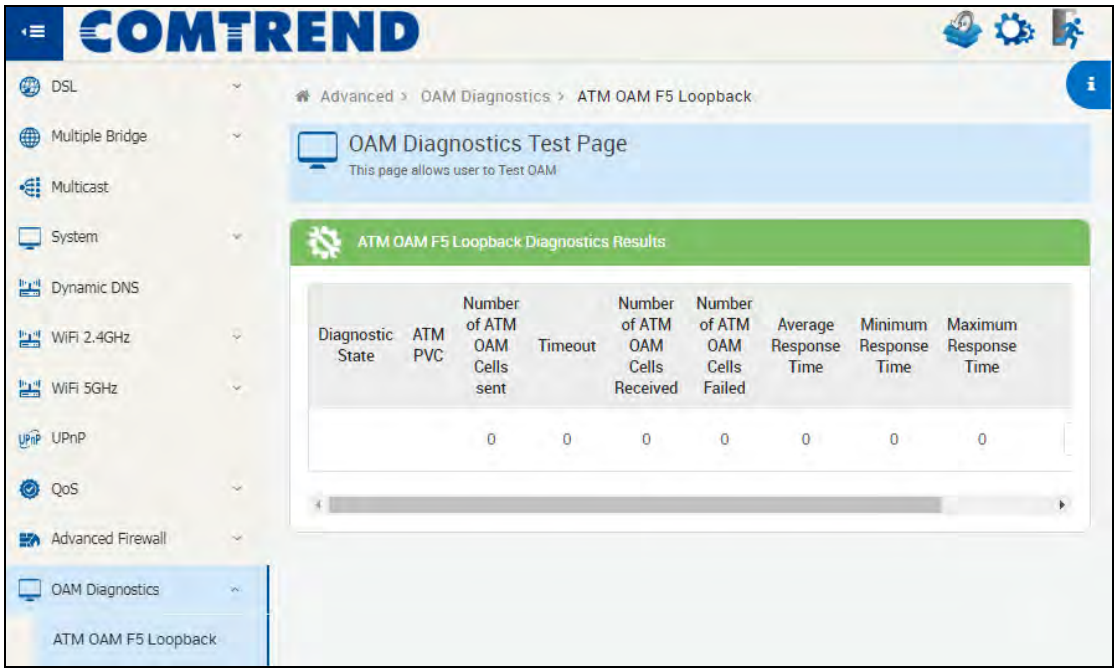


Click the Information icon on the upper right-hand side of this screen for information on Packet Filter settings.

5.11 OAM Diagnostics

This page allows user to Test OAM.

5.11.1 ATM OAM F5 Loopback

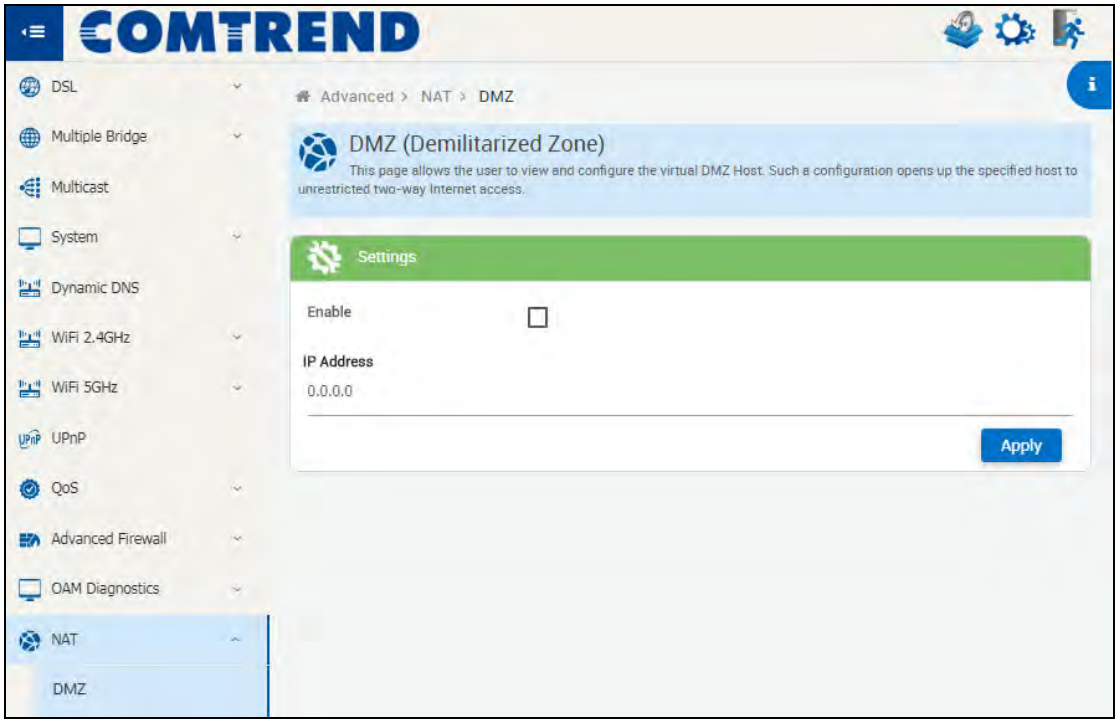


Click the Information icon on the upper right-hand side of this screen for information on ATM OAM F5 Loopback Diagnostic results.

