COMTREND

VR-3063

Home Gateway

User Manual

261099-048

Version A1.0, July 31, 2018

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.
- This equipment complies with EU radiation exposure limits set forth for an uncontrolled environment. This equipment should be installed and operated with minimum distance 25cm between the radiator & your body.
- For indoor use only.
- Do NOT open the casing.
- Do NOT use near water.

Power Specifications:

I/P： 12Vdc / 2.5A ⊖-(•)-⊕

WARNING

- Disconnect the power line from the device before servicing.
- Power supply specifications are clearly stated in Appendix C - Specifications.
- 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.

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 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 25 centimeters between the radiator and your body.

1.L'émetteur ne doit pas être colocalisé ni fonctionner conjointement avec à autre antenne ou autre émetteur. 2.Cet appareil est conforme aux limites d'exposition aux rayonnements de la IC pour un environnement non contrôlé. L'antenne doit être installé de façon à garder une distance minimale de 25 centimètres entre la source de rayonnements et votre corps.

ISED
This device complies with the ISED portable RF exposure limit set forth for an uncontrolled environment and are safe for intended operation as described in this manual. The further RF exposure reduction can be achieved if the product can be kept as far as possible from the user body or set the device to lower output power if such function is available.

Déclaration d'exposition aux radiationsCet appareil est conforme aux limites d'exposition aux radiofréquences portables établies au ISED pour un environnement non contrôlé et ne présente pas de risque dans le cadre d’une utilisation conforme à celle décrite dans ce manuel. Une réduction accrue de l’exposition aux radiofréquences peut être obtenue en tenant l’appareil aussi éloigné que possible du corps humain ou en réglant l’appareil sur une puissante inférieure si cette fonction est disponible.

Copyright

Copyright©2018 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 **9**

CHAPTER 2 INSTALLATION **10**
2.1 HARDWARE SETUP 10
2.2 LED INDICATORS 13

CHAPTER 3 WEB USER INTERFACE **16**
3.1 DEFAULT SETTINGS 16
3.2 IP CONFIGURATION 17
3.3 LOGIN PROCEDURE 19

CHAPTER 4 DEVICE INFORMATION **21**
4.1 WAN 22
4.2 STATISTICS 23
4.2.1 LAN Statistics *23*
4.2.2 WAN Service *24*
4.2.3 XTM Statistics *25*
4.2.4 xDSL Statistics *26*
4.3 ROUTE 31
4.4 ARP 32
4.5 DHCP 32
4.6 IGMP INFO 34
4.7 IPV6 35
4.7.1 IPv6 Info *35*
4.7.2 IPv6 Neighbor *36*
4.7.3 IPv6 Route *37*
4.8 CPU & MEMORY 38
4.9 NETWORK MAP 39
4.10 WIRELESS 39
4.10.1 Station Info *39*
4.10.2 Site Survey *41*

CHAPTER 5 BASIC SETUP **43**
5.1 WAN SETUP 44
5.1.1 WAN Service Setup *45*
5.2 NAT 46
5.2.1 Virtual Servers *46*
5.2.2 Port Triggering *48*
5.2.3 DMZ Host *50*
5.3 LAN 51
5.3.1 Lan VLAN Setting *53*
5.3.2 LAN IPv6 Autoconfig *54*
5.3.3 Static IP Neighbor *56*
5.3.4 UPnP *57*
5.4 WIRELESS 58
5.4.1 Basic 2.4GHz *58*
5.4.2 Security 2.4GHz *60*
5.4.3 Basic 5GHz *62*
5.4.4 Security 5GHz *64*
5.5 PARENTAL CONTROL 66
5.5.1 Time Restriction *66*
5.5.2 URL Filter *67*
5.6 HOME NETWORKING 68
5.6.1 Print Server *68*
5.6.2 DLNA *68*

CHAPTER 6 ADVANCED SETUP **71**
6.1 SECURITY 71
6.1.1 IP Filtering *71*

6.1.2 MAC Filtering *74*
6.2 QUALITY OF SERVICE (QOS) 76
6.2.1 QoS Queue *77*
6.2.1.1 QoS Queue Configuration *77*
6.2.1.2 Wlan Queue *80*
6.2.2 QoS Classification *81*
6.2.3 QoS Port Shaping *83*
6.3 ROUTING 84
6.3.1 Default Gateway *84*
6.3.2 Static Route *85*
6.3.3 Policy Routing *86*
6.3.4 RIP *87*
6.4 DNS 88
6.4.1 DNS Server *88*
6.4.2 Dynamic DNS *89*
6.5 DSL 90
6.6 DNS PROXY 91
6.7 INTERFACE GROUPING 92
6.8 IP TUNNEL 94
6.8.1 IPv6inIPv4 ..... *94*
6.8.2 IPv4inIPv6 ..... *95*
6.9 IP SEC 96
6.10 CERTIFICATE 100
6.10.1 Local *100*
6.10.2 Trusted CA *102*
6.11 POWER MANAGEMENT 103
6.12 MULTICAST 104
6.13 WIRELESS 107
6.13.1 Basic 2.4GHz *107*
6.13.2 Security 2.4GHz *109*
6.13.3 WPS 2.4GHz *111*
6.13.4 Advanced 2.4GHz *113*
6.13.5 Basic 5GHz *115*
6.13.6 Security 5GHz *117*
6.13.7 WPS 5GHz *119*
6.13.8 Advanced 5GHz *121*

CHAPTER 7 DIAGNOSTICS 123
7.1 DIAGNOSTICS – INDIVIDUAL TESTS 123
7.2 ETHERNET OAM 124
7.3 PING 127
7.4 TRACE ROUTE 128

CHAPTER 8 MANAGEMENT 129
8.1 SETTINGS 129
8.1.1 Backup Settings *129*
8.1.2 Update Settings *130*
8.1.3 Restore Default *130*
8.2 SYSTEM LOG 131
8.3 SNMP AGENT 133
8.4 TR-069 CLIENT 134
8.5 INTERNET TIME 136
8.6 ACCESS CONTROL 137
8.6.1 Accounts *137*
8.6.2 Services *139*
8.6.3 IP Address *140*
8.7 UPDATE SOFTWARE 141
8.8 REBOOT 142

CHAPTER 9 LOGOUT 143

APPENDIX A - FIREWALL 144

APPENDIX B - PIN ASSIGNMENTS **147**
APPENDIX C – SPECIFICATIONS **148**
APPENDIX D - SSH CLIENT **150**
APPENDIX E - PRINTER SERVER **151**
APPENDIX F - CONNECTION SETUP **158**

Chapter 1 Introduction

VR-3063 is a Multi-DSL solution for high-performance Internet access. In addition, VR-3063 supports high power (400mw/26 dBm) dual bands (802.11n 2.4GHz & 802.11ac 5GHz) to create a large Wi-Fi footprint for the most seamless video experience as well as blazing fast data speed and a toll-quality voice experience.

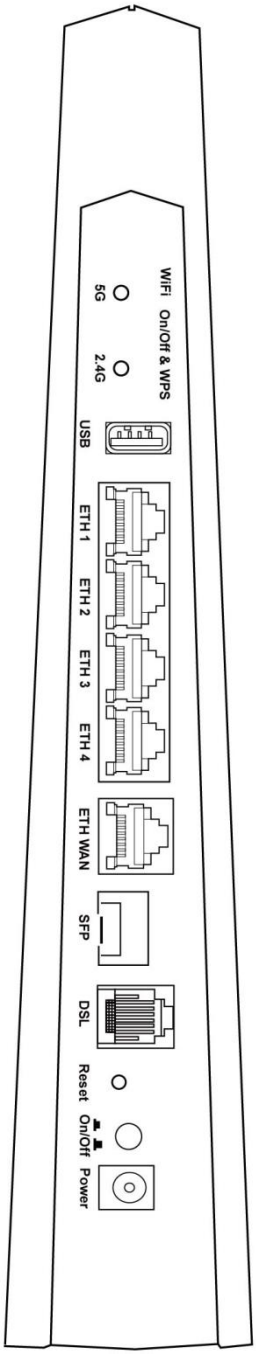
Chapter 2 Installation

2.1 Hardware Setup

Follow the instructions below to complete the hardware setup.

BACK PANEL

The figure below shows the back panel of the device.



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 2.2 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.

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 2.2 LED Indicators for details).

NOTE:	If pressed down for more than 60 seconds, the VR-3063 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.

DSL Port
Connect to an ADSL2/2+ or VDSL with this RJ11 Port. This device contains a micro filter which removes the analog phone signal. If you wish, you can connect a regular telephone to the same line by using a POTS splitter.

SFP Port
SFP (Small form-factor pluggable transceiver) port provides an additional interface for modular fiber/giga/g.fast transceivers.

ETH WAN PORT
This port has the same features as the LAN ports described below with additional Ethernet WAN functionality.

Ethernet (LAN) Ports
Use 1000-BASE-T RJ-45 cables to connect up to four network devices to a Gigabit LAN, or 10/100BASE-T RJ-45 cables for standard network usage. These ports are auto-sensing MDI/X; so either straight-through or crossover cable can be used.

USB Host Port (Type A)
A USB host port supports compatible printers (See Appendix E for setup instructions) or storage devices. If a storage device is connected to the USB host port, it can be used to stream the DLNA service. Support for other devices may be added in future firmware upgrades.

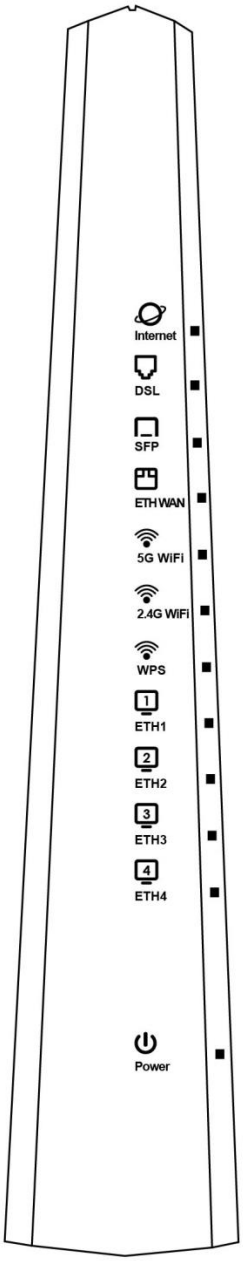
2.4G WiFi On/Off & WPS Button
Press and release the WiFi-WPS button to activate WPS for the 2.4GHz WiFi interface (make sure the WPS is enabled in Wireless->2.4GHz->Security page). Press and hold WiFi-WPS button more than 10 seconds to enable/disable 2.4GHz WiFi.

5G WiFi On/Off & WPS Button

Press and release the WiFi-WPS button to activate WPS for the 5GHz WiFi interface (make sure the WPS is enabled in Wireless->5GHz->Security page).
Press and hold WiFi-WPS button more than 10 seconds to enable/disable 5GHz WiFi.

2.2 LED Indicators

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
POWER	GREEN	On	The device is powered up.
		Off	The device is powered down.
		Blink	Software upgrade is in progress.
	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.

ETH 4 to 1	GREEN	On	Ethernet is connected at 1000 Mbps.
		Off	Ethernet is not connected.
		Blink	In TX/RX over 1000 Mbps.
	ORANGE	On	Ethernet is connected at 10/100 Mbps.
		Off	Ethernet is not connected.
		Blink	In TX/RX over 10/100 Mbps.
WPS	GREEN	On	WPS(2.4G) connection successful. The LED will stay on for 3 minutes.
		Off	(2.4G) No WPS association process ongoing.
		Blink	(2.4G) WPS connection in progress.
	ORANGE	On	WPS(5G) connection successful. The LED will stay on for 3 minutes.
		Off	(5G) No WPS association process ongoing.
		Blink	(5G) WPS connection in progress.
WiFi 2.4G	GREEN	On	The wireless module is ready. (i.e. installed and enabled).
		Off	The wireless module is not ready. (i.e. either not installed or disabled).
		Blink	Data transmitting or receiving over WLAN.
WiFi 5G	GREEN	On	The wireless module is ready. (i.e. installed and enabled).
		Off	The wireless module is not ready. (i.e. either not installed or disabled).
		Blink	Data transmitting or receiving over WLAN.
ETH WAN	GREEN	On	WAN is connected at 1000 Mbps. SFP module is connected.
		Off	Ethernet WAN is not connected. SFP module is connected.
		Blink	In TX/RX over 1000 Mbps.
	ORANGE	On	Ethernet is connected at 10/100 Mbps.
		Off	Ethernet WAN is not connected.
		Blink	In TX/RX over 1000 Mbps.
SFP	GREEN	On	SFP module is activated
		Off	SFP module is deactivated
		Blink	traffic passing on SFP-connected interface (eth0)
DSL	GREEN	On	xDSL Link is established.
		Off	The device is powered down.
		Blink	The xDSL link is training.
INTERNET	GREEN	On	IP connected and no traffic detected (the device has a WAN IP address from IPCP or DHCP is up or a static IP address is configured, PPP negotiation has successfully completed. If the IP or PPPoE session is dropped due to an idle

			timeout, the light will remain Green. 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 thru 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.)

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-3063 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.

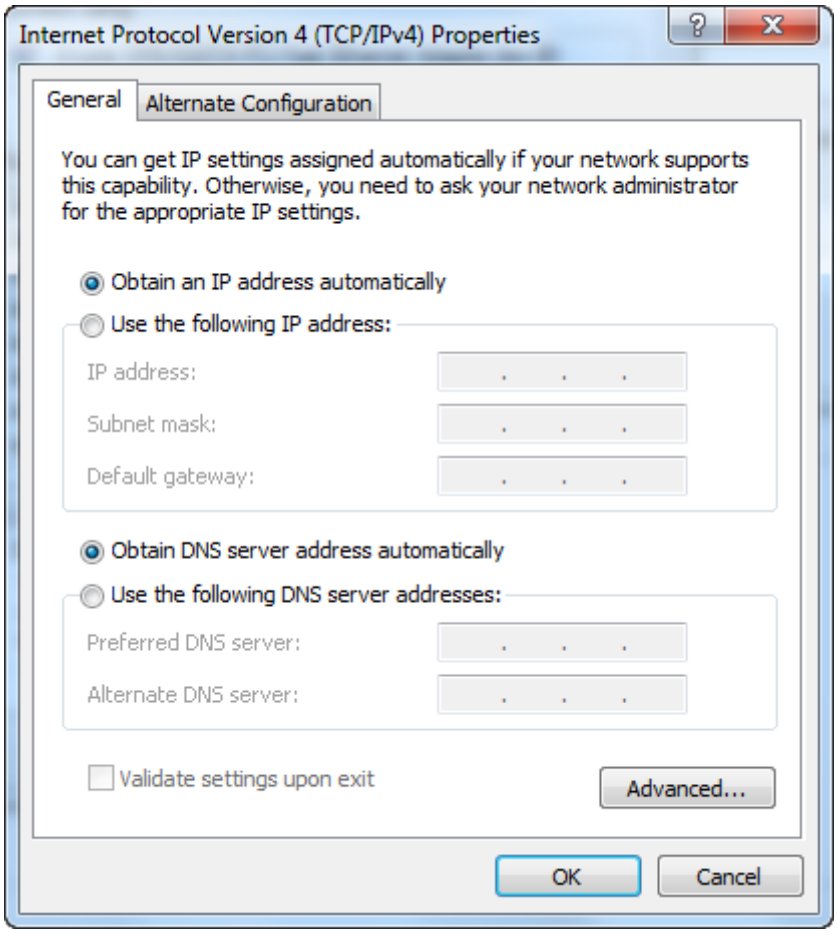
To obtain an IP address from the DCHP server, follow the steps provided below.

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.

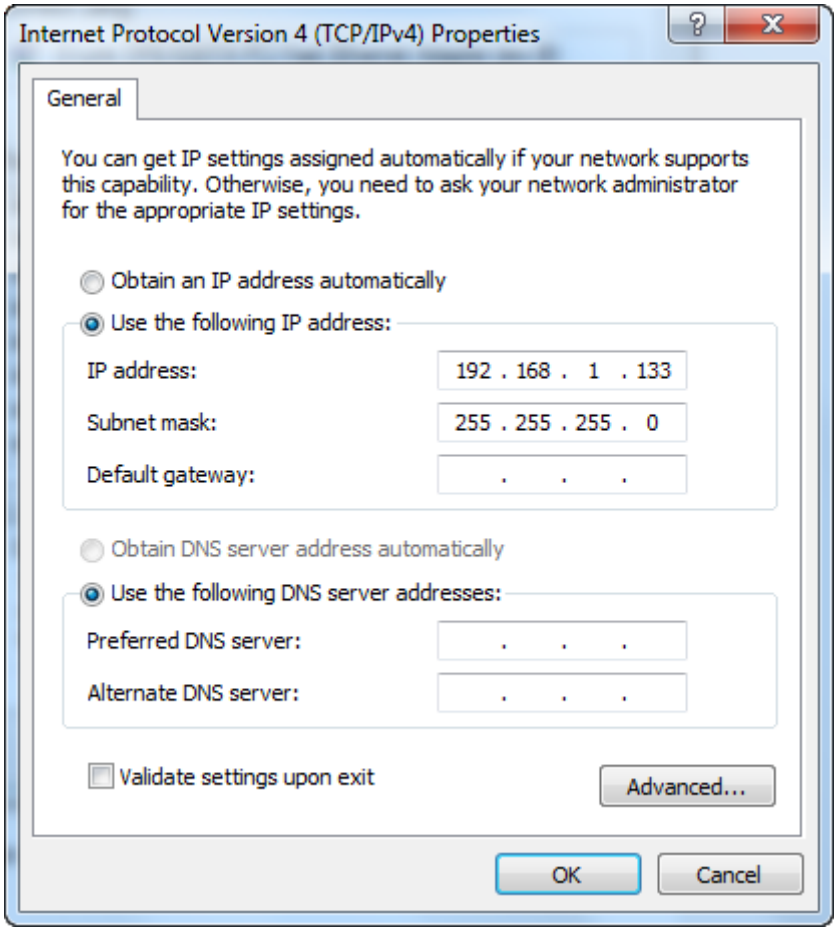
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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

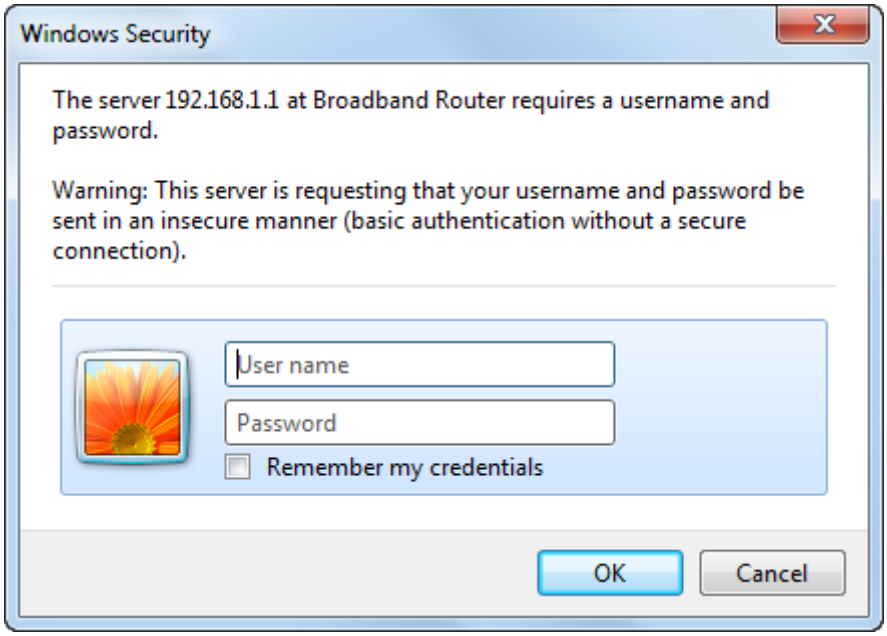
Perform the following steps to login to the web user interface.