5.12 NAT

5.12.1 DMZ

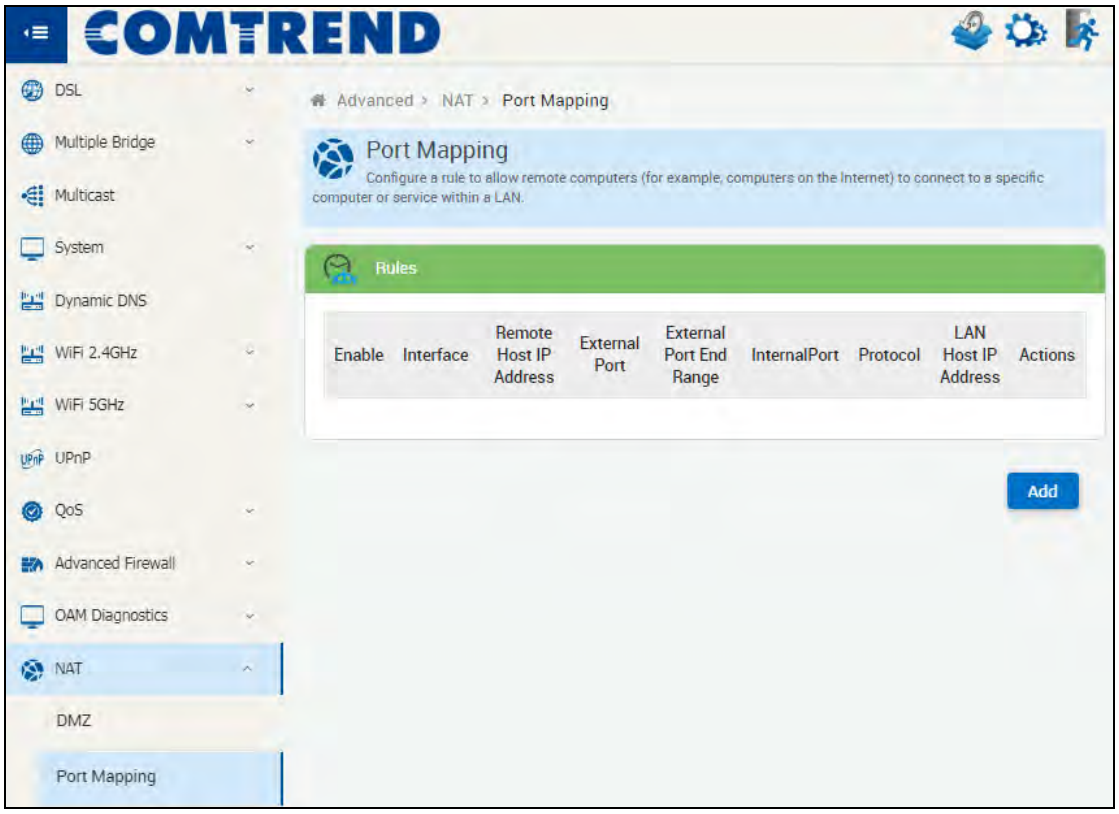
This page allows the user to view and configure the virtual DMZ Host. Such a configuration opens up the specified host to unrestricted two-way Internet access.



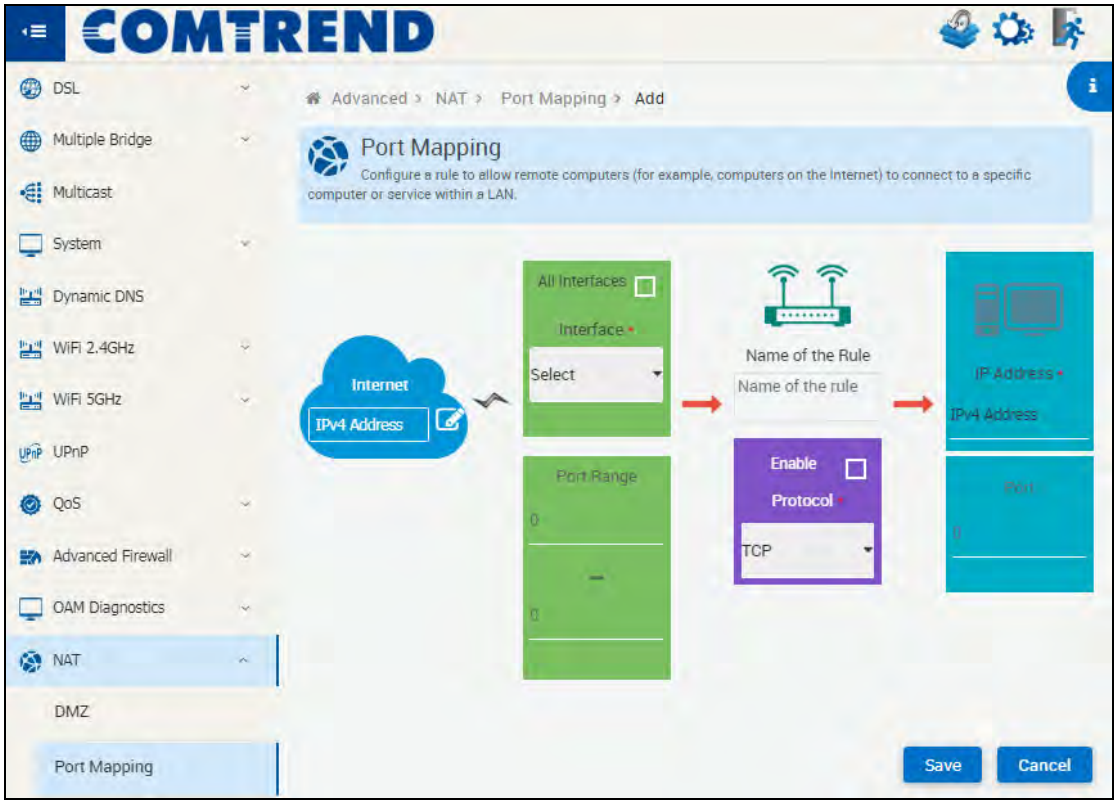
Click the Information icon on the upper right-hand side of this screen for information on DMZ settings.

5.12.2 Port Mapping

Configure a rule to allow remote computers (for example, computers on the Internet) to connect to a specific computer or service within a LAN.



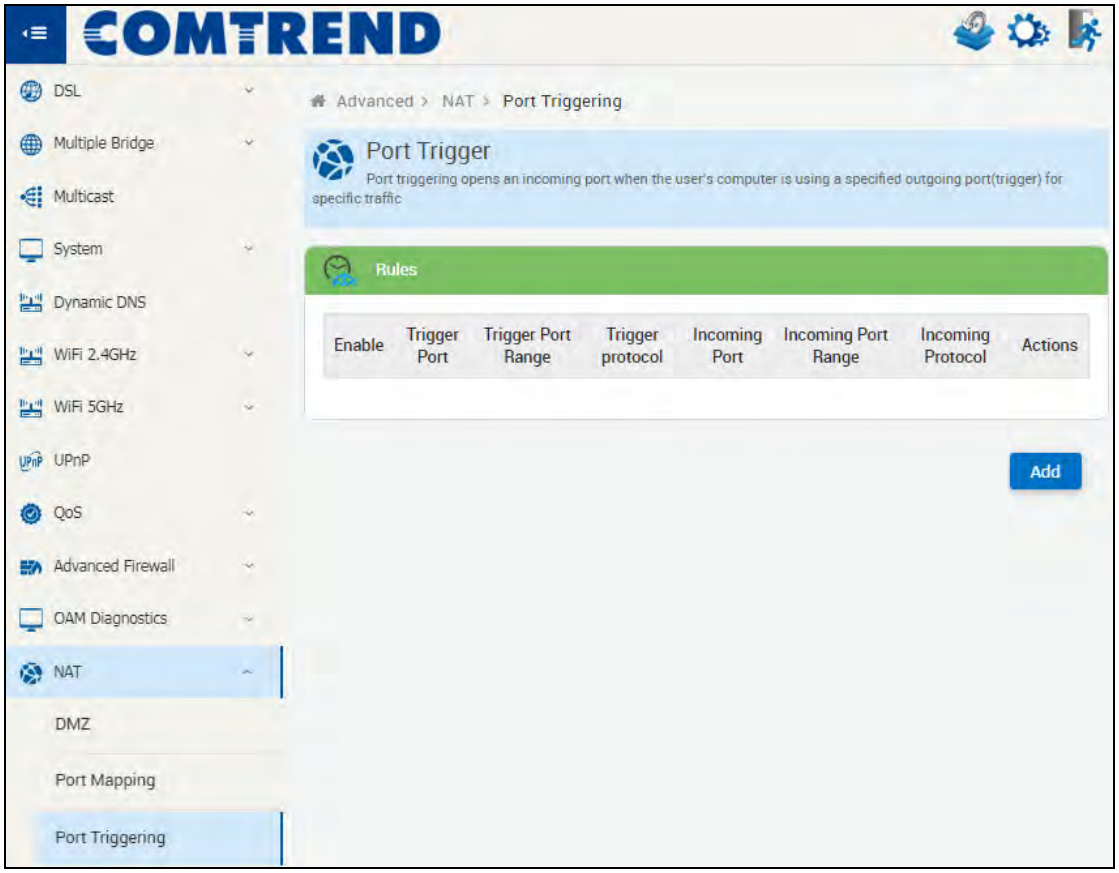
Click the button to display the following.



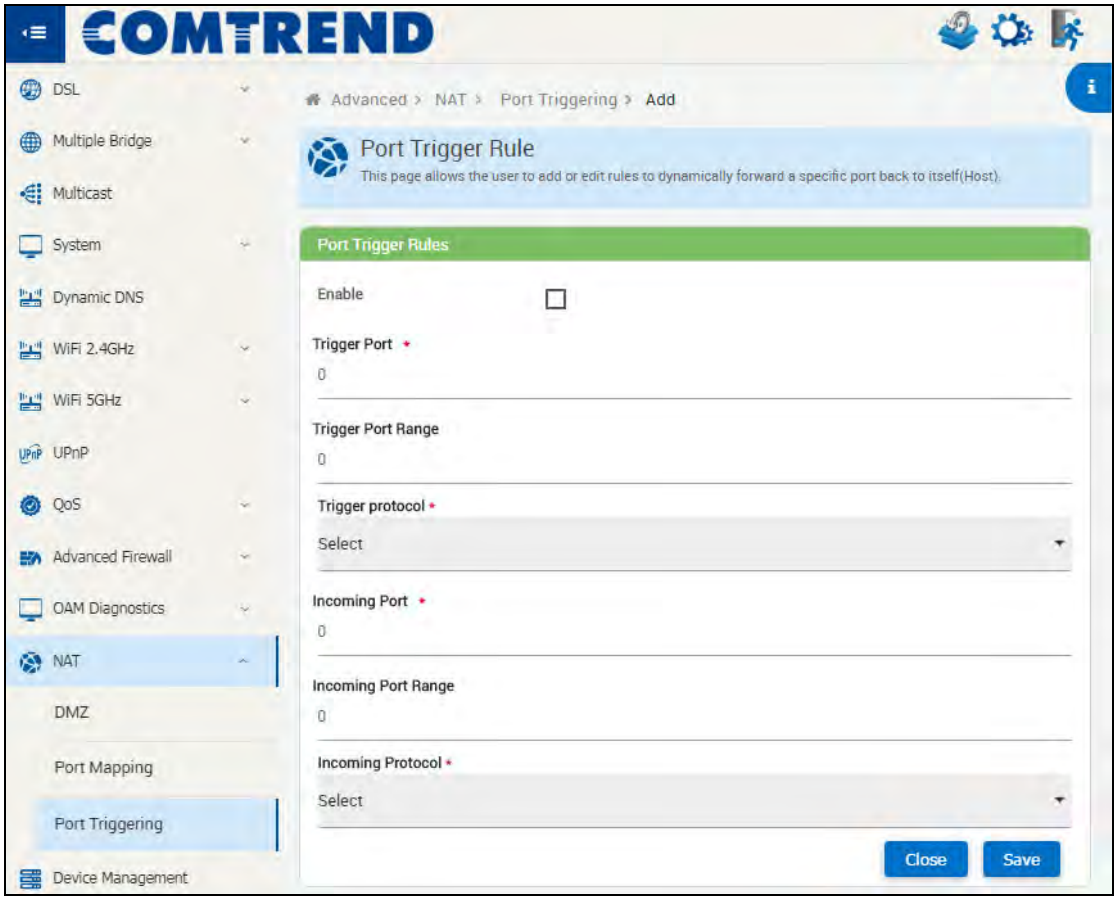
Click the Information icon on the upper right-hand side of this screen for information on Port Mapping settings.