NOTE:	The default settings can be found in section 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. For remote access (i.e. WAN), use the IP address shown on the Device Information screen and login with remote username and password.

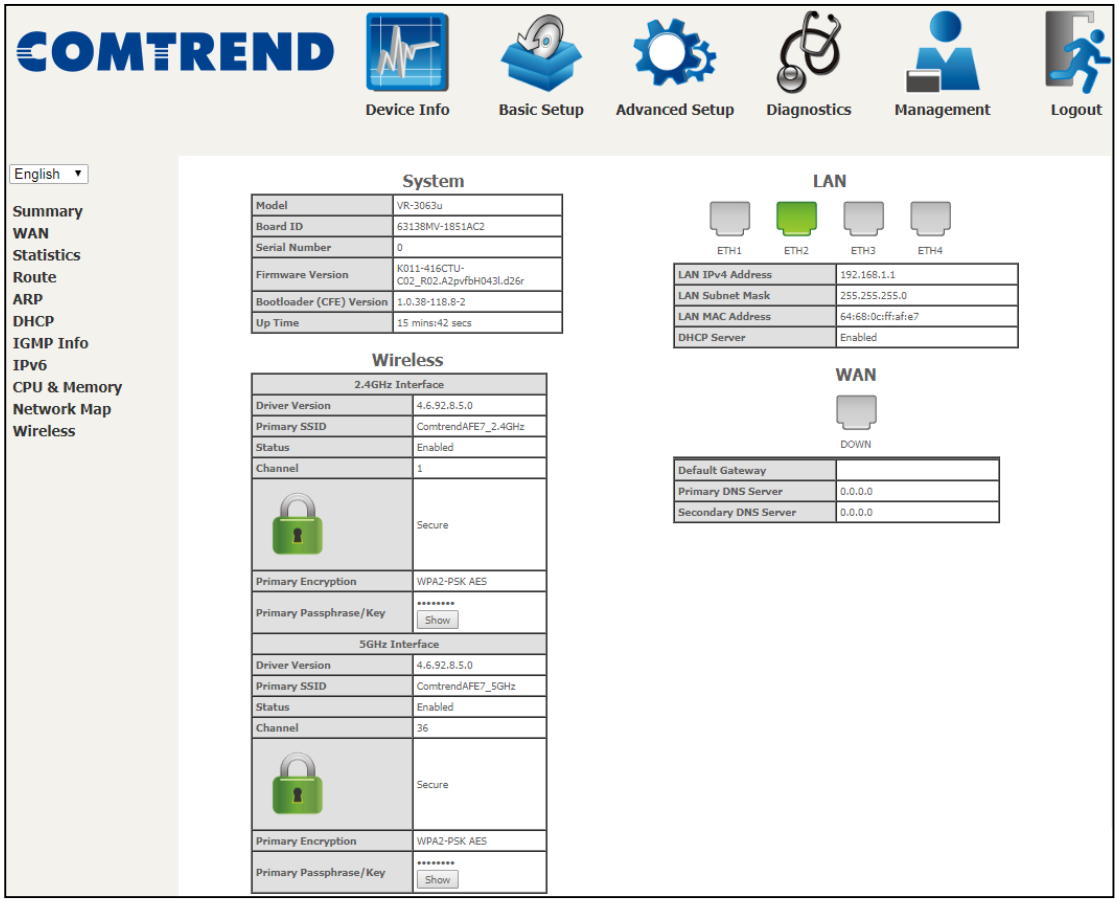
STEP 2: A dialog box will appear, such as the one below. Enter the default username and password, as defined in section 3.1 Default Settings.



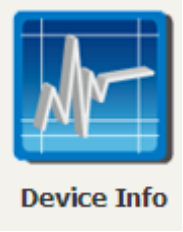
Click **OK** to continue.

NOTE:	The login password can be changed later (see section 8.6.1 Accounts).

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 Device Information

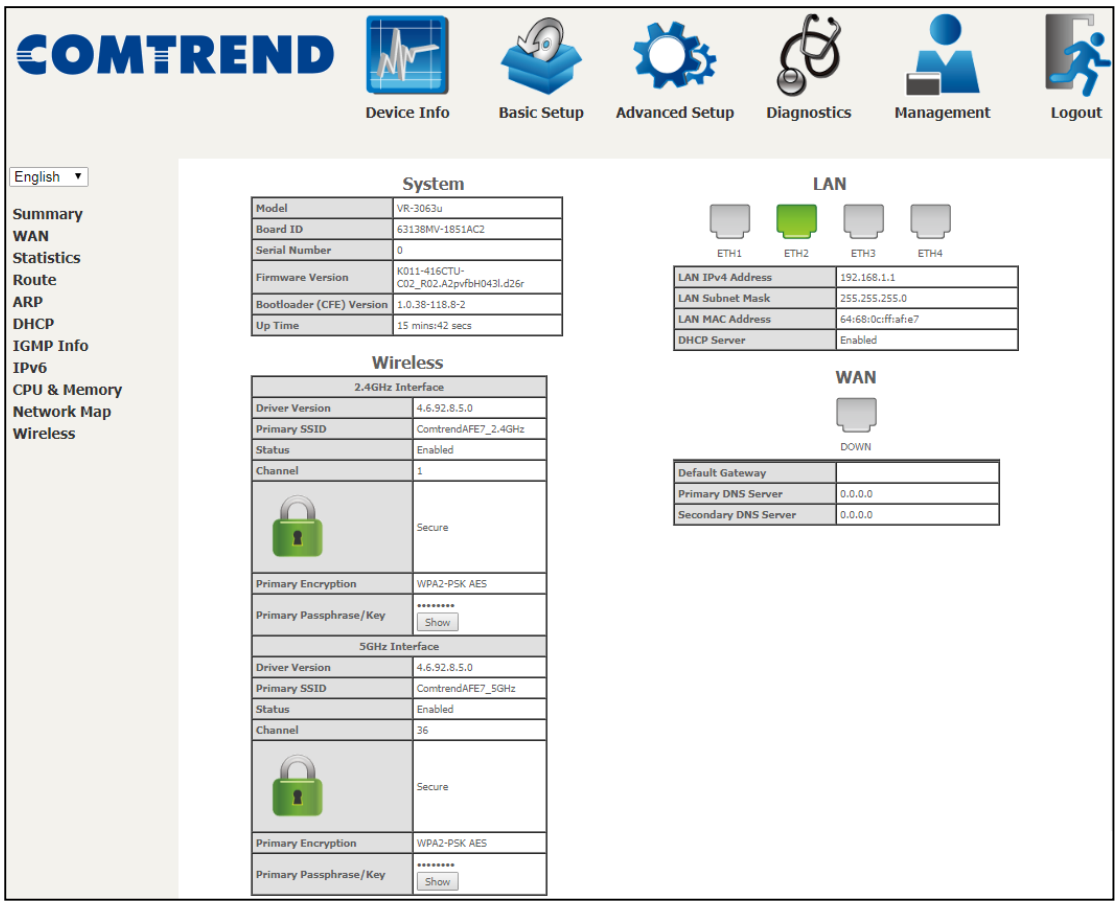
You can reach this page by clicking on the following icon located at the top of the screen.

The web user interface window is divided into two frames, the main menu (on the 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, user account has limited access to configuration modification.

Device Info is the first selection on the main menu so it will be discussed first. Subsequent chapters will introduce the other main menu options in sequence.

The Device Info Summary screen displays at startup.



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

4.1 WAN

Select WAN from the Device Info submenu to display the configured PVC(s).

Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
VlanMuxId	Shows 802.1Q VLAN ID
IPv6	Shows WAN IPv6 status
Igmp Pxy	Shows Internet Group Management Protocol (IGMP) proxy status
Igmp Src Enbl	Shows the status of WAN interface used as IGMP source
MLD Pxy	Shows Multicast Listener Discovery (MLD) proxy status
MLD Src Enbl	Shows the status of WAN interface used as MLD source
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the status of Firewall
Status	Lists the status of DSL link
IPv4 Address	Shows WAN IPv4 address
IPv6 Address	Shows WAN IPv6 address

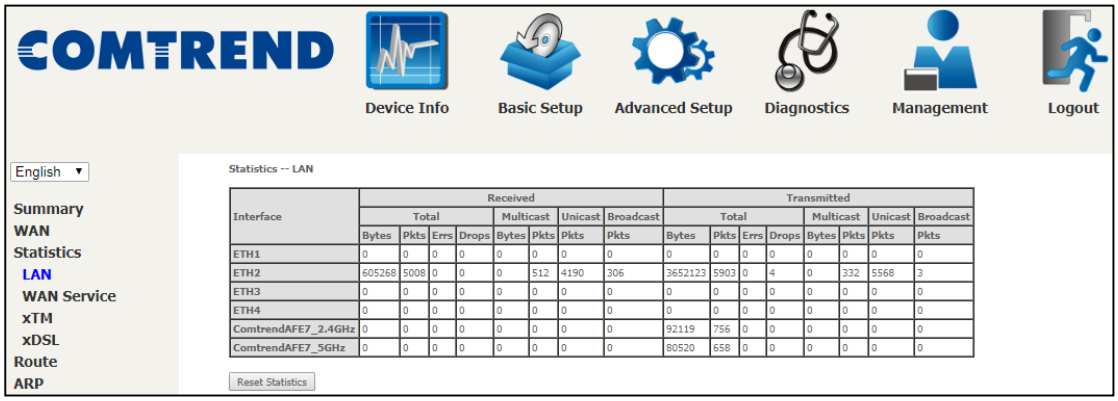
4.2 Statistics

This selection provides LAN, WAN, ATM and xDSL statistics.

NOTE:	These screens are updated automatically every 15 seconds. Click **Reset Statistics** to perform a manual update.

4.2.1 LAN Statistics

This screen shows data traffic statistics for each LAN interface.

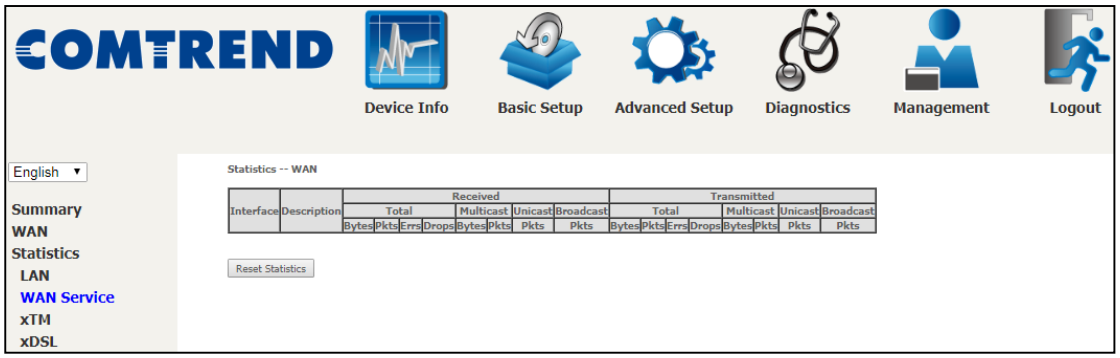


Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
ETH1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ETH2	605268	5008	0	0	0	512	4190	306	3652123	5903	0	4	0	332	5568	3
ETH3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ETH4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ComtrendAFE7_2.4GHz	0	0	0	0	0	0	0	0	92119	756	0	0	0	0	0	0
ComtrendAFE7_5GHz	0	0	0	0	0	0	0	0	80520	658	0	0	0	0	0	0

Heading	Description
Interface	LAN interface(s)
Received/Transmitted: - Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

4.2.2 WAN Service

This screen shows data traffic statistics for each WAN interface.



Heading	Description
Interface	WAN interfaces
Description	WAN service label
Received/Transmitted - Bytes - Pkts - Errs - Drops	Number of Bytes Number of Packets Number of packets with errors Number of dropped packets

4.2.3 XTM Statistics

The following figure shows ATM (Asynchronous Transfer Mode)/PTM (Packet Transfer Mode) statistics.

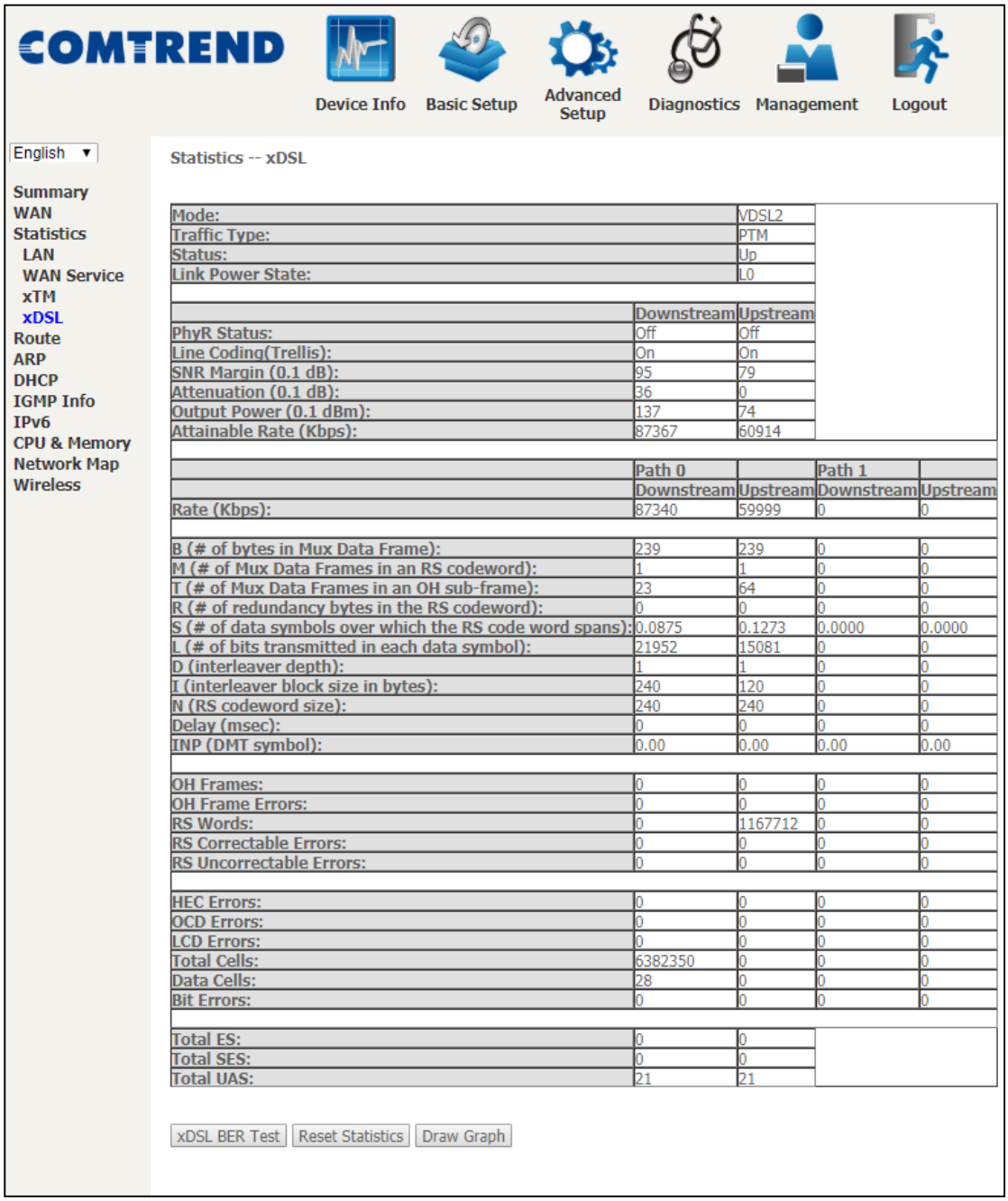
XTM Interface Statistics

Heading	Description
Port Number	ATM PORT (0-1)
In Octets	Number of octets received over the interface
Out Octets	Number of octets transmitted over the interface
In Packets	Number of packets received over the interface
Out Packets	Number of packets transmitted over the interface
In OAM Cells	Number of OAM Cells received over the interface
Out OAM Cells	Number of OAM Cells transmitted over the interface
In ASM Cells	Number of ASM Cells received over the interface
Out ASM Cells	Number of ASM Cells transmitted over the interface
In Packet Errors	Number of packets in Error
In Cell Errors	Number of cells in Error

4.2.4 xDSL Statistics

The xDSL Statistics screen displays information corresponding to the xDSL type. The two examples below (VDSL & ADSL) show this variation.