5.12.3 Port Triggering

Port triggering opens an incoming port when the user's computer is using a specified outgoing port(trigger) for specific traffic.

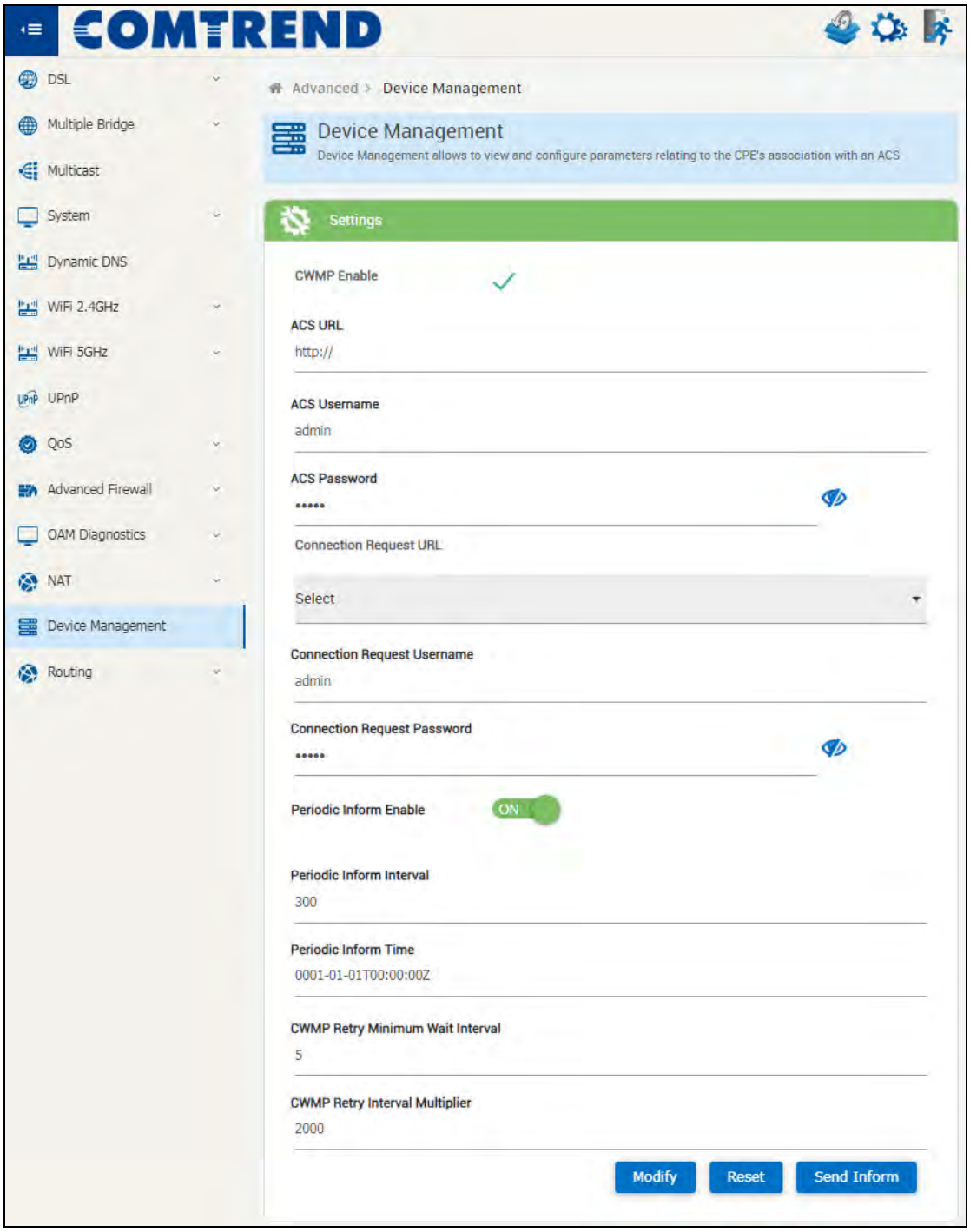


Click the button to display the following.



Click the Information icon on the upper right-hand side of this screen for information on Port Trigger settings.

5.13 Device Management



The settings shown above are described below.

Heading	Description
CWMP Enable	Shows if enabled or disabled
ACS URL	ACS URL
ACS Username	Admin by default
ACS Password	Admin by default
Connection Request URL	Connection Request URL
Connection Request Username	Admin by default
Connection Request Password	Admin by default
Periodic Inform Enable	Periodic Inform Enable
Periodic Inform Interval	300 seconds by default
Periodic Inform Time	Periodic Inform Time
CWMP Retry Minimum Wait Interval	5 seconds as default
CWMP Retry Interval Multiplier	Max Retry Interval 2000 seconds

If you need to modify the settings, first make the change, and then click the Modify button.

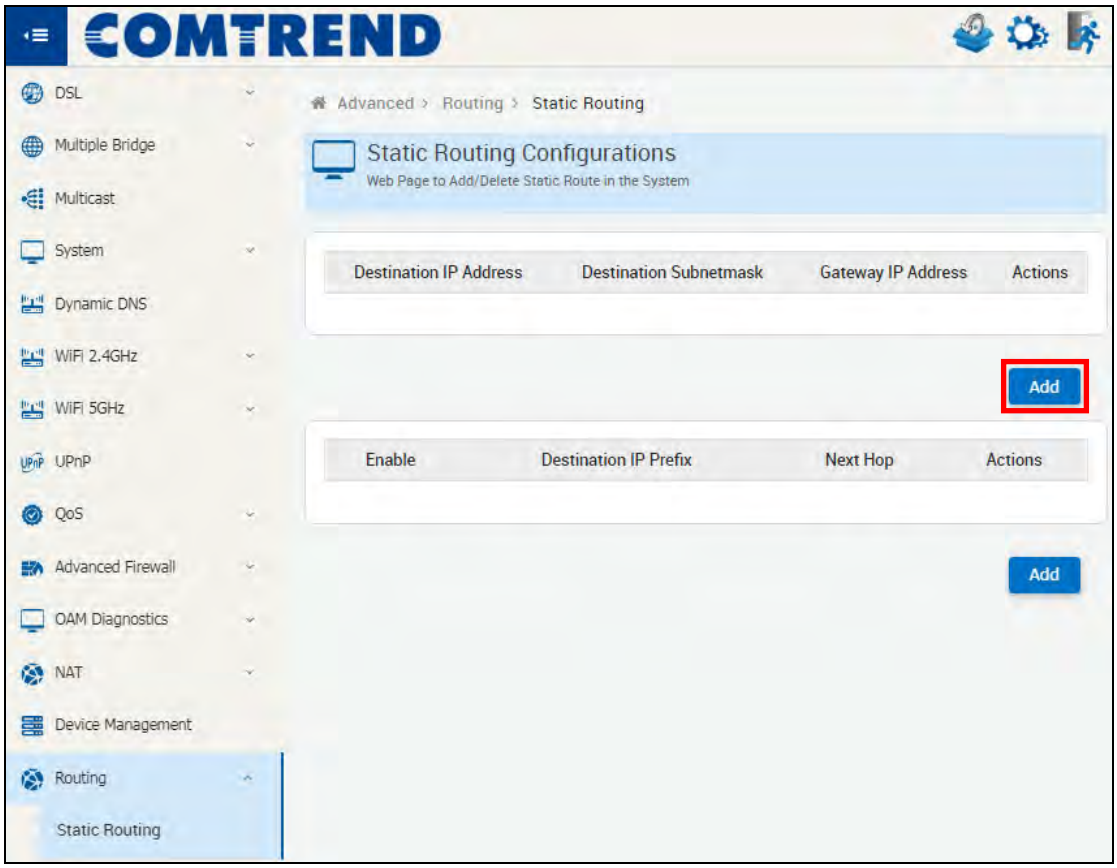
Click the Reset button to refresh to previous settings.

Click the Send Inform button to send the inform details to the ACS server.