VDSL2

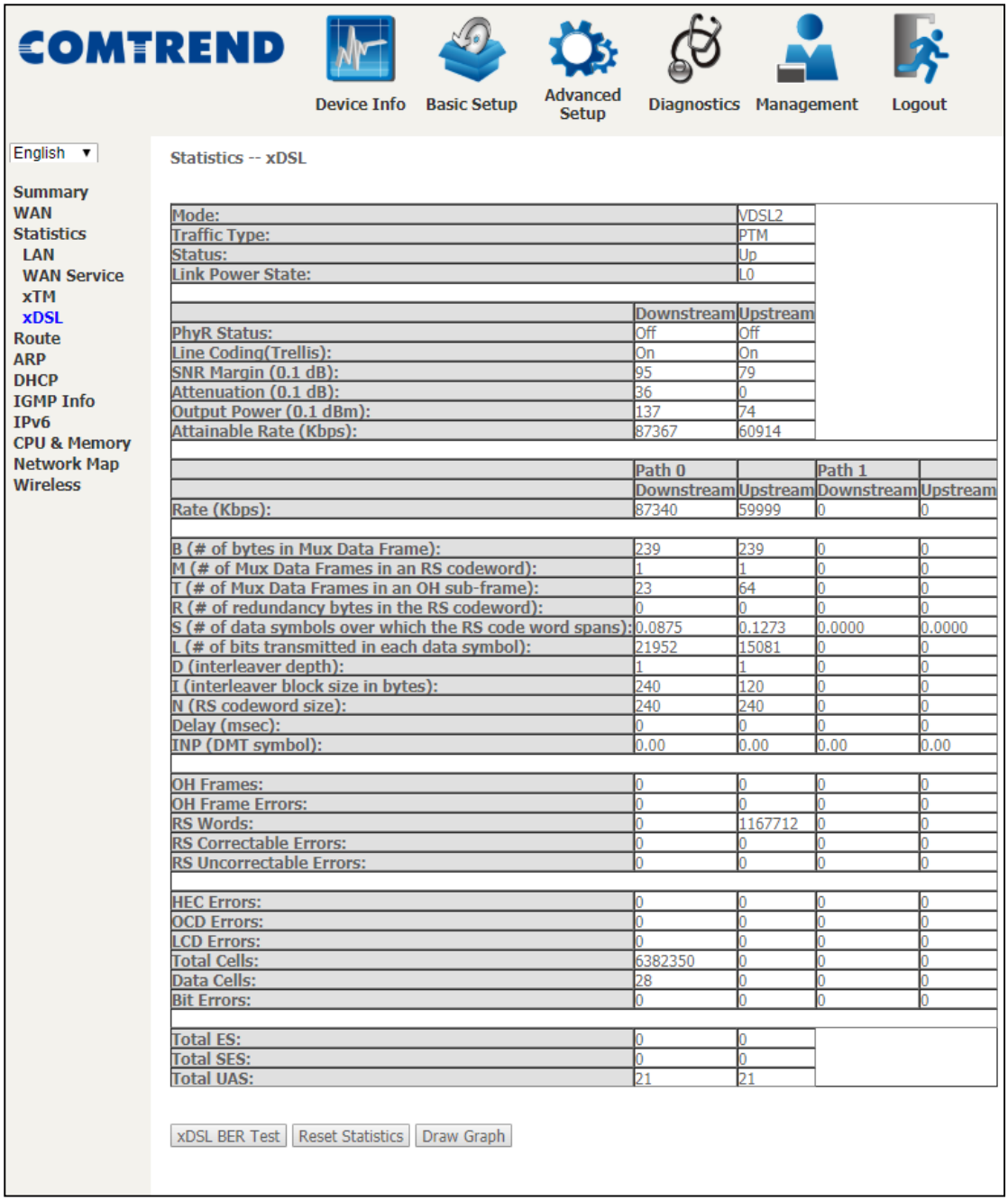


Mode:		VDSL2
Traffic Type:		PTM
Status:		Up
Link Power State:		L0

	Downstream	Upstream
PhyR Status:	Off	Off
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	95	79
Attenuation (0.1 dB):	36	0
Output Power (0.1 dBm):	137	74
Attainable Rate (Kbps):	87367	60914

	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	87340	59999	0	0
B (# of bytes in Mux Data Frame):	239	239	0	0
M (# of Mux Data Frames in an RS codeword):	1	1	0	0
T (# of Mux Data Frames in an OH sub-frame):	23	64	0	0
R (# of redundancy bytes in the RS codeword):	0	0	0	0
S (# of data symbols over which the RS code word spans):	0.0875	0.1273	0.0000	0.0000
L (# of bits transmitted in each data symbol):	21952	15081	0	0
D (interleaver depth):	1	1	0	0
I (interleaver block size in bytes):	240	120	0	0
N (RS codeword size):	240	240	0	0
Delay (msec):	0	0	0	0
INP (DMT symbol):	0.00	0.00	0.00	0.00
OH Frames:	0	0	0	0
OH Frame Errors:	0	0	0	0
RS Words:	0	1167712	0	0
RS Correctable Errors:	0	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	0	0	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	6382350	0	0	0
Data Cells:	28	0	0	0
Bit Errors:	0	0	0	0
Total ES:	0	0		
Total SES:	0	0		
Total UAS:	21	21		

ADSL2+



Mode:		VDSL2
Traffic Type:		PTM
Status:		Up
Link Power State:		L0

	Downstream	Upstream
PhyR Status:	Off	Off
Line Coding(Trellis):	On	On
SNR Margin (0.1 dB):	95	79
Attenuation (0.1 dB):	36	0
Output Power (0.1 dBm):	137	74
Attainable Rate (Kbps):	87367	60914

	Path 0		Path 1	
	Downstream	Upstream	Downstream	Upstream
Rate (Kbps):	87340	59999	0	0
B (# of bytes in Mux Data Frame):	239	239	0	0
M (# of Mux Data Frames in an RS codeword):	1	1	0	0
T (# of Mux Data Frames in an OH sub-frame):	23	64	0	0
R (# of redundancy bytes in the RS codeword):	0	0	0	0
S (# of data symbols over which the RS code word spans):	0.0875	0.1273	0.0000	0.0000
L (# of bits transmitted in each data symbol):	21952	15081	0	0
D (interleaver depth):	1	1	0	0
I (interleaver block size in bytes):	240	120	0	0
N (RS codeword size):	240	240	0	0
Delay (msec):	0	0	0	0
INP (DMT symbol):	0.00	0.00	0.00	0.00
OH Frames:	0	0	0	0
OH Frame Errors:	0	0	0	0
RS Words:	0	1167712	0	0
RS Correctable Errors:	0	0	0	0
RS Uncorrectable Errors:	0	0	0	0
HEC Errors:	0	0	0	0
OCD Errors:	0	0	0	0
LCD Errors:	0	0	0	0
Total Cells:	6382350	0	0	0
Data Cells:	28	0	0	0
Bit Errors:	0	0	0	0
Total ES:	0	0		
Total SES:	0	0		
Total UAS:	21	21		

Click the **Reset Statistics** button to refresh this screen.

Field	Description
Mode	VDSL, VDSL2
Traffic Type	ATM, PTM
Status	Lists the status of the DSL link
Link Power State	Link output power state

Field	Description
phyR Status	Shows the status of PhyR™ (Physical Layer Re-Transmission) impulse noise protection
Line Coding (Trellis)	Trellis On/Off
SNR Margin (0.1 dB)	Signal to Noise Ratio (SNR) margin
Attenuation (0.1 dB)	Estimate of average loop attenuation in the downstream direction
Output Power (0.1 dBm)	Total upstream output power
Attainable Rate (Kbps)	The sync rate you would obtain
Rate (Kbps)	Current sync rates downstream/upstream

In ADSL2/VDSL mode, the following section is inserted.

MSGc	Number of bytes in overhead channel message
B	Number of bytes in Mux Data Frame
M	Number of Mux Data Frames in a RS codeword
T	Number of Mux Data Frames in an OH sub-frame
R	Number of redundancy bytes in the RS codeword
S	Number of data symbols the RS codeword spans
L	Number of bits transmitted in each data symbol
D	The interleaver depth
I	The interleaver block size in bytes
N	RS codeword size
Delay	The delay in milliseconds (msec)
INP	DMT symbol

Super Frames	Total number of super frames
Super Frame Errors	Number of super frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

OH Frames	Total number of OH frames
OH Frame Errors	Number of OH frames received with errors
RS Words	Total number of Reed-Solomon code errors
RS Correctable Errors	Total Number of RS with correctable errors
RS Uncorrectable Errors	Total Number of RS words with uncorrectable errors

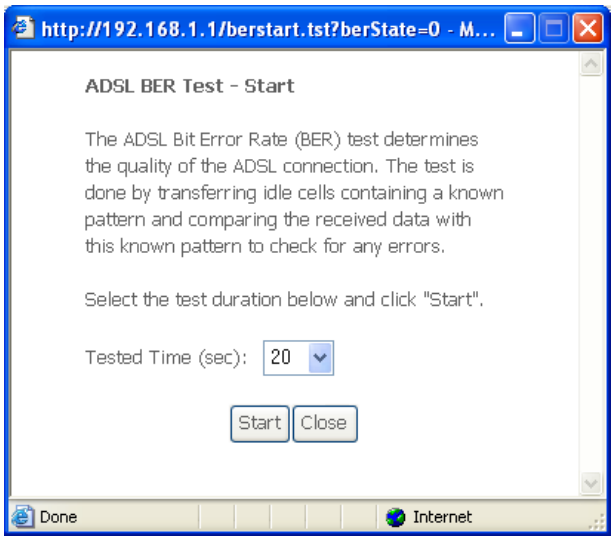
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of Out-of-Cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle + data cells)

Data Cells	Total number of ATM data cells
Bit Errors	Total number of bit errors

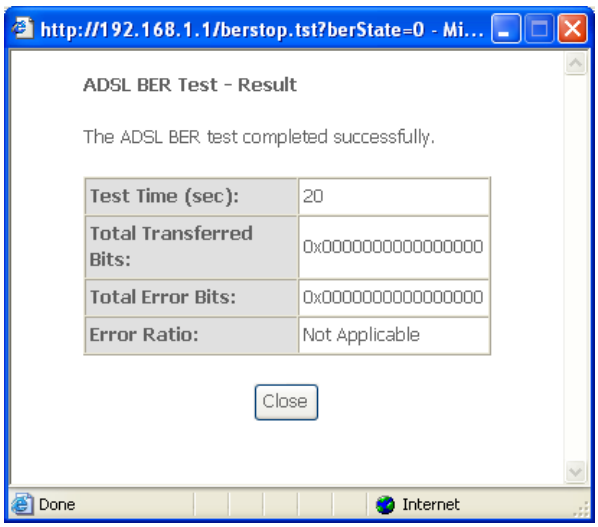
Total ES	Total Number of Errored Seconds
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

xDSL BER TEST

Click **xDSL BER Test** on the xDSL Statistics screen to test the Bit Error Rate (BER). A small pop-up window will open after the button is pressed, as shown below.

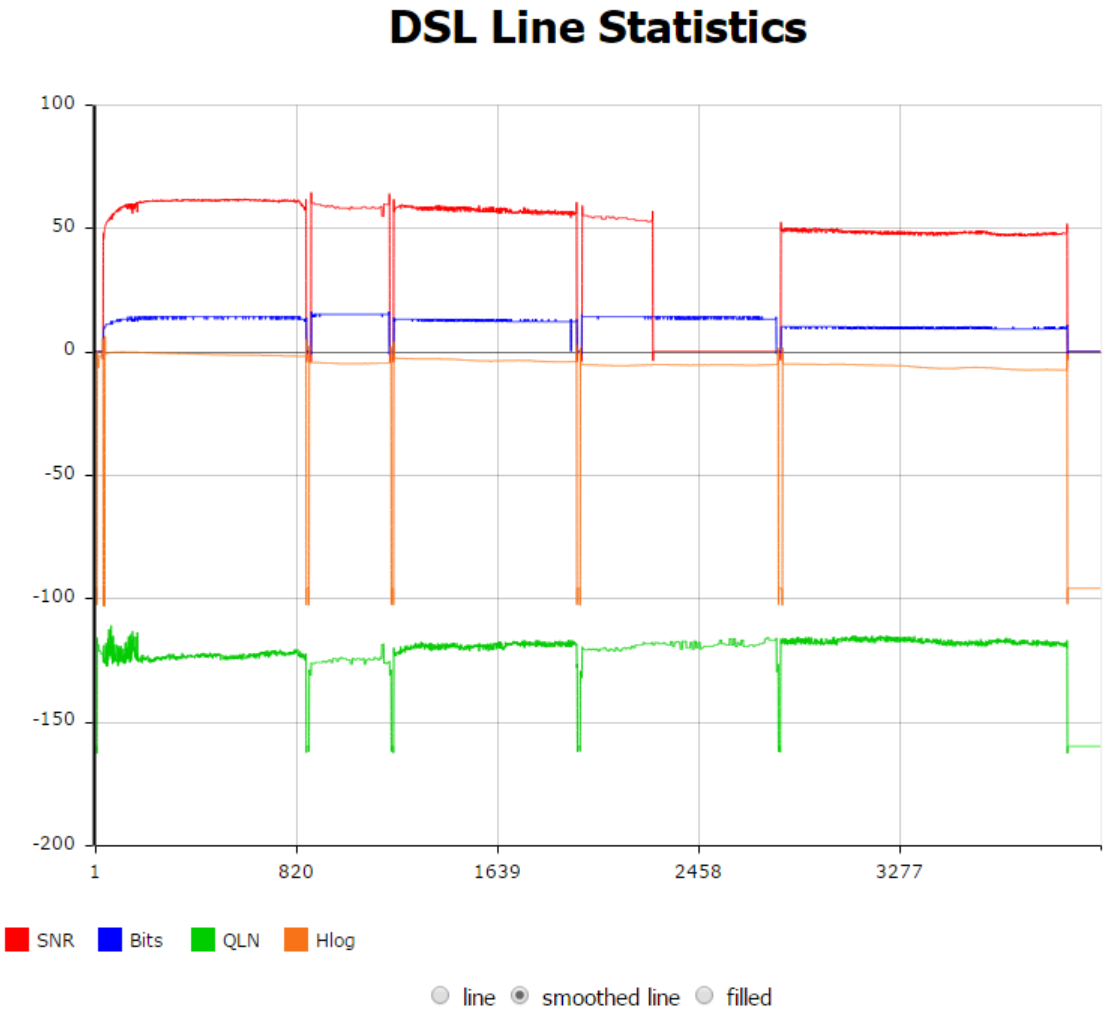


Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



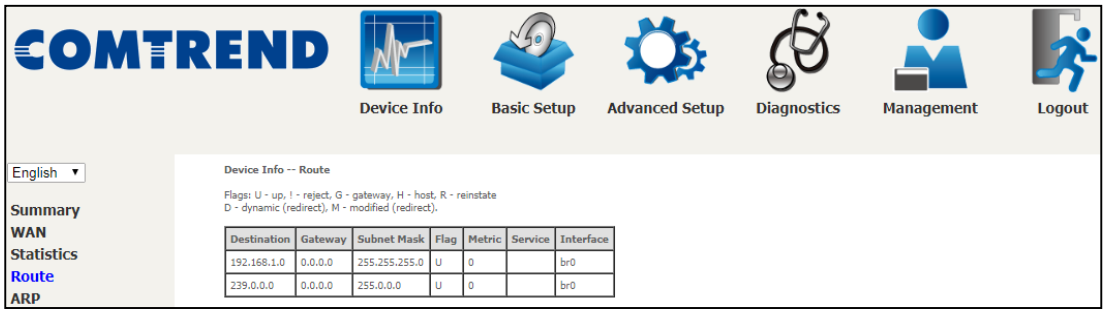
xDSL TONE GRAPH

Click **Draw Graph** on the xDSL Statistics screen and a pop-up window will display the xDSL statistics graph, including SNR, Bits per tone, QLN and Hlog of the xDSL line connection, as shown below.



4.3 Route

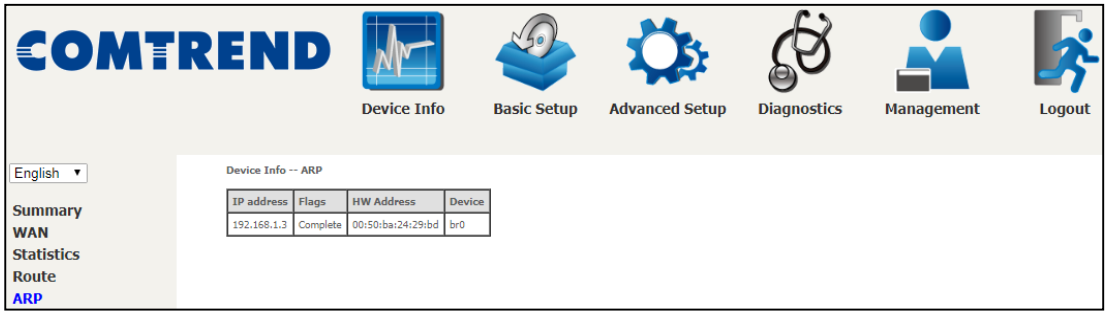
Choose **Route** to display the routes that the VR-3063 has found.



Field	Description
Destination	Destination network or destination host
Gateway	Next hop IP address
Subnet Mask	Subnet Mask of Destination
Flag	U: route is up !: reject route G: use gateway H: target is a host R: reinstate route for dynamic routing D: dynamically installed by daemon or redirect M: modified from routing daemon or redirect
Metric	The 'distance' to the target (usually counted in hops). It is not used by recent kernels, but may be needed by routing daemons.
Service	Shows the WAN connection label
Interface	Shows connection interfaces

4.4 ARP

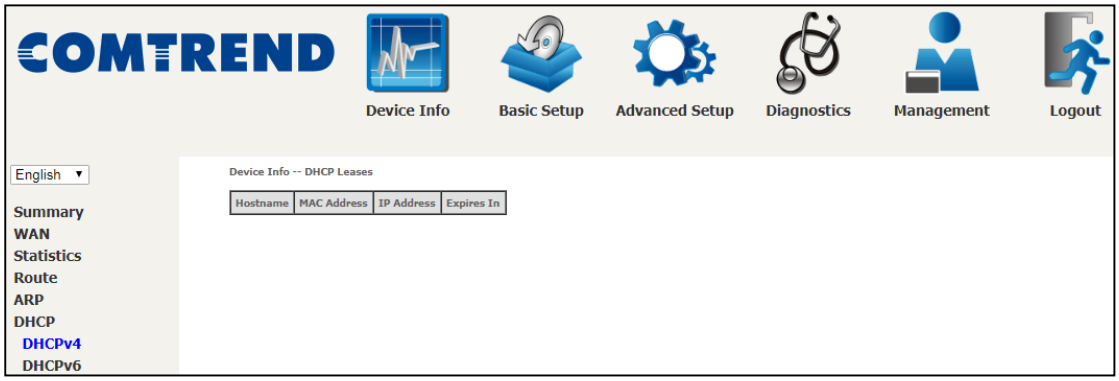
Click **ARP** to display the ARP information.



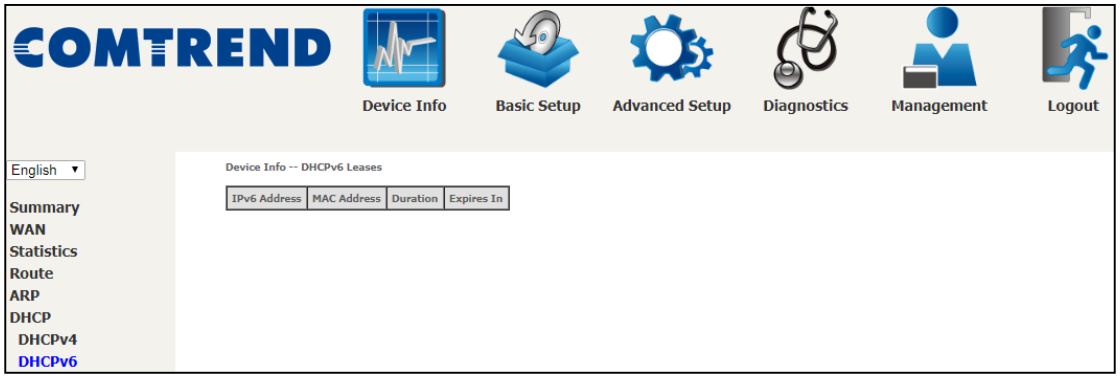
Field	Description
IP address	Shows IP address of host PC
Flags	Complete, Incomplete, Permanent, or Publish
HW Address	Shows the MAC address of host PC
Device	Shows the connection interface

4.5 DHCP

Click **DHCP** to display all DHCP Leases.



Field	Description
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP Address	Shows IP address of device/host/PC
Expires In	Shows how much time is left for each DHCP Lease



Field	Description
IPv6 Address	Shows IP address of device/host/PC
MAC Address	Shows the Ethernet MAC address of the device/host/PC
Duration	Shows leased time in hours
Expires In	Shows how much time is left for each DHCP Lease

4.6 IGMP Info

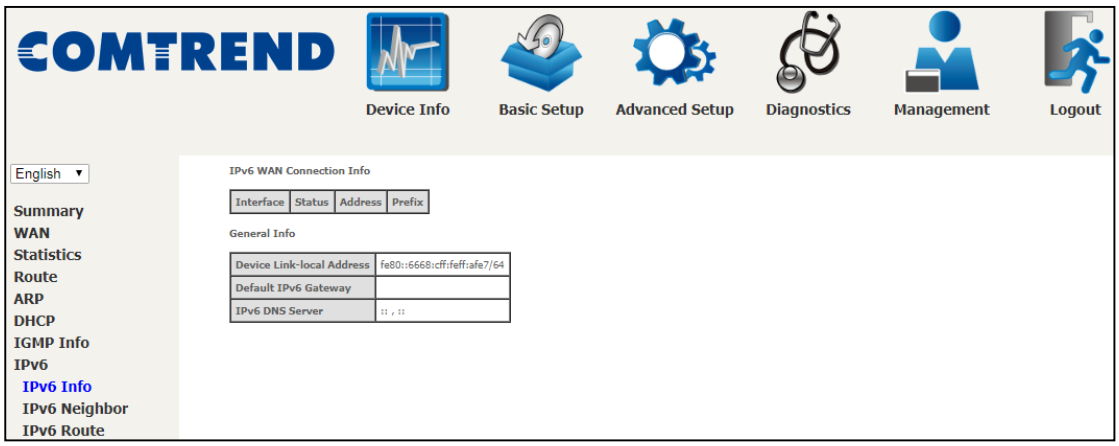
Click **IGMP Info** to display the list of IGMP entries broadcasting through the IGMP proxy enabled WAN connection.

Field	Description
Interface	The Source interface from which the IGMP report was received
WAN	The WAN interface from which the multicast traffic is received
Groups	The destination IGMP group address
Member	The Source IP from which the IGMP report was received
Timeout	The time remaining before the IGMP report expires

4.7 IPv6

4.7.1 IPv6 Info

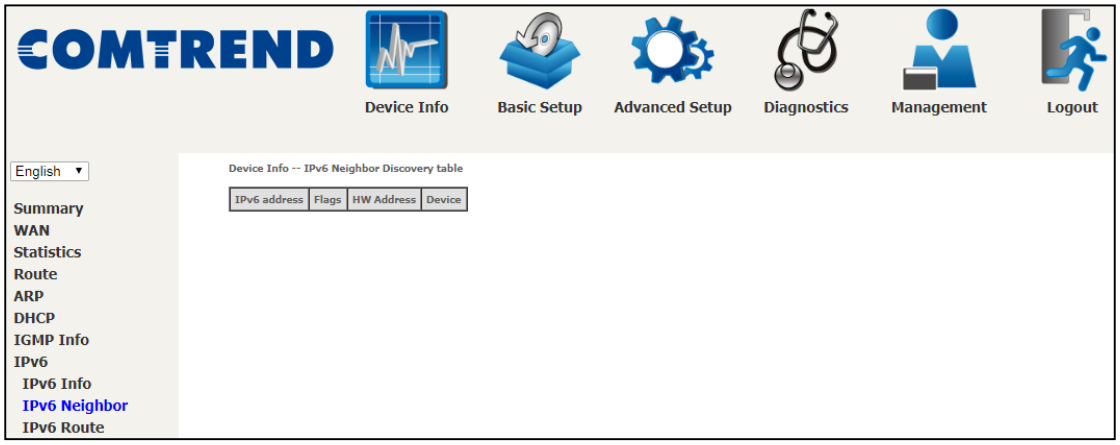
Click **IPv6 Info** to display the IPv6 WAN connection info.



Field	Description
Interface	WAN interface with IPv6 enabled
Status	Connection status of the WAN interface
Address	IPv6 Address of the WAN interface
Prefix	Prefix received/configured on the WAN interface
Device Link-local Address	The CPE's LAN Address
Default IPv6 Gateway	The default WAN IPv6 gateway
IPv6 DNS Server	The IPv6 DNS servers received from the WAN interface / configured manually

4.7.2 IPv6 Neighbor

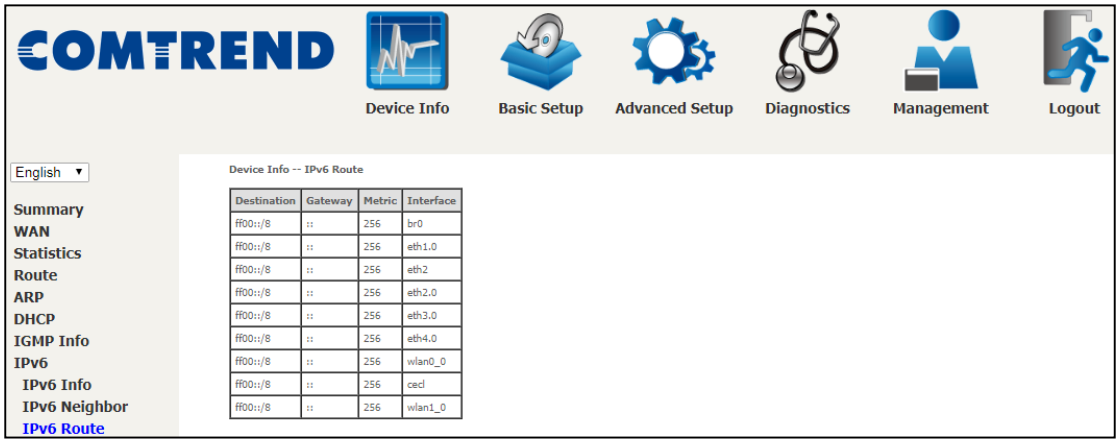
Click IPv6 Neighbor to display the list of IPv6 nodes discovered.



Field	Description
IPv6 Address	Ipv6 address of the device(s) found
Flags	Status of the neighbor device
HW Address	MAC address of the neighbor device
Device	Interface from which the device is located

4.7.3 IPv6 Route

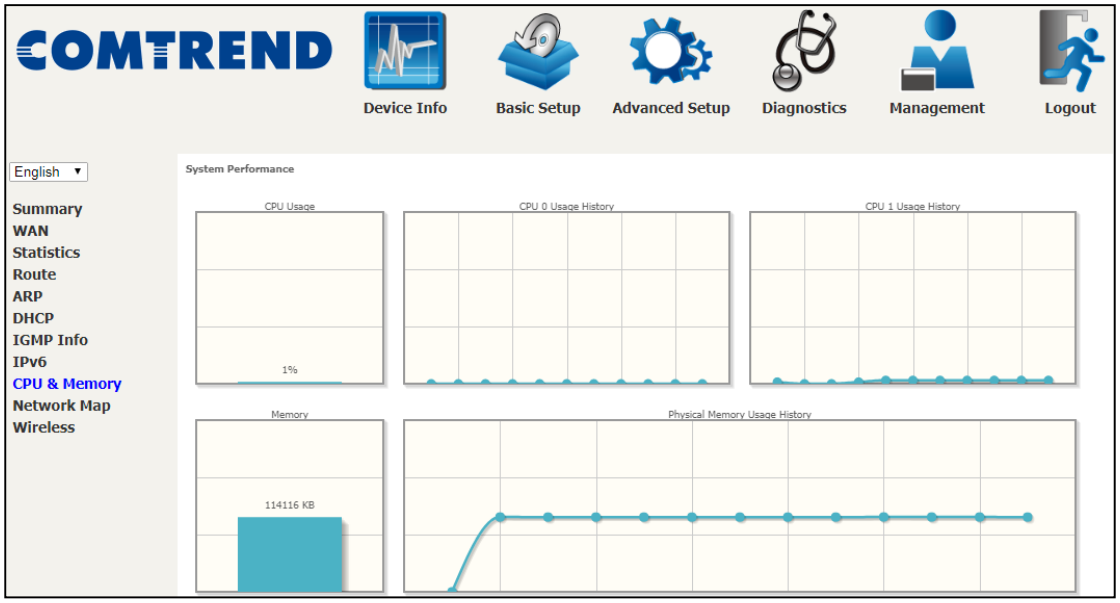
Click **IPv6 Route** to display the IPv6 route info.



Field	Description
Destination	Destination IP Address
Gateway	Gateway address used for destination IP
Metric	Metric specified for gateway
Interface	Interface used for destination IP

4.8 CPU & Memory

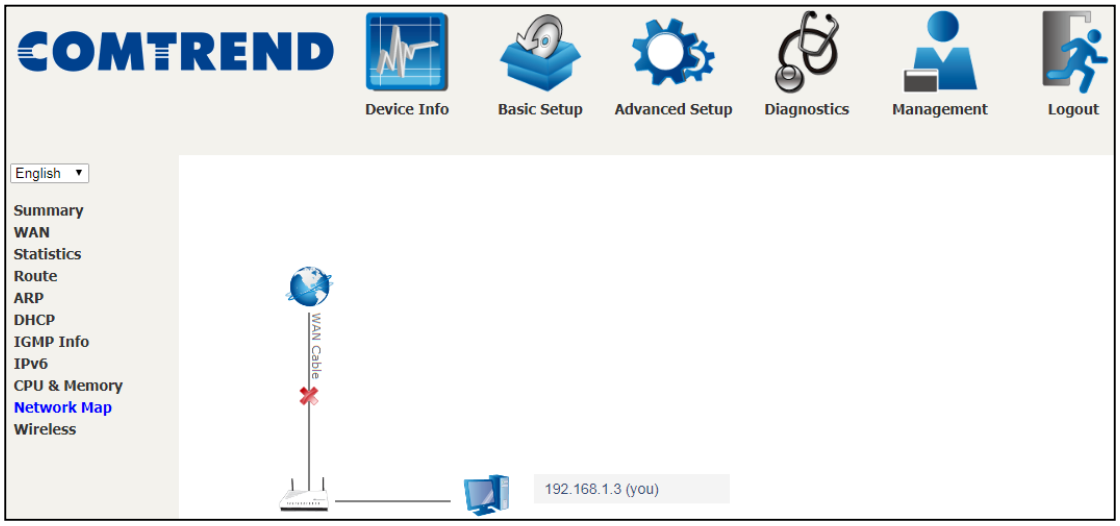
Displays the system performance graphs. Shows the current loading of the CPU and memory usage with dynamic updates.



4.9 Network Map

The network map is a graphical representation of router's wan status and LAN devices.

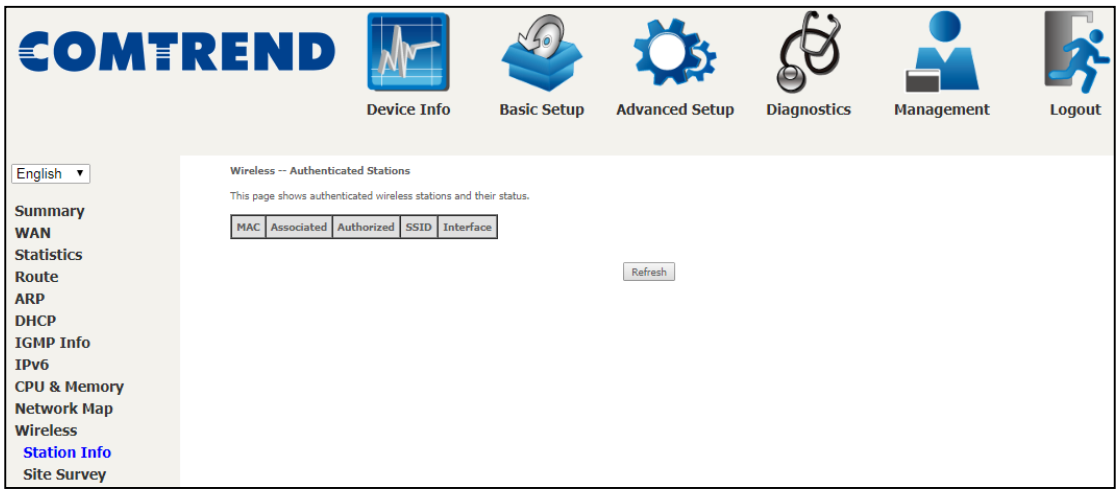
Note: This graph is unavailable for Internet Explorer users.



4.10 Wireless

4.10.1 Station Info

This page shows authenticated wireless stations and their status. Click the **Refresh** button to update the list of stations in the WLAN.



Consult the table below for descriptions of each column heading.