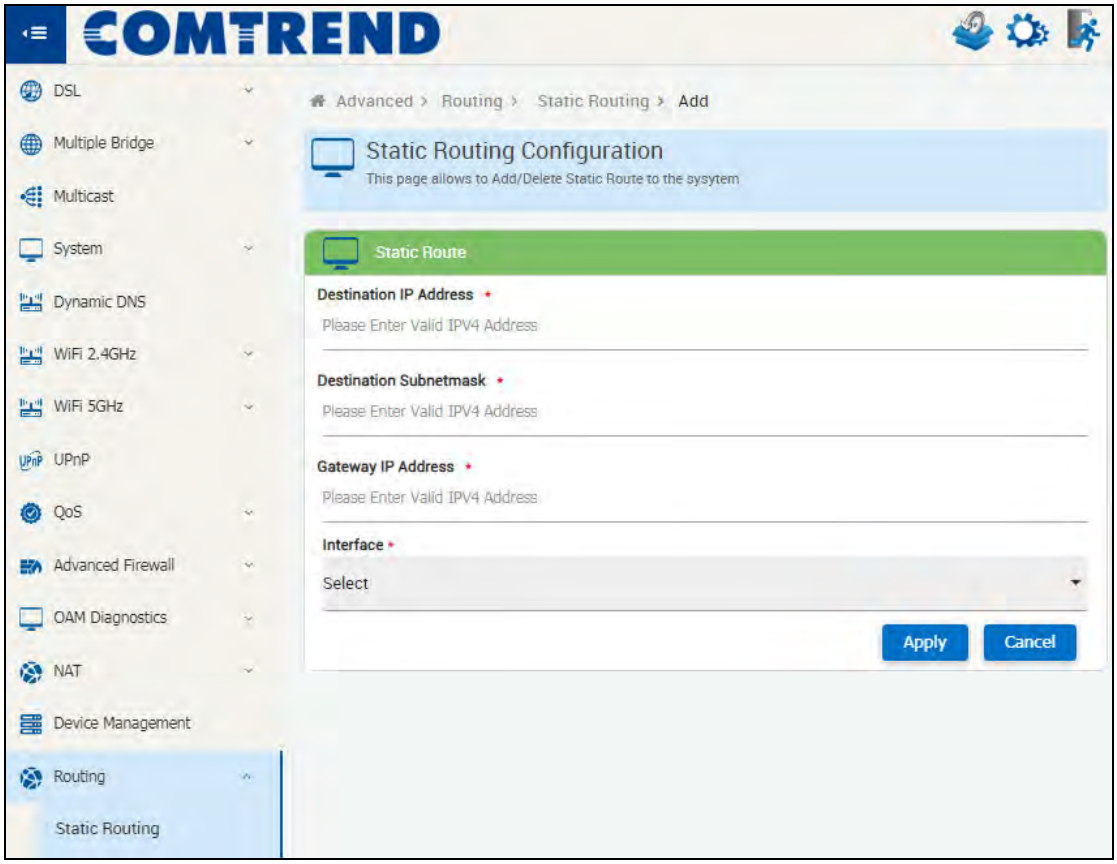
5.14 Routing

Web Page to Add/Delete Static Route in the System.

5.14.1 Static Routing

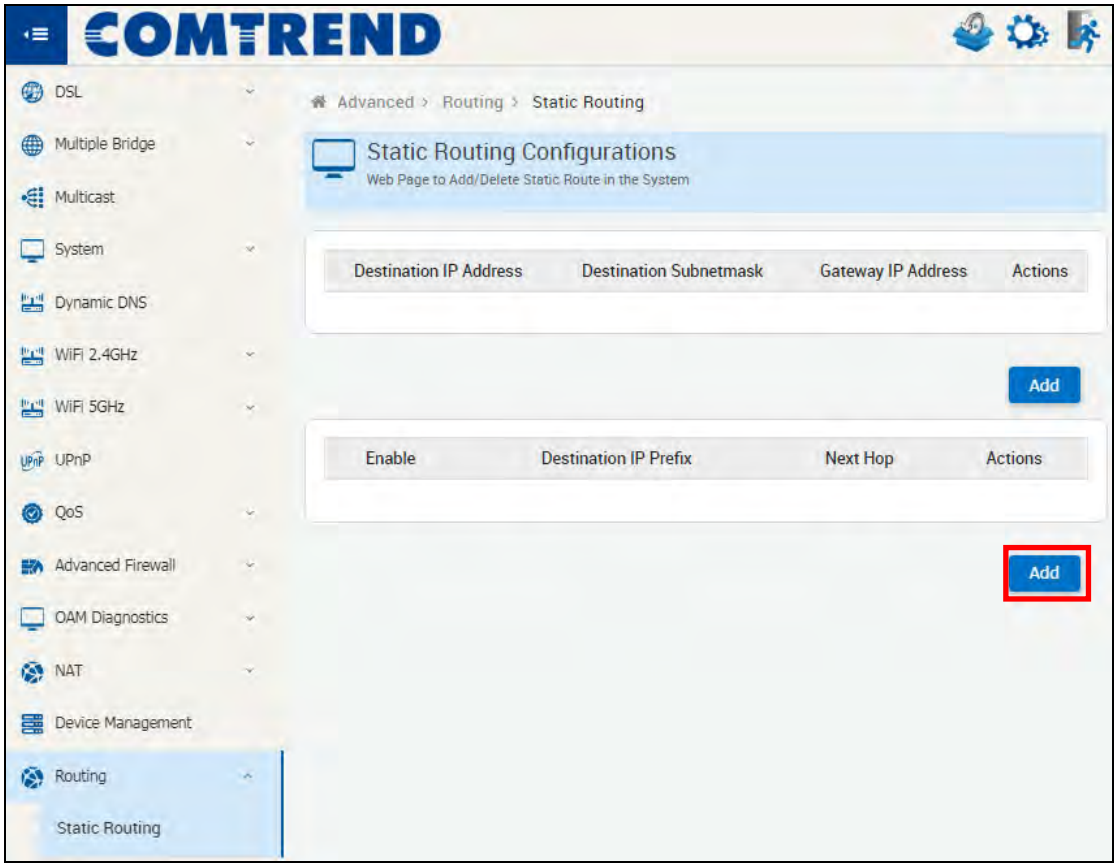


Click the first button to display the following (IPv4 Static Route).