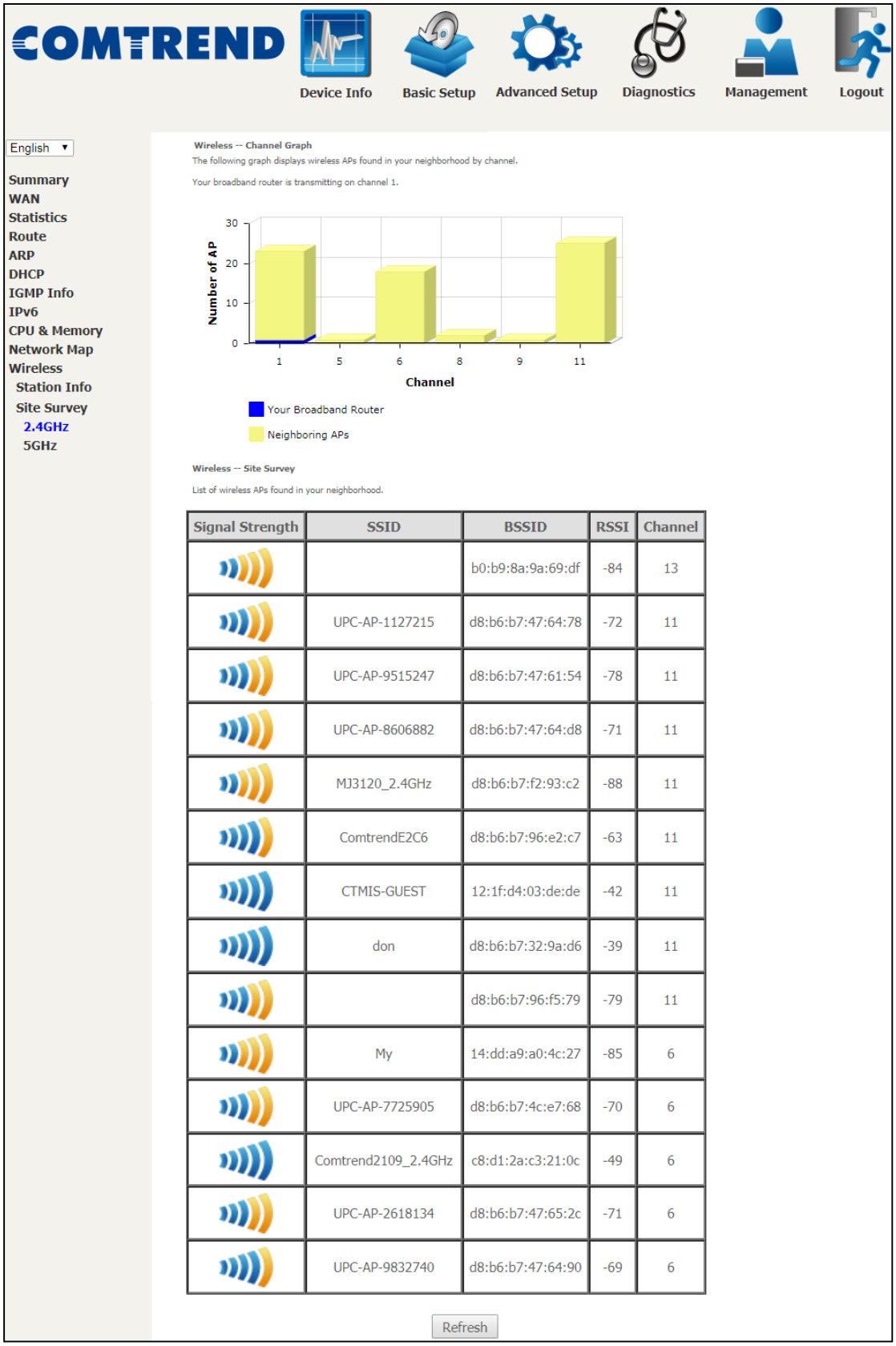
Field	Description
MAC	Lists the MAC address of all the stations.

Field	Description
Associated	Lists all the stations that are associated with the Access Point, along with the amount of time since packets were transferred to and from each station. If a station is idle for too long, it is removed from this list.
Authorized	Lists those devices with authorized access.
SSID	Lists which SSID of the modem that the stations connect to.
Interface	Lists which interface of the modem that the stations connect to.

4.10.2 Site Survey

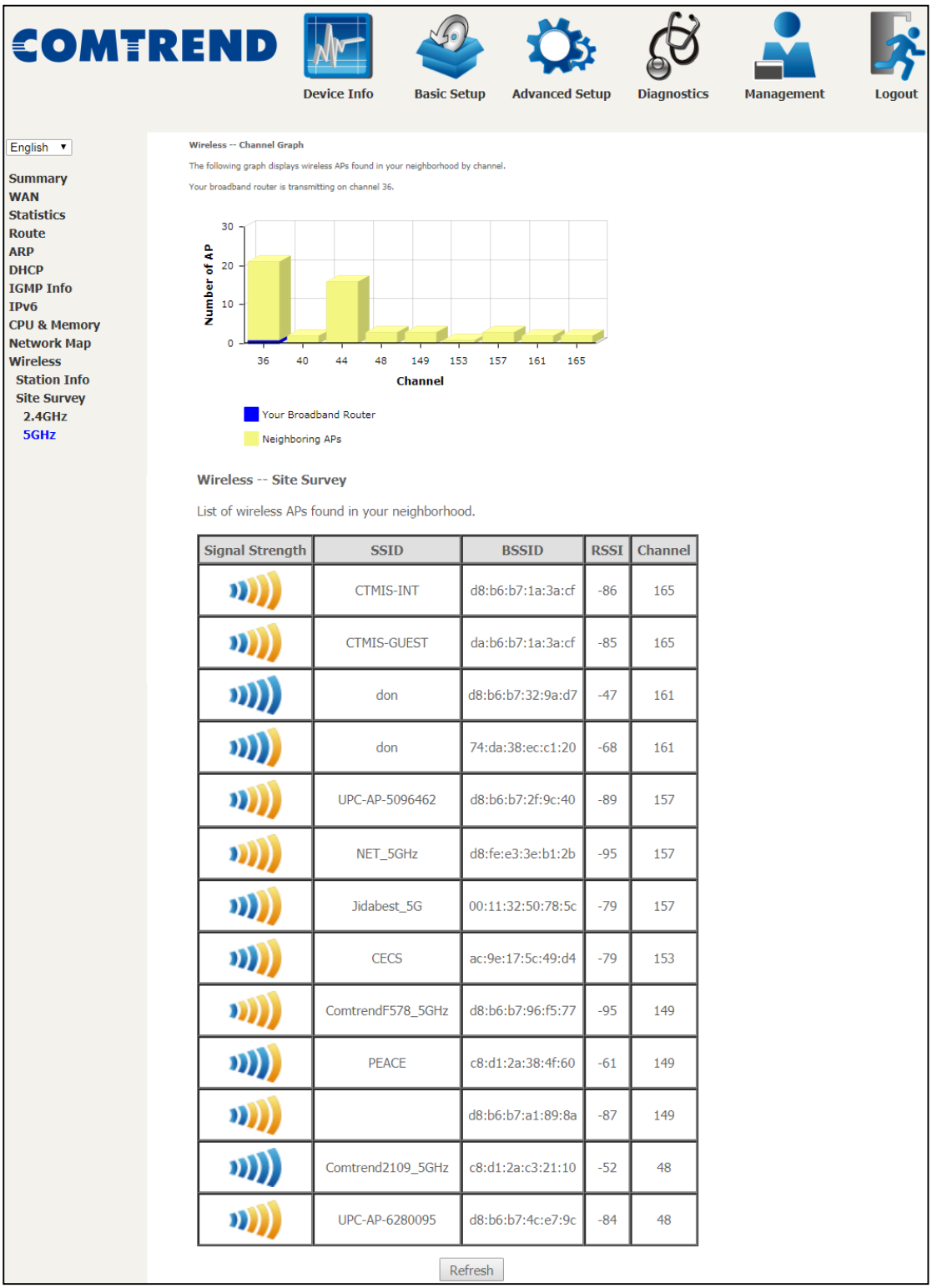
The graph displays wireless APs found in your neighborhood by channel.

2.4GHz



Signal Strength	SSID	BSSID	RSSI	Channel
		b0:b9:8a:9a:69:df	-84	13
	UPC-AP-1127215	d8:b6:b7:47:64:78	-72	11
	UPC-AP-9515247	d8:b6:b7:47:61:54	-78	11
	UPC-AP-8606882	d8:b6:b7:47:64:d8	-71	11
	MJ3120_2.4GHz	d8:b6:b7:f2:93:c2	-88	11
	ComtrendE2C6	d8:b6:b7:96:e2:c7	-63	11
	CTMIS-GUEST	12:1f:d4:03:de:de	-42	11
	don	d8:b6:b7:32:9a:d6	-39	11
		d8:b6:b7:96:f5:79	-79	11
	My	14:dd:a9:a0:4c:27	-85	6
	UPC-AP-7725905	d8:b6:b7:4c:e7:68	-70	6
	Comtrend2109_2.4GHz	c8:d1:2a:c3:21:0c	-49	6
	UPC-AP-2618134	d8:b6:b7:47:65:2c	-71	6
	UPC-AP-9832740	d8:b6:b7:47:64:90	-69	6

5GHz

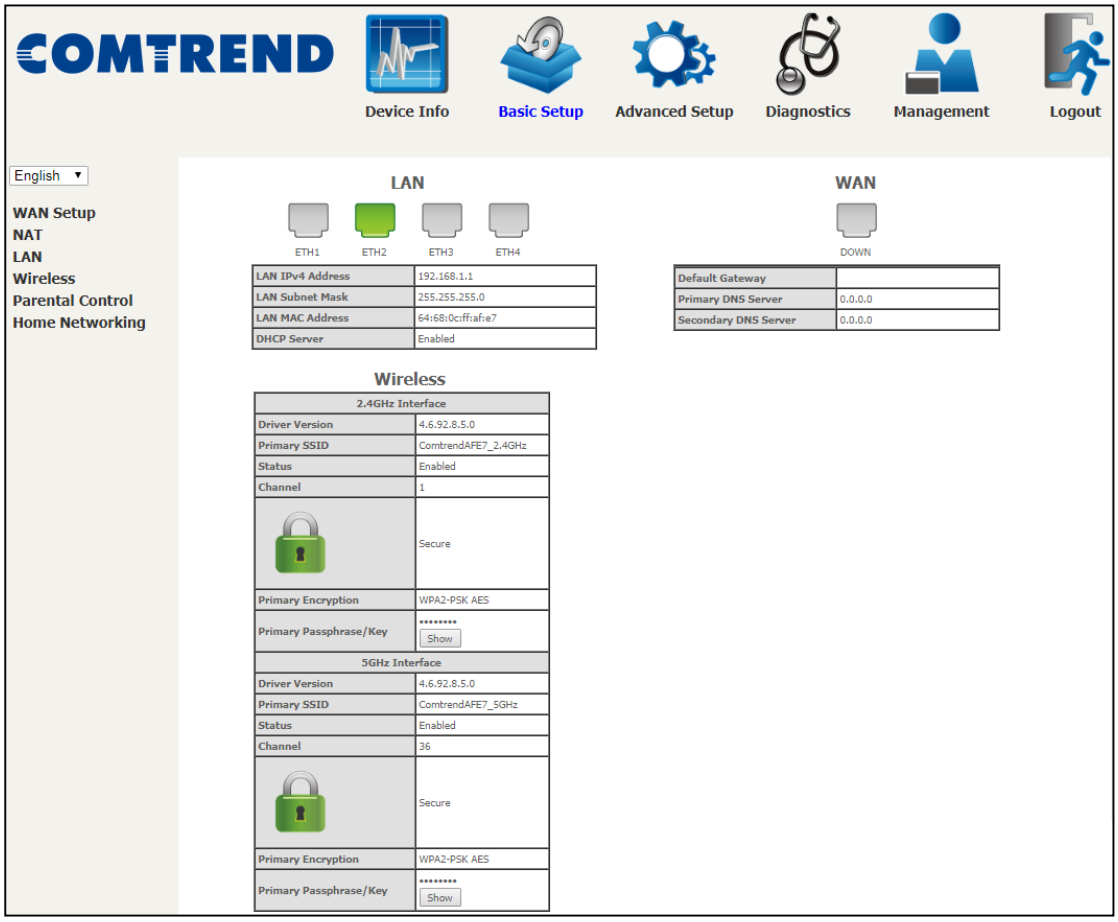


Signal Strength	SSID	BSSID	RSSI	Channel
	CTMIS-INT	d8:b6:b7:1a:3a:cf	-86	165
	CTMIS-GUEST	da:b6:b7:1a:3a:cf	-85	165
	don	d8:b6:b7:32:9a:d7	-47	161
	don	74:da:38:ec:c1:20	-68	161
	UPC-AP-5096462	d8:b6:b7:2f:9c:40	-89	157
	NET_5GHz	d8:fe:e3:3e:b1:2b	-95	157
	Jidabest_5G	00:11:32:50:78:5c	-79	157
	CECS	ac:9e:17:5c:49:d4	-79	153
	ComtrendF578_5GHz	d8:b6:b7:96:f5:77	-95	149
	PEACE	c8:d1:2a:38:4f:60	-61	149
		d8:b6:b7:a1:89:8a	-87	149
	Comtrend2109_5GHz	c8:d1:2a:c3:21:10	-52	48
	UPC-AP-6280095	d8:b6:b7:4c:e7:9c	-84	48

Chapter 5 Basic Setup

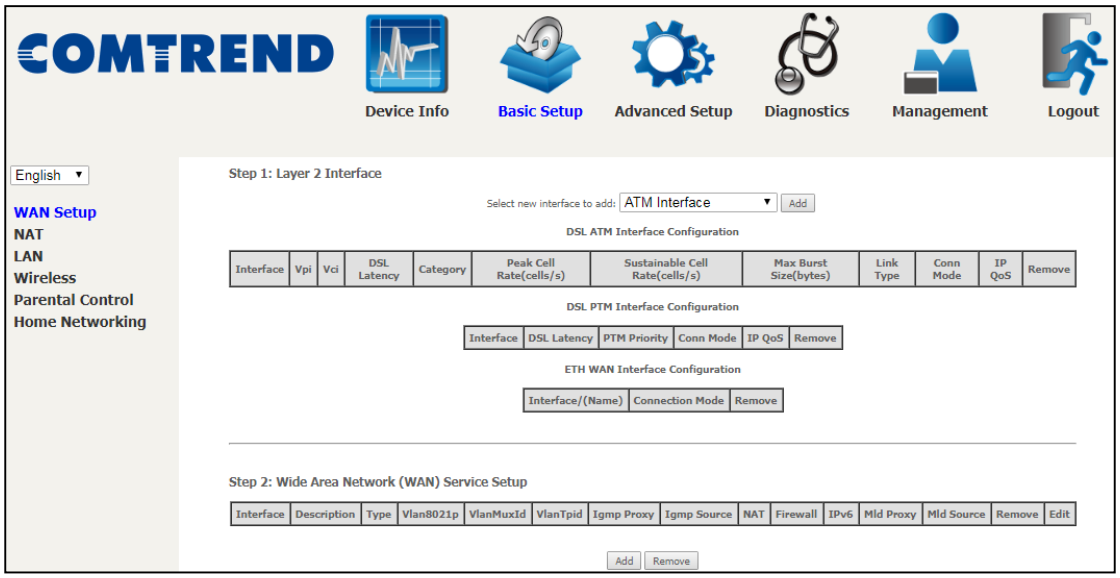
You can reach this page by clicking on the following icon located at the top of the screen.

This will bring you to the following screen.



5.1 Wan Setup

Click WAN Setup on the on the left of your screen.
Add or remove ATM, PTM and ETH WAN interface connections here.

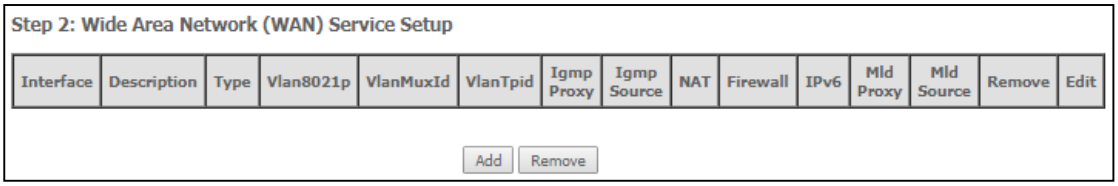


Click **Add** to create a new Layer 2 Interface (see Appendix F - Connection Setup).

To remove a connection, click the **Remove** button.

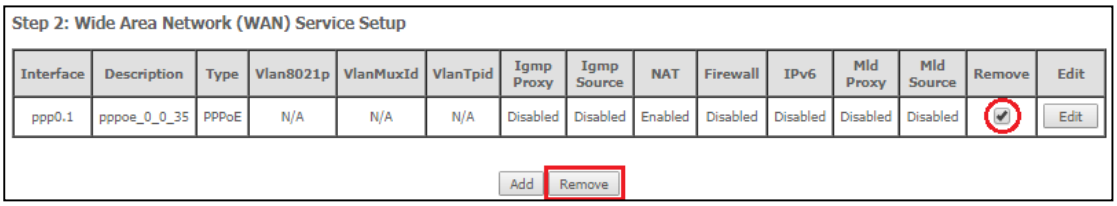
5.1.1 WAN Service Setup

This screen allows for the configuration of WAN interfaces.



Click the **Add** button to create a new connection. For connections on ATM or PTM or ETH WAN interfaces see Appendix F - Connection Setup.

To remove a connection, select its Remove column radio button and click **Remove.**



Heading	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
Vlan8021p	VLAN ID is used for VLAN Tagging (IEEE 802.1Q)
VlanMuxId	Shows 802.1Q VLAN ID
VlanTpid	VLAN Tag Protocol Identifier
IGMP Proxy	Shows Internet Group Management Protocol (IGMP) Proxy status
IGMP Source	Shows the status of WAN interface used as IGMP source
NAT	Shows Network Address Translation (NAT) status
Firewall	Shows the Security status
IPv6	Shows the WAN IPv6 address
MLD Proxy	Shows Multicast Listener Discovery (MLD) Proxy status
Mld Source	Shows the status of WAN interface used as MLD source
Remove	Select interfaces to remove
Edit	Click the Edit button to make changes to the WAN interface.

To remove a connection, select its Remove column radio button and click **Remove.**

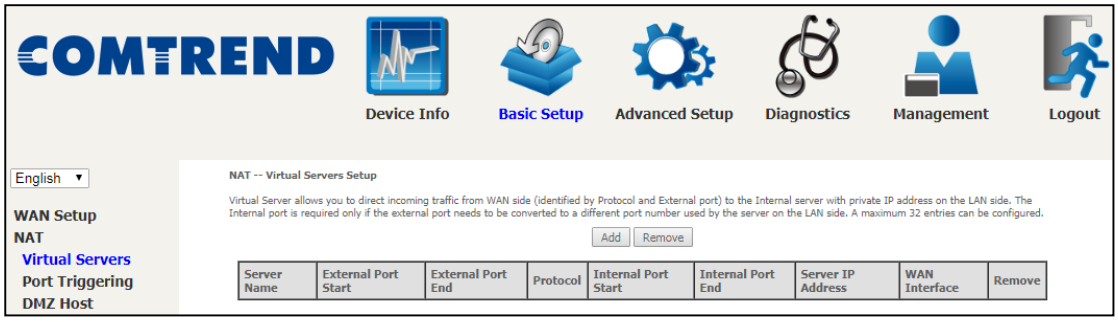
NOTE:	Up to 16 PVC profiles can be configured and saved in flash memory.

5.2 NAT

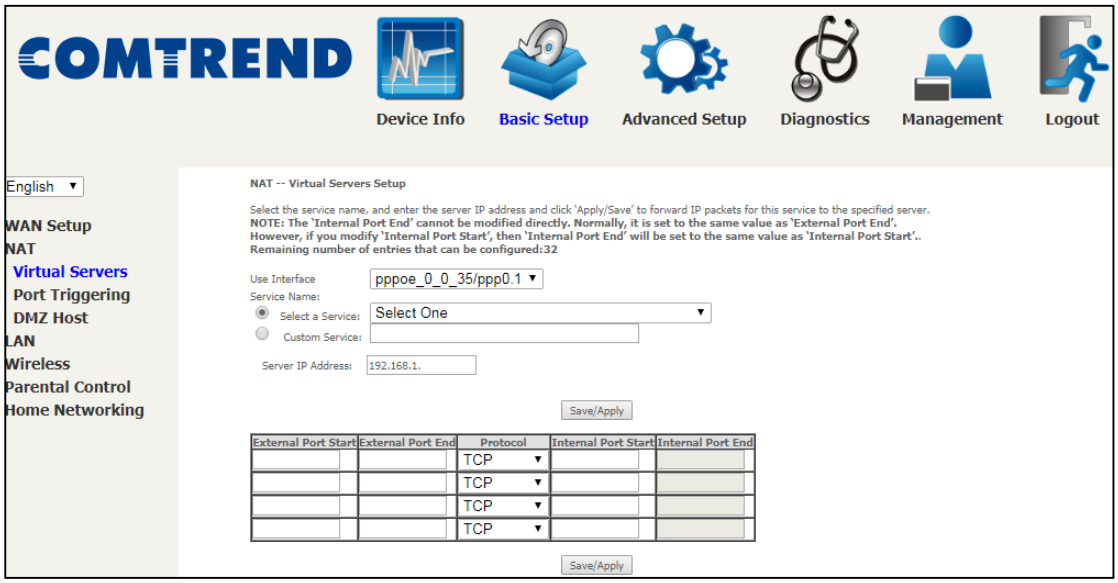
For NAT features under this section to work, NAT must be enabled in at least one PVC.

5.2.1 Virtual Servers

Virtual Servers allow you to direct incoming traffic from the WAN side (identified by Protocol and External port) to the internal server with private IP addresses on the LAN side. The Internal port is required only if the external port needs to be converted to a different port number used by the server on the LAN side.
A maximum of 32 entries can be configured.



To add a Virtual Server, click **Add**. The following will be displayed.



Click **Apply/Save** to apply and save the settings.

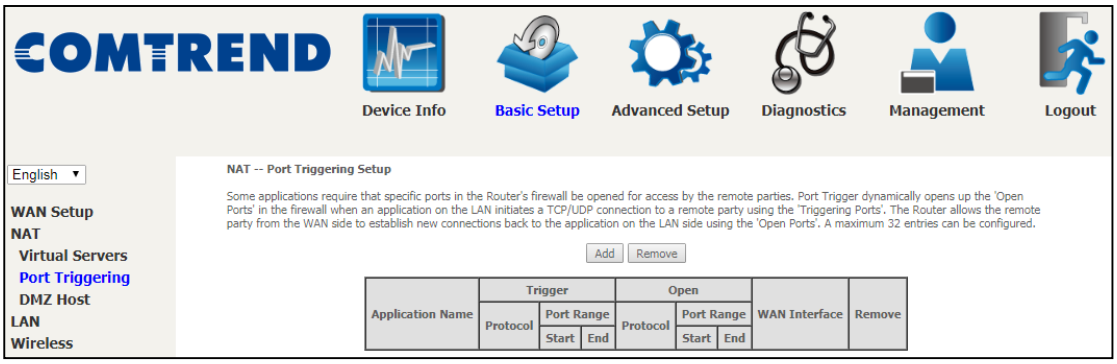
Consult the table below for field and header descriptions.

Field/Header	Description
Use Interface	Select a WAN interface from the drop-down menu.
Select a Service **Or** Custom Service	User should select the service from the list. **Or** User can enter the name of their choice.

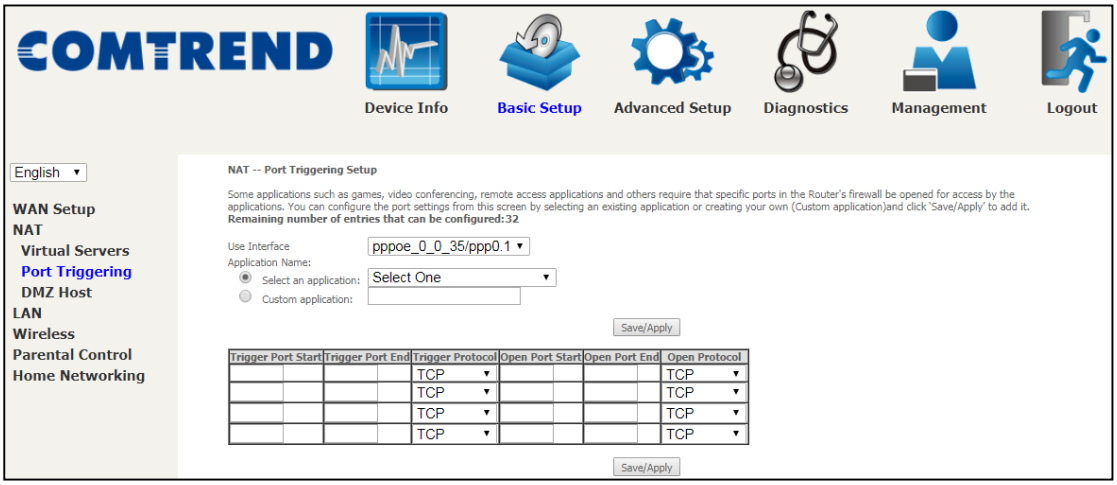
Field/Header	Description
Server IP Address	Enter the IP address for the server.
External Port Start	Enter the starting external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
External Port End	Enter the ending external port number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.
Protocol	TCP, TCP/UDP, or UDP.
Internal Port Start	Enter the internal port starting number (when you select Custom Server). When a service is selected the port ranges are automatically configured
Internal Port End	Enter the internal port ending number (when you select Custom Server). When a service is selected, the port ranges are automatically configured.

5.2.2 Port Triggering

Some applications require that specific ports in the firewall be opened for access by the remote parties. Port Triggers dynamically 'Open Ports' in the firewall when an application on the LAN initiates a TCP/UDP connection to a remote party using the 'Triggering Ports'. The Router allows the remote party from the WAN side to establish new connections back to the application on the LAN side using the 'Open Ports'. A maximum 32 entries can be configured.



To add a Trigger Port, click **Add**. The following will be displayed.



Click **Save/Apply** to save and apply the settings.

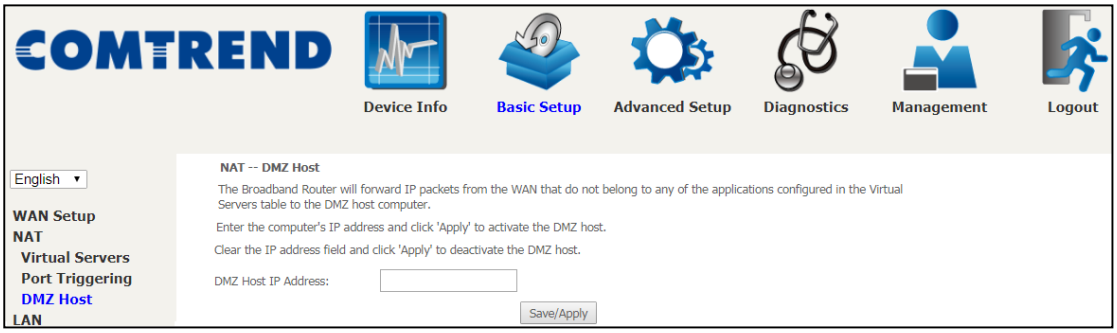
Consult the table below for field and header descriptions.

Field/Header	Description
Use Interface	Select a WAN interface from the drop-down menu.
Select an Application **Or** Custom Application	User should select the application from the list. **Or** User can enter the name of their choice.

Field/Header	Description
Trigger Port Start	Enter the starting trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Port End	Enter the ending trigger port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Trigger Protocol	TCP, TCP/UDP, or UDP.
Open Port Start	Enter the starting open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Port End	Enter the ending open port number (when you select custom application). When an application is selected, the port ranges are automatically configured.
Open Protocol	TCP, TCP/UDP, or UDP.

5.2.3 DMZ Host

The DSL router will forward IP packets from the WAN that do not belong to any of the applications configured in the Virtual Servers table to the DMZ host computer.



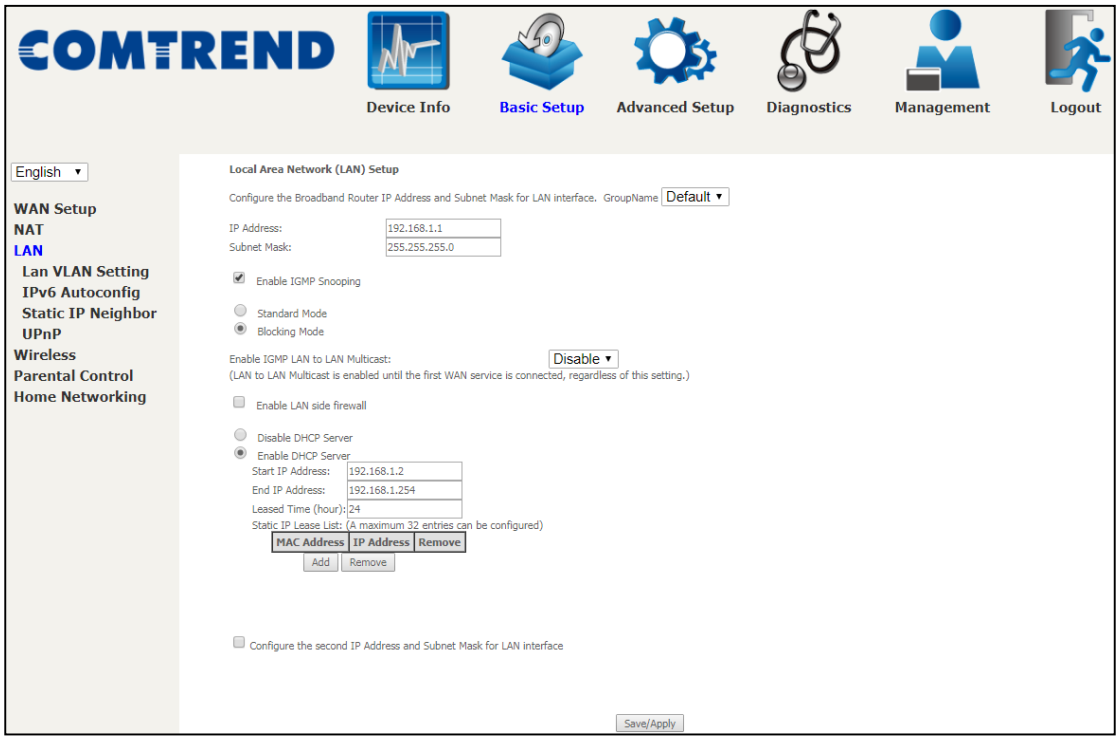
To **Activate** the DMZ host, enter the DMZ host IP address and click **Save/Apply**.

To **Deactivate** the DMZ host, clear the IP address field and click **Save/Apply**.

Enable NAT Loopback allows PC on the LAN side to access servers in the LAN network via the router's WAN IP.

5.3 LAN

Configure the LAN interface settings and then click **Apply/Save**.



Consult the field descriptions below for more details.

GroupName: Select an Interface Group.

<u>1st LAN INTERFACE</u>

IP Address: Enter the IP address for the LAN port.

Subnet Mask: Enter the subnet mask for the LAN port.

Enable IGMP Snooping:

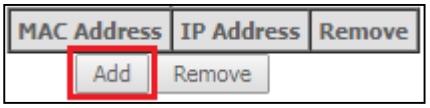
Standard Mode: In standard mode, multicast traffic will flood to all bridge ports when no client subscribes to a multicast group even if IGMP snooping is enabled.

Blocking Mode: In blocking mode, the multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group.

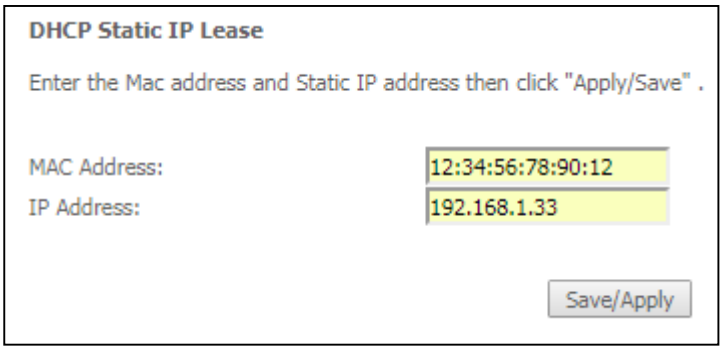
Enable IGMP LAN to LAN Multicast: Select Enable from the drop-down menu to allow IGMP LAN to LAN Multicast forwarding

Enable LAN side firewall: Enable by ticking the checkbox ☑.

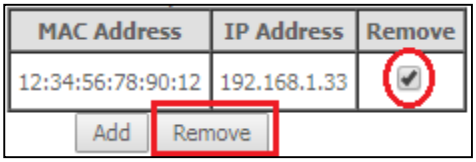
Static IP Lease List: A maximum of 32 entries can be configured.



To add an entry, enter MAC address and Static IP address and then click **Save/Apply**.



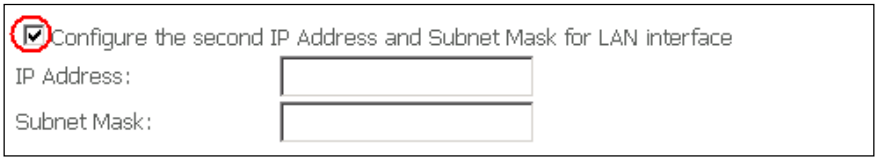
To remove an entry, tick the corresponding checkbox ☑ in the Remove column and then click the **Remove** button, as shown below.



Select **Enable DHCP Server Relay** (not available if **NAT** enabled), and enter the DHCP Server IP Address. This allows the Router to relay the DHCP packets to the remote DHCP server. The remote DHCP server will provide the IP address.

2ND LAN INTERFACE

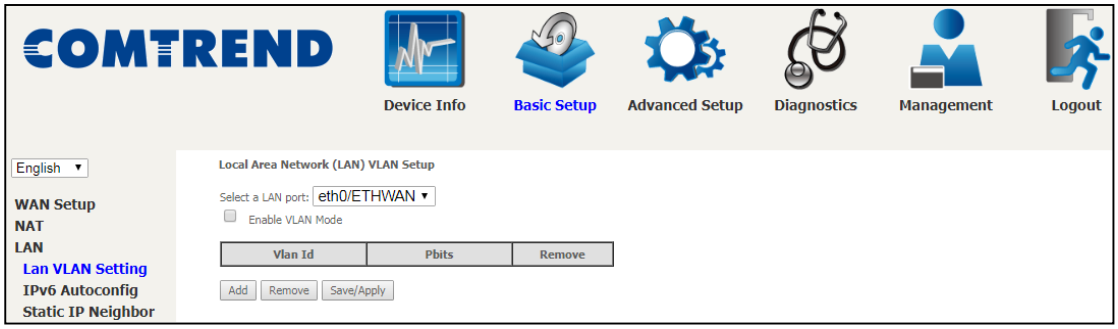
To configure a secondary IP address, tick the checkbox ☑ outlined (in RED) below.



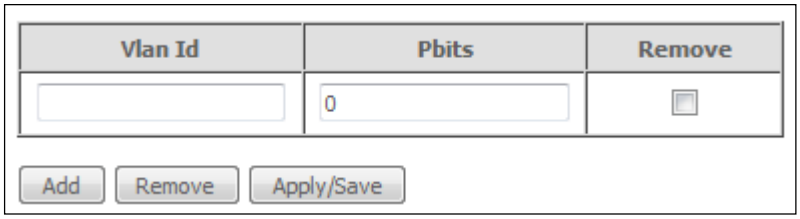
IP Address: Enter the secondary IP address for the LAN port.
Subnet Mask: Enter the secondary subnet mask for the LAN port.

5.3.1 Lan VLAN Setting

The CPE will tag VLAN on specific LAN port(s) when this feature is used.