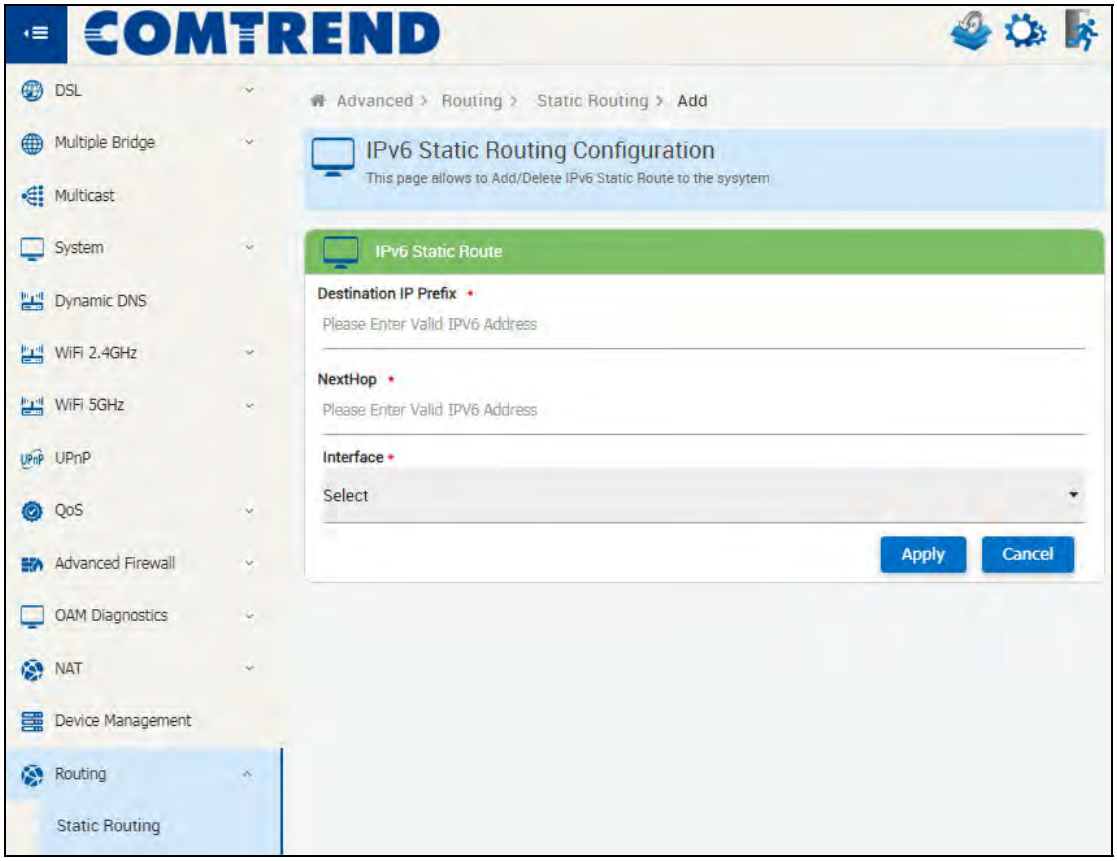
The settings shown above are described below.

Heading	Description
Destination IP Address	Destination Server or Gateway IP
Destination Subnetmask	255.255.x.x
Gateway IP Address	192.168.1.x
Interface	Interface connect to Destination Server or GW (br-lan or ptm)



Click the second

button to display the following (IPv6 Static Route).

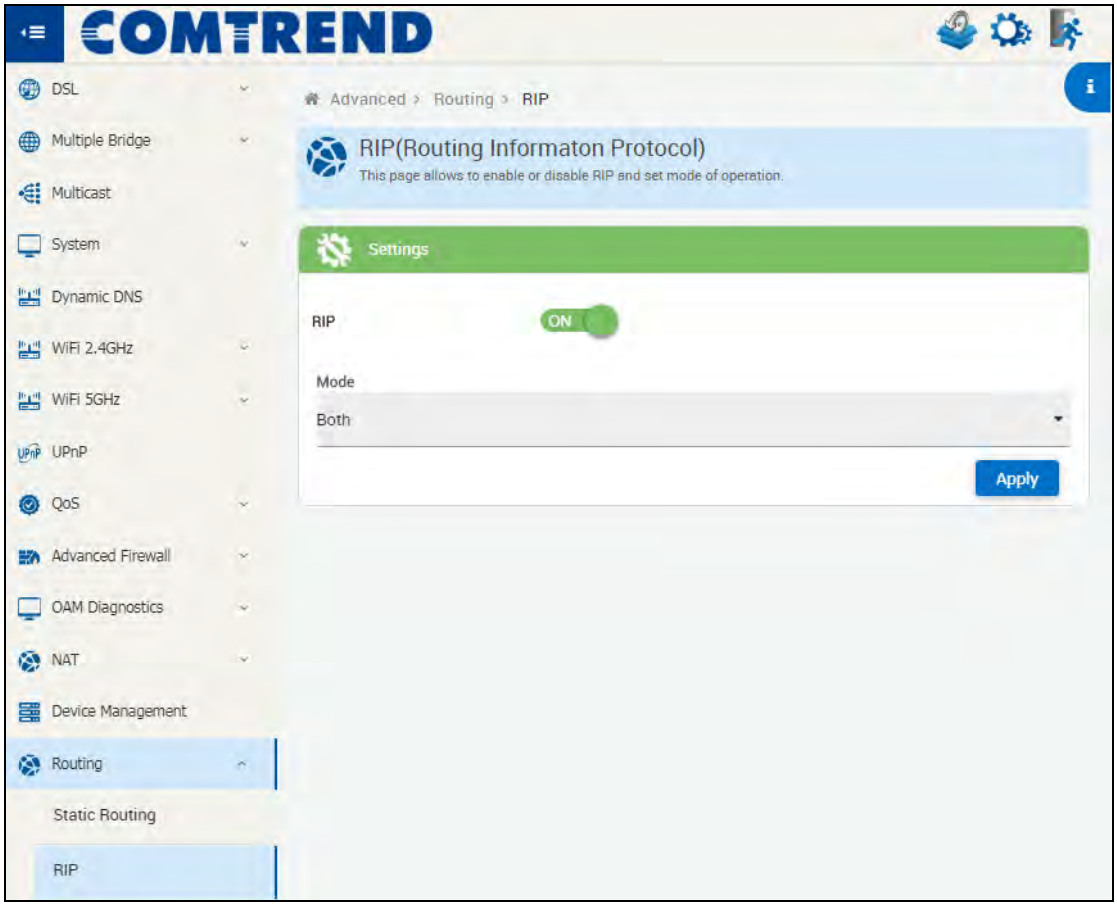


The settings shown above are described below.

Heading	Description
Destination IP Prefix	EX: 2001:DB8:3000:0/16
NextHop	EX: 2001:DB8:1:1
Interface	EX: Ethernet1/0

5.14.2 RIP

This page allows to enable or disable RIP and set mode of operation.