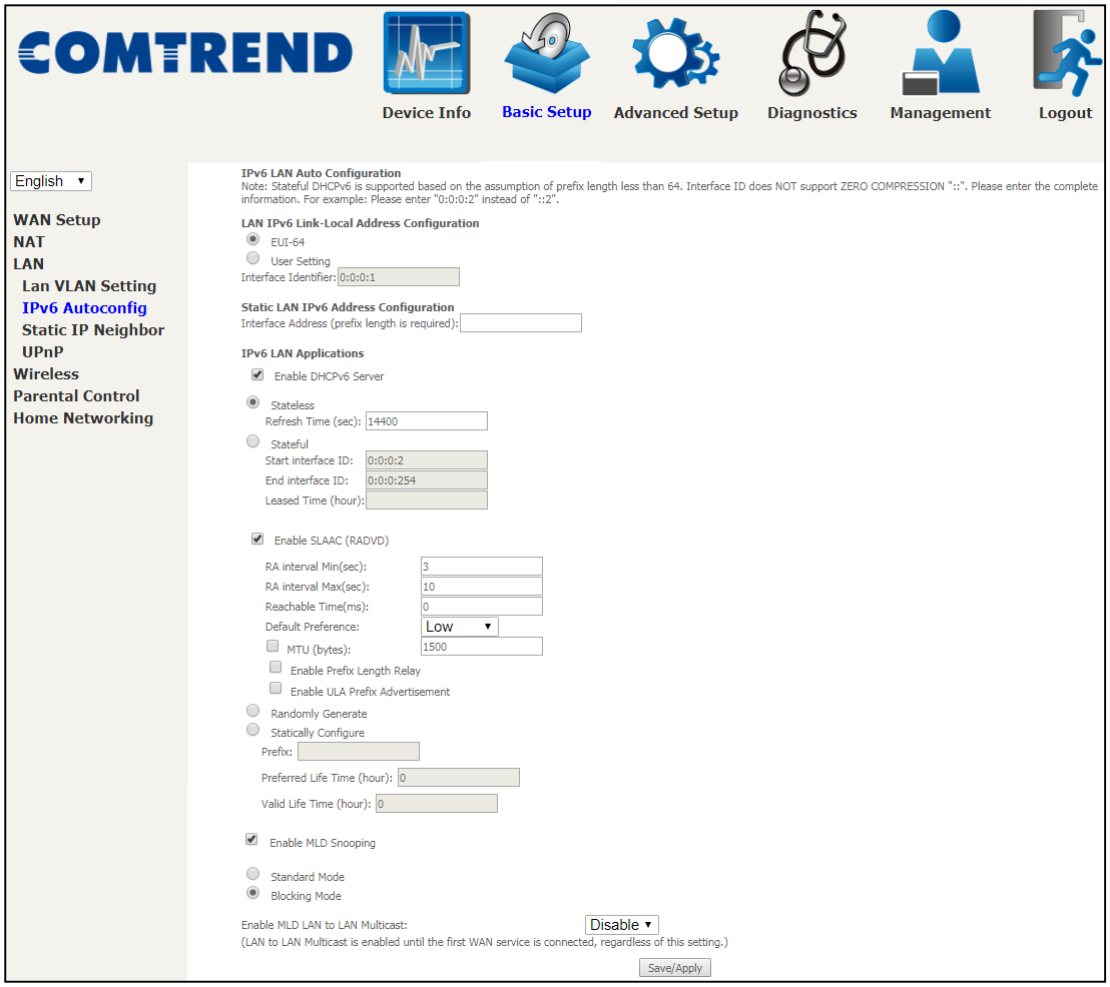
Click the **Add** button to display the following.



Heading	Description
Vlan ID	The VLAN ID to be supported on the LAN port.
pbits	The VLAN priority bit to be supported on the LAN port.
Remove	Tick the checkbox and click the Remove button to delete entries.

5.3.2 LAN IPv6 Autoconfig

Configure the LAN interface settings and then click **Save/Apply**.



Consult the field descriptions below for more details.

LAN IPv6 Link-Local Address Configuration

Heading	Description
EUI-64	Use EUI-64 algorithm to calculate link-local address from MAC address
User Setting	Use the Interface Identifier field to define a link-local address

Static LAN IPv6 Address Configuration

Heading	Description
Interface Address (prefix length is required):	Configure static LAN IPv6 address and subnet prefix length

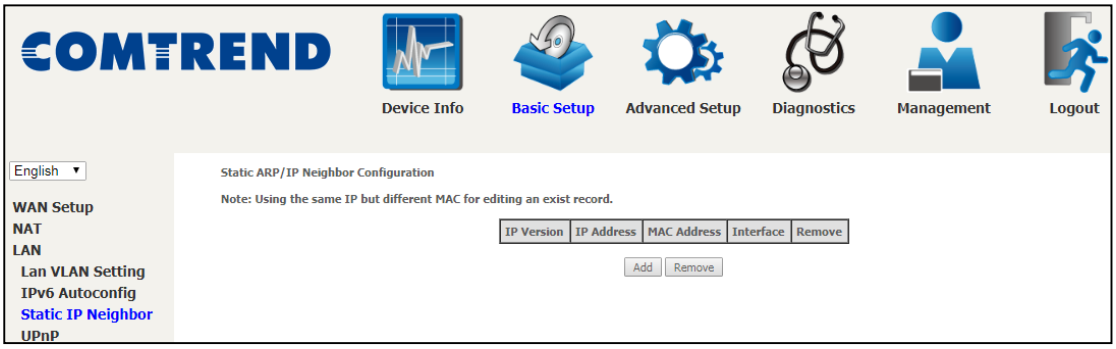
IPv6 LAN Applications

Heading	Description
Stateless	Use stateless configuration
Refresh Time (sec):	The information refresh time option specifies how long a client should wait before refreshing information retrieved from DHCPv6
Stateful	Use stateful configuration
Start interface ID:	Start of interface ID to be assigned to dhcpv6 client
End interface ID:	End of interface ID to be assigned to dhcpv6 client
Leased Time (hour):	Lease time for dhcpv6 client to use the assigned IP address

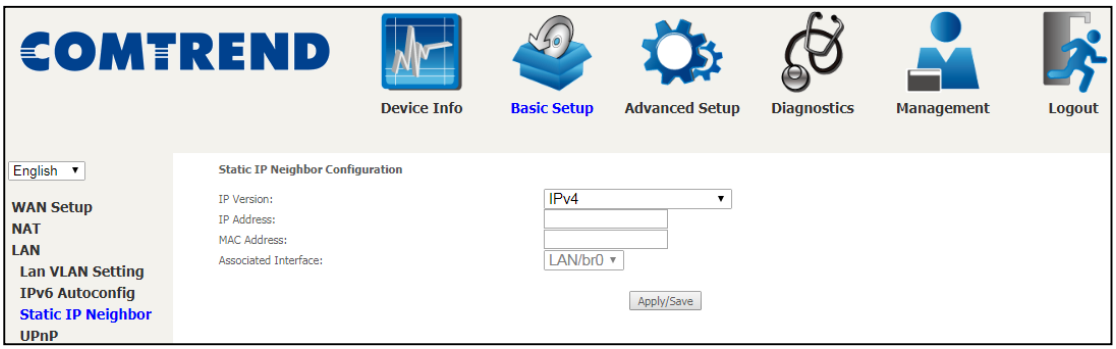
Heading	Description
Enable RADVD	Enable use of router advertisement daemon
RA interval Min(sec):	Minimum time to send router advertisement
RA interval Max(sec):	Maximum time to send router advertisement
Reachable Time(ms):	The time, in milliseconds that a neighbor is reachable after receiving reachability confirmation
Default Preference:	Preference level associated with the default router
MTU (bytes):	MTU value used in router advertisement messages to insure that all nodes on a link use the same MTU value
Enable Prefix Length Relay	Use prefix length receive from WAN interface
Enable ULA Prefix Advertisement	Allow RADVD to advertise Unique Local Address Prefix
Randomly Generate	Use a Randomly Generated Prefix
Statically Configure	Specify the prefix to be used
Prefix	The prefix to be used
Preferred Life Time (hour)	The preferred life time for this prefix
Valid Life Time (hour)	The valid life time for this prefix
Enable MLD Snooping	Enable/disable IPv6 multicast forward to LAN ports
Standard Mode Blocking Mode	In standard mode, IPv6 multicast traffic will flood to all bridge ports when no client subscribes to a multicast group even if MLD snooping is enabled In blocking mode, IPv6 multicast data traffic will be blocked and not flood to all bridge ports when there are no client subscriptions to any multicast group
Enable MLD LAN To LAN Multicast	Enable/disable IPv6 multicast between LAN ports

5.3.3 Static IP Neighbor

This page is used to configure a static IPv4 or IPv6 Neighbor entry. Static ARP entries will be created for these neighbor devices.



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



Click **Apply/Save** to apply and save the settings.

Heading	Description
IP Version	The IP version used for the neighbor device
IP Address	Define the IP Address for the neighbor device
MAC Address	The MAC Address of the neighbor device
Associated Interface	The interface where the neighbor device is located

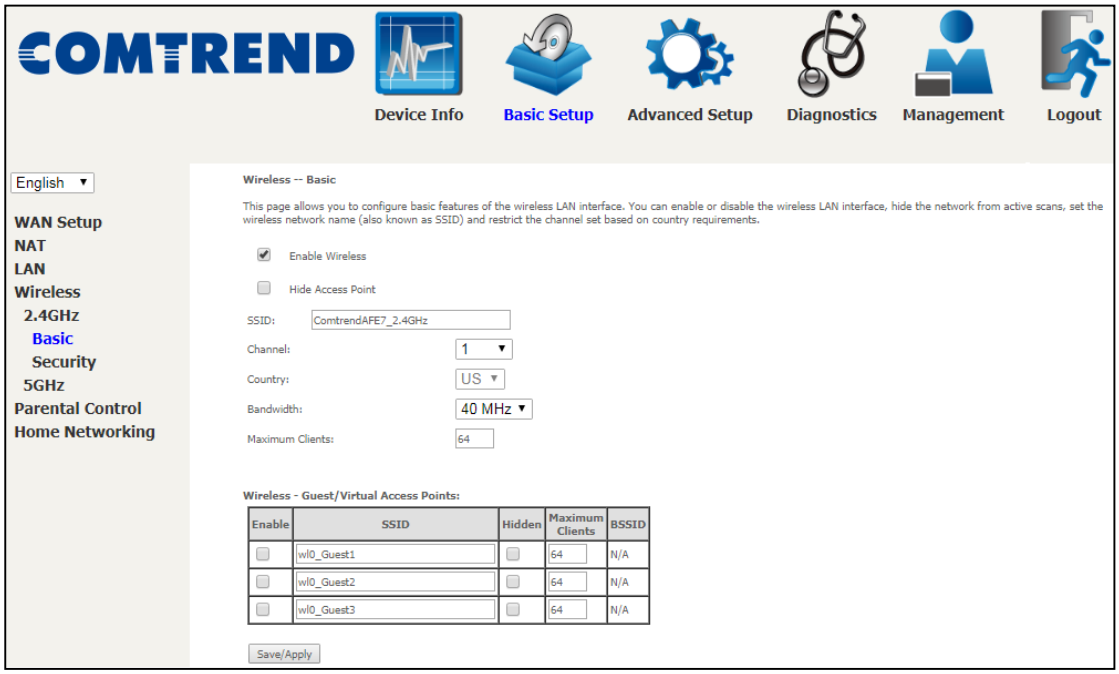
5.3.4 UPnP

Select the checkbox ☑ provided and click **Save/Apply** to enable UPnP protocol.

5.4 Wireless

5.4.1 Basic 2.4GHz

The Basic option allows you to configure basic features of the wireless LAN interface. Among other things, you can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and configure the channel setting for the wireless LAN interface.



Click the **Save/Apply** button to apply the selected wireless options.

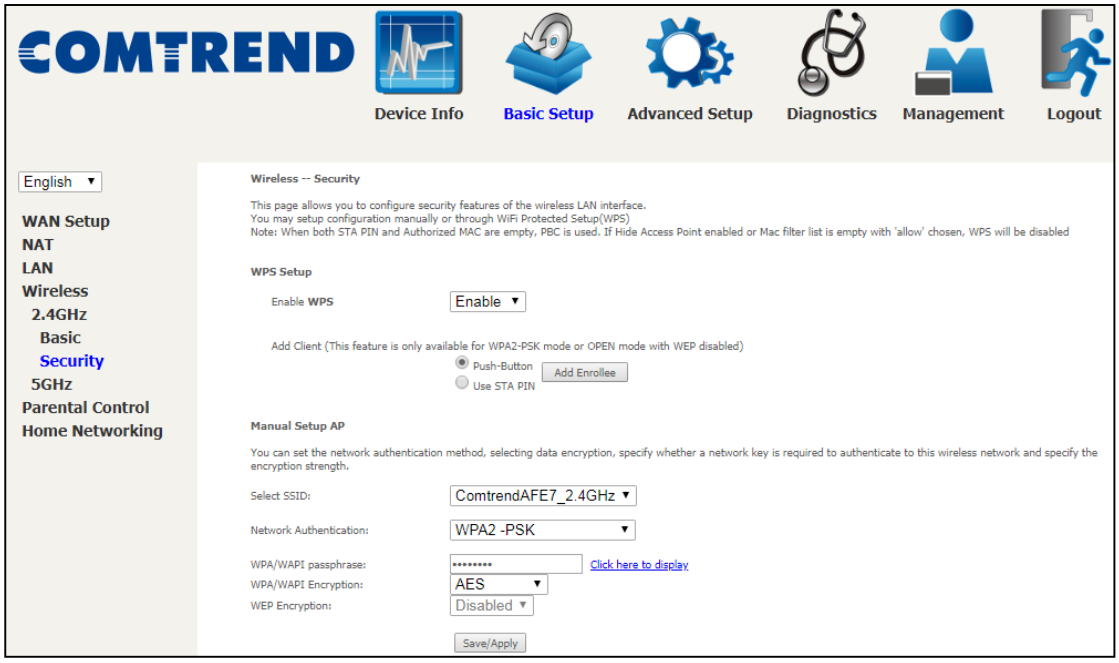
Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox ☑ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To view and connect to available wireless networks in Windows, open Connect to a Network by clicking the network icon (or) in the notification area. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.

Option	Description
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
Channel	Drop-down menu that allows selection of a specific channel.
Country	Local regulations limit channel range: US/Canada = 1-11.
Bandwidth	To utilize maximum data throughput, select 40MHz in 2.4G band.
Max Clients	The maximum number of clients that can access the router.
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes ☑ in the **Enabled** column. To hide a Guest SSID, select its checkbox ☑ in the **Hidden** column. Do the same for **Isolate Clients** and **Disable WMM Advertise**. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for **Enable WMF**, **Max Clients** and **BSSID**, consult the matching entries in this table. **NOTE:** Remote wireless hosts cannot scan Guest SSIDs.

5.4.2 Security 2.4GHz

The following screen appears when Wireless Security is selected. The options shown here allow you to configure security features of the wireless LAN interface.



WIRELESS SECURITY

Setup requires that the user configure these settings using the Web User Interface (see the table below).

Select SSID
Select the wireless network name from the drop-down menu. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that client will not be granted access.

Network Authentication
This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified. Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below.
Choosing **WPA2-PSK**, you must enter WPA/WAPI passphrase and Group Rekey Interval.
WEP Encryption
This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key.

Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic.
When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers.

Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

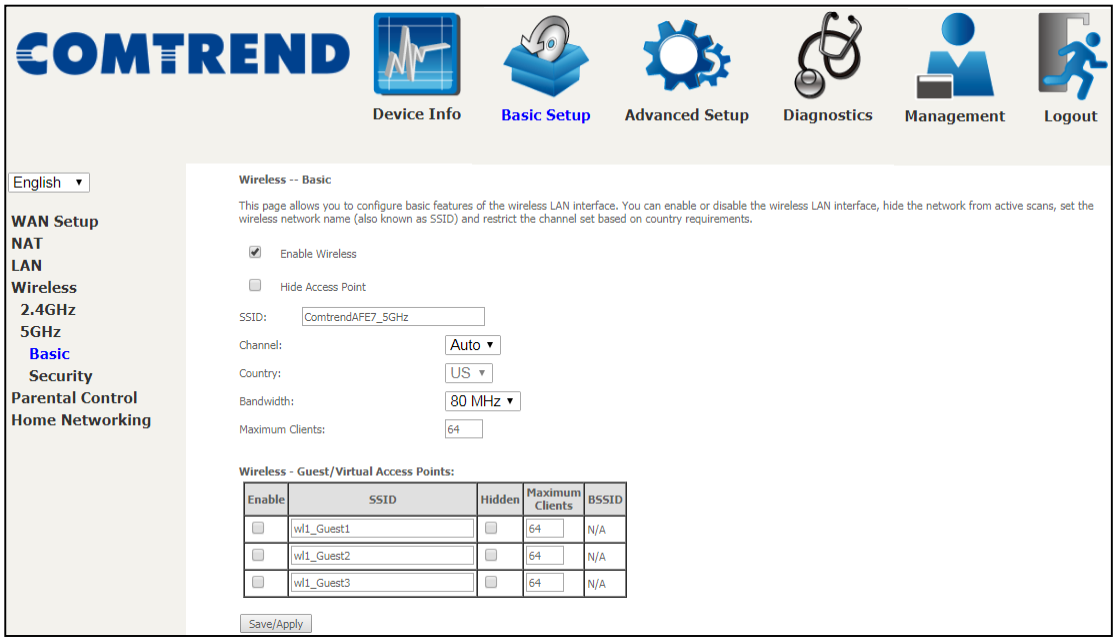
Click **Save/Apply** to implement new configuration settings.

Please see 6.13.3 for WPS setup instructions.

Please see 6.13.4 for Advanced Wireless features.

5.4.3 Basic 5GHz

The Basic option allows you to configure basic features of the wireless LAN interface. Among other things, you can enable or disable the wireless LAN interface, hide the network from active scans, set the wireless network name (also known as SSID) and configure the channel setting for the wireless LAN interface.



Click the **Save/Apply** button to apply the selected wireless options.

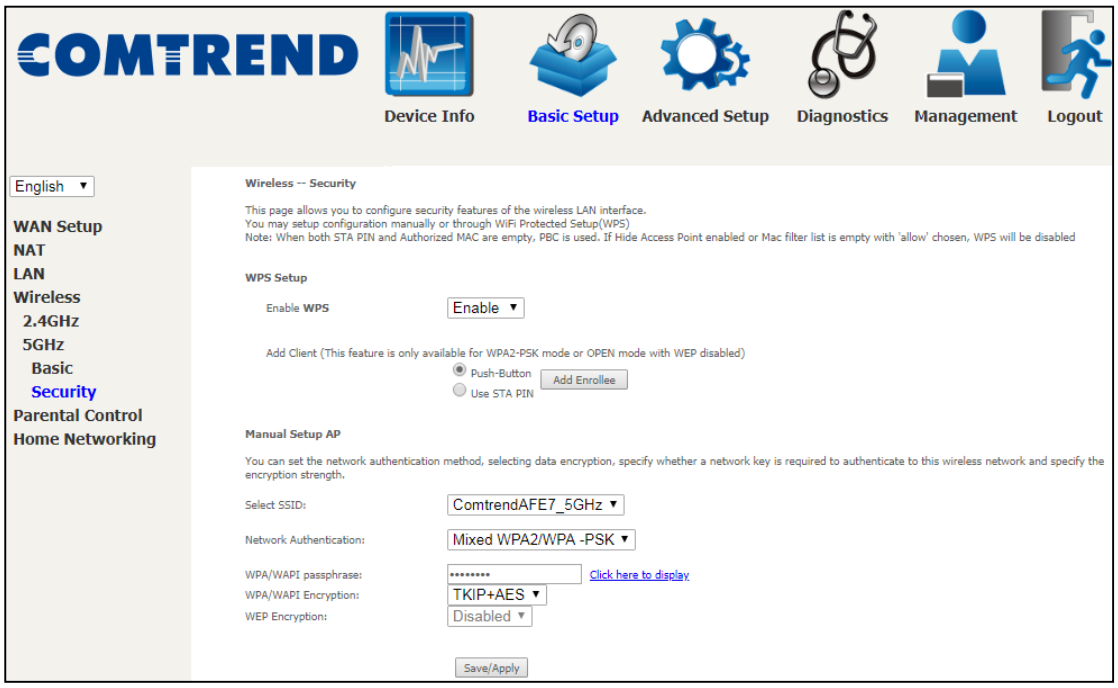
Consult the table below for descriptions of these options.

Option	Description
Enable Wireless	A checkbox ☑ that enables or disables the wireless LAN interface. When selected, a set of basic wireless options will appear.
Hide Access Point	Select Hide Access Point to protect the access point from detection by wireless active scans. To view and connect to available wireless networks in Windows, open Connect to a Network by clicking the network icon (or) in the notification area. If the access point is hidden, it will not be listed there. To connect a client to a hidden access point, the station must add the access point manually to its wireless configuration.
SSID [1-32 characters]	Sets the wireless network name. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that user will not be granted access.
Channel	Drop-down menu that allows selection of a specific channel.
Country	Local regulations limit channel range: US/Canada = 1-11.
Bandwidth	To utilize maximum data throughput, select 80MHz in 5G band.
Max Clients	The maximum number of clients that can access the router.

Option	Description
Wireless - Guest / Virtual Access Points	This router supports multiple SSIDs called Guest SSIDs or Virtual Access Points. To enable one or more Guest SSIDs select the checkboxes ☑ in the **Enabled** column. To hide a Guest SSID, select its checkbox ☑ in the **Hidden** column. Do the same for **Isolate Clients** and **Disable WMM Advertise**. For a description of these two functions, see the previous entries for "Clients Isolation" and "Disable WMM Advertise". Similarly, for **Enable WMF**, **Max Clients** and **BSSID**, consult the matching entries in this table. **NOTE:** Remote wireless hosts cannot scan Guest SSIDs.

5.4.4 Security 5GHz

The following screen appears when Wireless Security is selected. The options shown here allow you to configure security features of the wireless LAN interface.



Click **Save/Apply** to implement new configuration settings.

Please see 6.13.7 for WPS setup instructions.

WIRELESS SECURITY

Setup requires that the user configure these settings using the Web User Interface (see the table below).

Select SSID
Select the wireless network name from the drop-down menu. SSID stands for Service Set Identifier. All stations must be configured with the correct SSID to access the WLAN. If the SSID does not match, that client will not be granted access.

Network Authentication
This option specifies whether a network key is used for authentication to the wireless network. If network authentication is set to Open, then no authentication is provided. Despite this, the identity of the client is still verified. Each authentication type has its own settings. For example, selecting 802.1X authentication will reveal the RADIUS Server IP address, Port and Key fields. WEP Encryption will also be enabled as shown below. Choosing **WPA2-PSK**, you must enter WPA/WAPI passphrase and Group Rekey Interval.
Choosing **WPA2-PSK**, you must enter WPA/WAPI passphrase and Group Rekey Interval.

WEP Encryption
This option specifies whether data sent over the network is encrypted. The same network key is used for data encryption and network authentication. Four network keys can be defined although only one can be used at any one time. Use the Current Network Key list box to select the appropriate network key. Security options include authentication and encryption services based on the wired equivalent privacy (WEP) algorithm. WEP is a set of security services used to protect 802.11 networks from unauthorized access, such as eavesdropping; in this case, the capture of wireless network traffic. When data encryption is enabled, secret shared encryption keys are generated and used by the source station and the destination station to alter frame bits, thus avoiding disclosure to eavesdroppers. Under shared key authentication, each wireless station is assumed to have received a secret shared key over a secure channel that is independent from the 802.11 wireless network communications channel.

Please see 6.13.8 for Advanced Wireless features.

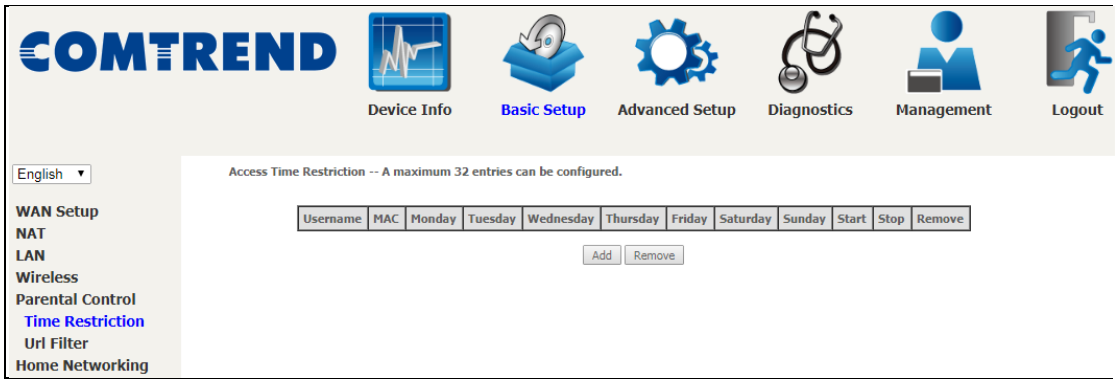
5.5 Parental Control

This selection provides WAN access control functionality.

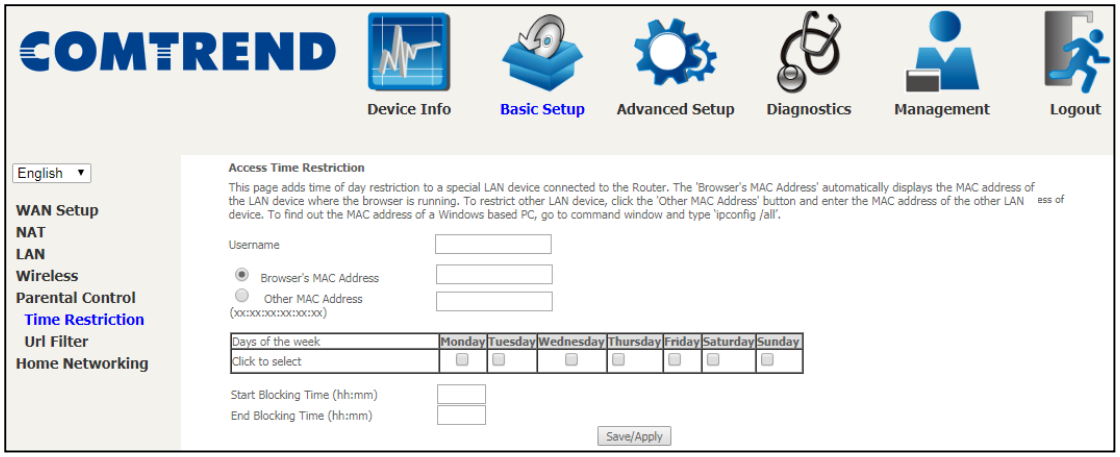
5.5.1 Time Restriction

This feature restricts access from a LAN device to an outside network through the device on selected days at certain times. Make sure to activate the Internet Time server synchronization as described in section 8.5 Internet Time, so that the scheduled times match your local time.

Clicking on the checkbox in the Enable field allows the user to select all / none entries for Enabling/Disabling.



Click **Add** to display the following screen.

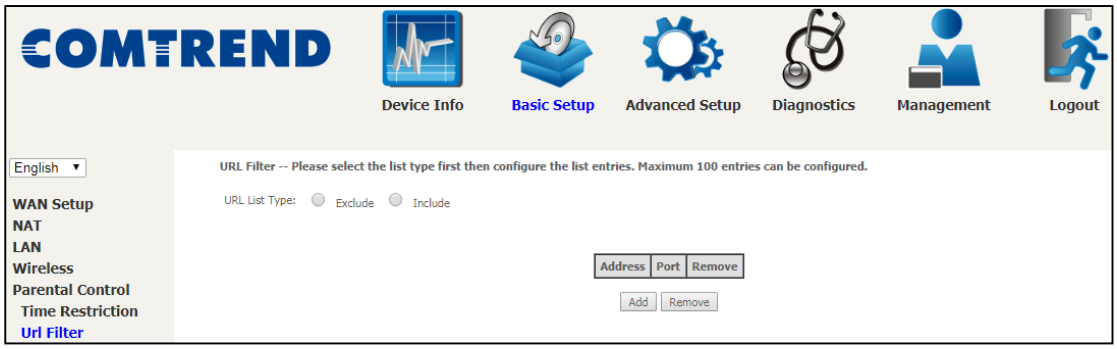


See below for field descriptions. Click **Save/Apply** to add a time restriction.

User Name: A user-defined label for this restriction.
Browser's MAC Address: MAC address of the PC running the browser.
Other MAC Address: MAC address of another LAN device.
Days of the Week: The days the restrictions apply.
Start Blocking Time: The time the restrictions start.
End Blocking Time: The time the restrictions end.

5.5.2 URL Filter

This screen allows for the creation of a filter rule for access rights to websites based on their URL address and port number.

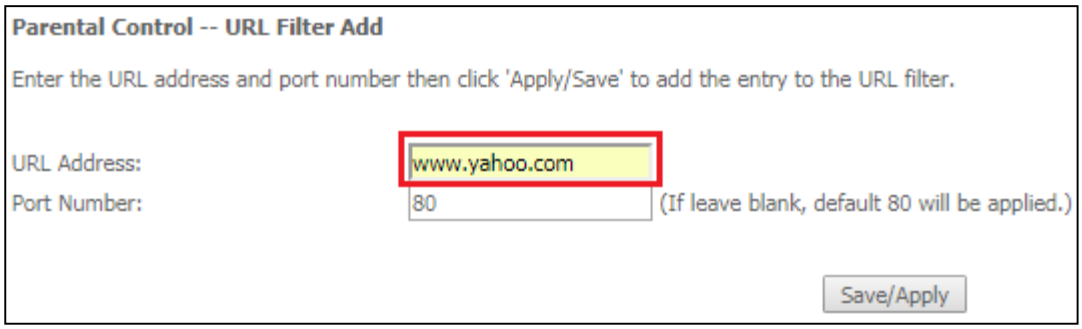


Select URL List Type: Exclude or Include.

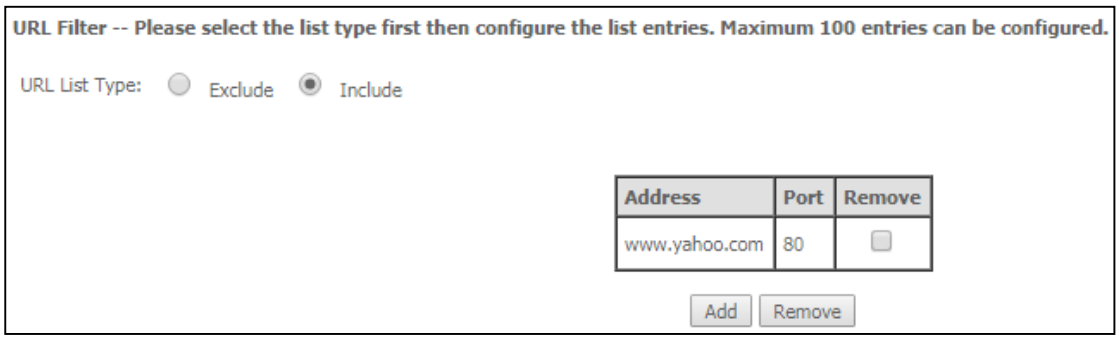
Tick the **Exclude** radio button to deny access to the websites listed.

Tick the **Include** radio button to restrict access to only those listed websites.

Then click **Add** to display the following screen.



Enter the URL address and port number then click **Save/Apply** to add the entry to the URL filter. URL Addresses begin with "www", as shown in this example.

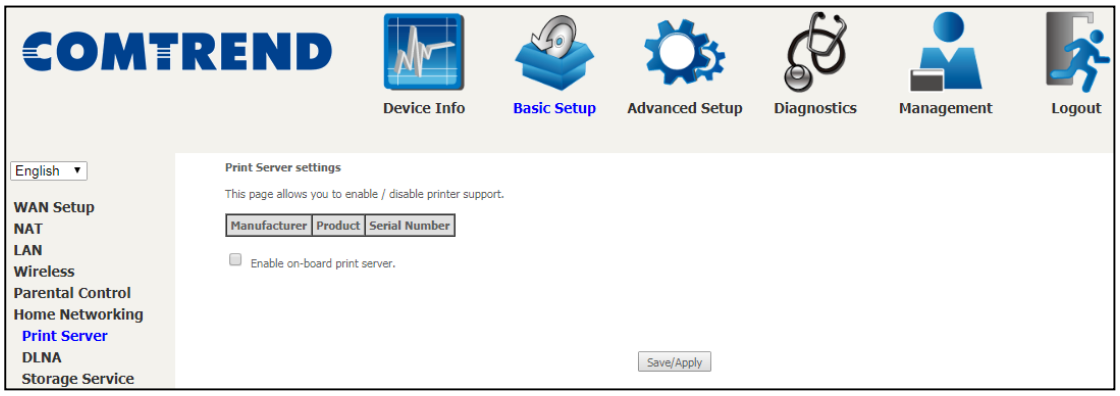


A maximum of 100 entries can be added to the URL Filter list.

5.6 Home Networking

5.6.1 Print Server

This page allows you to enable or disable printer support.

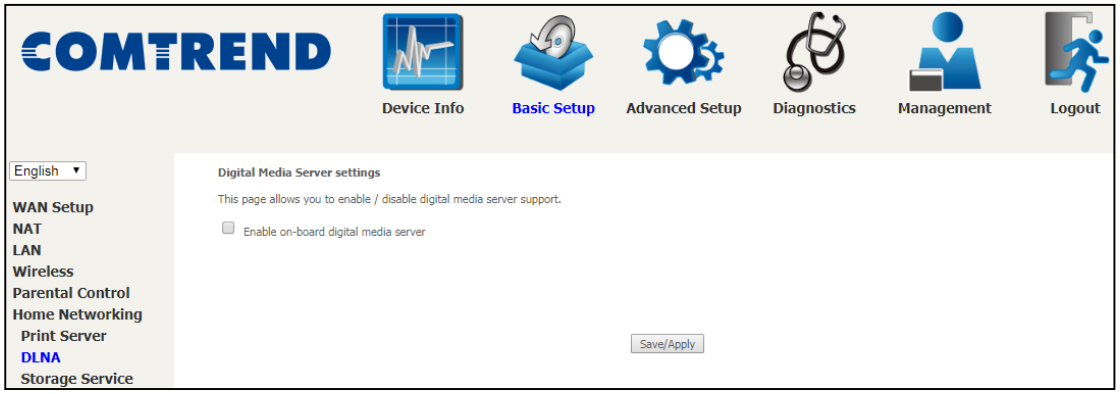


Please reference **Appendix E** to see the procedure for enabling the Printer Server.

5.6.2 DLNA

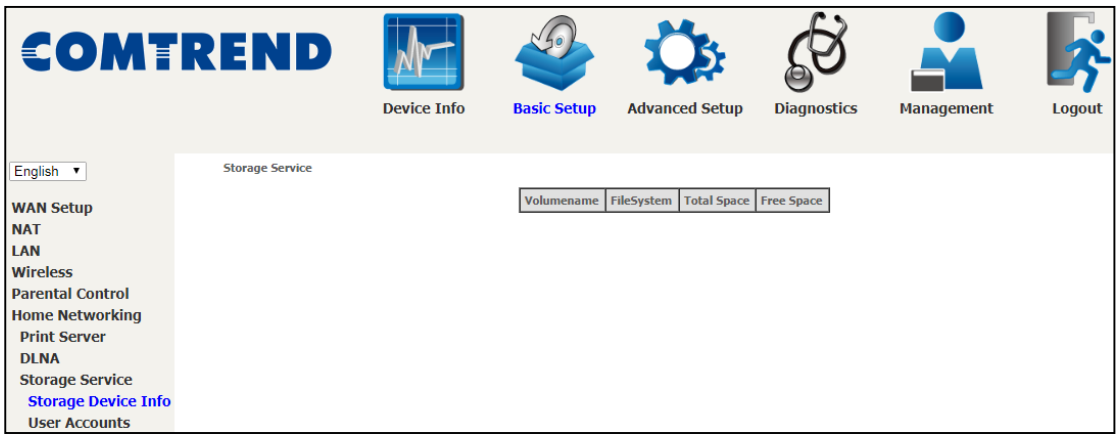
Enabling DLNA allows users to share digital media, like pictures, music and video, to other LAN devices from the digital media server.

Insert the USB drive into the USB host port on the back of the router.
Click Enable on-board digital media server, a dropdown list of directories found on the USB driver will be available for selection. Select media path from the drop-down list or manually modify the media library path and click **Save/Apply** to enable the DLNA media server.



5.6.3.1 Storage Device Info

This page also displays storage devices attached to the USB host.



Display after storage device attached (for your reference).

Volumename	FileSystem	Total Space	Free Space
disk1_1	fat	7711	7035