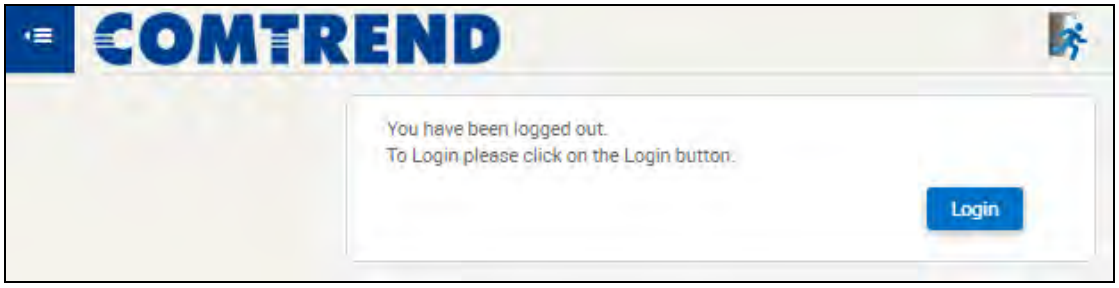


Click the Information icon on the upper right-hand side of this screen for information on Routing Information Protocol settings.

Chapter 6 Logout

To log out from the device simply click the following icon located at the top of your screen.

Upon successful exit, the following message will be displayed.



Appendix A – Specifications

Hardware

- RJ-11 X1 for VDSL2 (35b)/ADSL2+ (Annex A)
- RJ-45 X 4 for GELAN
- RJ-45 X 1 for GEWAN
- Reset button X 1
- WPS button X 1
- Guest WiFi button X 1
- Internal Antenna X 2
- Power switch X 1

ADSL

- G.994
- G.992.1 (G.dmt) Annexes A
- G.992.2 (G.lite) Annexes A
- ANSI T1.413
- G.992.3 (ADSL2) Annexes A
- G.992.5 (ADSL2+) Annexes A

VDSL

- G.993.2(VDSL2) 35b, 30a, 17a, 12a, 12b, 8a, 8b, 8c, 8d
- G.993.5 (G.vector)
- G.998.4 (G.INP)
- SRA (Seamless Rate Adaptation)
- UPBO (Upstream Power Back-off)

Ethernet

- IEEE 802.3, IEEE 802.3u IEEE 802.3ab
- 10/100 /1000 BASE-T, auto-sense
- Support MDI/MDX

Networking Protocols

- RFC 2364 (PPPoA), RFC 2684 (RFC 1483) Bridge/Router, RFC 2516 (PPPoE); RFC 1577 (IPoA)
- PPPoE Pass-Through, Multiple PPPoE Sessions on Single WAN Interface
- PPPoE Filtering of Non-PPPoE Packets Between WAN and LAN
- Transparent Bridging Between all LAN and WAN Interfaces
- 802.1p/802.1q VLAN, DSCP
- IGMP Proxy V1/V2/V3, IGMP Snooping V1/V2/V3, Fast leave
- Static route, RIP v1/v2, ARP, RARP, SNTP
- DHCP Server/Client/Relay, DNS Proxy/ Relay, Dynamic DNS, UPnP, DLNA
- IPv6 Dual Stack, IPV6 Rapid Deployment (6RD)

Management

· TR-069/TR-098/TR-104/TR-111/TR-181, SNMP, Telnet, Web- Based Management, Configuration Backup and Restoration

· Software Upgrade via HTTP, TFTP Server, or FTP Server

Firewall/Filtering

· Stateful Packet Inspection Firewall

· Stateless Packet Filter

· URI/URL Filtering

· TCP/IP/Port/Interface Filtering Rules Support Both Incoming and Outgoing Filtering

NAT/PAT

· Port Triggering

· Port Forwarding (Virtual Server)

· Symmetric port-overloading NAT, Full-Cone NAT

· DMZ host

· VPN Pass Through (PPTP, L2TP, IPSec)

Wireless

· IEEE 802.11n, 2.4GHz, 2T2R
Backward compatible with 802.11g/b
2412～2462 MHz

· IEEE 802.11ac,5GHz, 2T2R,
Backward compatible with 802.11n/a
U-NII-1 (5150～5250 MHz)
U-NII-3 (5725～5825 MHz)

· WPA/WPA-PSK, WPA2/WPA2-PSK with TKIP & AES Security Type

· Multiple SSID

· MAC Address Filtering

Power Supply

· External power adapter: 12Vdc/ 2.0A ⊖-◐-⊕

Certification

· FCC, UL, IC, cUL standard

Note : Specification are subject to change without note.

Environment

· Operating Temperature: 0°C ~40°C (32°F ~104°F)

· Operating Humidity: 10%~90% non-condensing

· Storage Temperature: -25°C ~65°C (-23°F ~149°F)

· Storage Humidity: 5%~90% non-condensing

Kit Contents

(1*VR-3053, 1*RJ11 cable, 1*RJ45 cable, 1*power adapter, 1*CD-ROM)

NOTE: Specifications are subject to change without notice

Appendix B - SSH Client

Unlike Microsoft Windows, Linux OS has a ssh client included. For Windows users, there is a public domain one called "putty" that can be downloaded from here:

http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

To access the ssh client you must first enable SSH access for the LAN or WAN from the Management → Access Control → Services menu in the web user interface.

To access the router using the Linux ssh client

For LAN access, type: ssh -l root 192.168.1.1

For WAN access, type: ssh -l root *WAN IP address*

To access the router using the Windows "putty" ssh client

For LAN access, type: putty -ssh -l root 192.168.1.1

For WAN access, type: putty -ssh -l root *WAN IP address*

NOTE: The *WAN IP address* can be found on the Device Info → WAN screen