COMTREND

PBL-6201v2 (NL-3131u)

Wi-Fi 6E Gateway

User Manual

261103-031

Version A1.0 June 27, 2023

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

MPORTANT SAFETY INSTRUCTIONS

When using your telephone equipment (for unpacking, installation, use, and maintenance), basic safety precautions should always be followed to reduce the risk of fire, electric shock and injury to persons, including the following:
-Do not use this product near water for example, near a bathtub, washbowl, kitchen sink or laundry tub, in a wet basement or near a swimming pool. Also, do not expose the equipment to rain or damp areas (e.g. a wet basement).
-Never install telephone wiring during stormy weather conditions.
-Avoid using a telephone (other than a cordless type) during an electrical storm there may be a remote risk of electric shock from lightning.
-Do not use the telephone to report a gas leak in the vicinity of the leak
-Use only the power cord and batteries (or adapter) indicated in this manual.
-Do not dispose of batteries in a fire. They may explode. Check with local codes for possible special disposal instructions
-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.
SAVE THESE INSTRUCTIONS

CAUTION:

- 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.
- To prevent interference with cordless phones, ensure that the gateway is at least 5 feet (1.5m)from the cordless phone base station.
- If you experience trouble with this equipment, disconnect it from the network until the problem has been corrected or until you are sure that equipment is not malfunctioning.

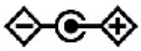
" CAUTION: To reduce the risk of fire, use only No. 26 AWG or larger (e.g. 24 AWG) UL Listed or CSA Certified Telecommunication Line Cord "

WARNING

- Disconnect the power line from the device before servicing
- For indoor use only
- Do NOT open the casing
- Do NOT use near water
- Keep away from the fire
- For use in ventilated environment / space
- Do NOT insert sharp objects into the RJ-11 jack
- 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'approchez pas du feu
- Veuillez utiliser dans un environnement aéré
- N'insérez pas d'objets tranchants dans la prise RJ-11
- Veuillez utiliser fil électrique de 26AWG pour port RJ-11

Power Specifications (Alimentation) :

Input : 12Vdc, 3.0A 

Output : USB3.0, ⎓ 900mA

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

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 49 cm 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 49 cm between the radiator & your body. This transmitter must not be co-located or operating in conjunction with any other antenna or transmitter.

"This product meets the applicable Innovation, Science and Economic development Canada technical specifications".

The device for operation in the band 5150–5250 MHz is only for indoor use to reduce the potential for harmful interference to co-channel mobile satellite systems.

This product meets the applicable Industry Canada technical specifications.

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.

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 49 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.
«Ce produit est conforme aux spécifications techniques applicables d'Innovation, Sciences et Développement économique Canada».

les dispositifs fonctionnant dans la bande 5150-5250 MHz sont réservés uniquement pour une utilisation à l'intérieur afin de réduire les risques de brouillage préjudiciable aux systèmes de satellites mobiles utilisant les mêmes canaux.

Le présent matériel est conforme aux specifications techniques applicables d'Industrie Canada.

Le numéro REN (Ringer Equivalence Number) indique le nombre maximal de périphériques pouvant être connectés à une interface téléphonique. La terminaison d'une interface peut consister en une combinaison quelconque d'appareils, à la condition que la somme des REN de tous les appareils ne dépasse pas cinq.

Certification

- FCC / IC standard
  - Part 15B / ICES-003
  - Part 15C / RSS-247(2.4GHz)
  - Part 15E / RSS-247(5GHz)
  - IC-CS03
  - CSA 62368-1

Copyright

NOTE:	This document is subject to change without notice.

Open Source Software Notice

Comtrend's products use open source software to fulfill their function.

Licenses for the open source software are granted under the GNU General Public License in various versions. For further information on the GNU General Public License see http://www.gnu.org/licenses/

You are allowed to modify all open source code (except for proprietary programs) and to conduct reverse engineering for the purpose of debugging such modifications; to the extent such programs are linked to libraries licensed under the GNU Lesser General Public License. You are not allowed to distribute information resulting from such reverse engineering or to distribute the modified proprietary programs.

The rights owners of the open source software require you to refer to the following disclaimer which shall apply with regard to those rights owners:

Warranty Disclaimer

THE OPEN SOURCE SOFTWARE IN THIS PRODUCT 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 APPLICABLE LICENSES FOR MORE DETAILS. Comtrend's products will strictly follow the market's standard requirements. It is not permitted to modify any Wi-Fi parameters, including the Wi-Fi power setting.

Obtain Source Code
If you wish to download the open source code please see:
https://www.comtrend.com/gplcddl.html

If you do not see the required source code on our website link and wish to be provided with the entire source code for that product, we will provide it to you and any third party with the source code of the software licensed under an open source software license. Please send us a written request by email or mail to one of the following addresses:

Email: Comtrend support team - opensource@comtrend.com

Postal: Comtrend Corporation
3F-1, 10 Lane 609,
Chongxin Rd., Section 5,
Sanchong Dist,
New Taipei City 241405,
Taiwan
Tel: 886-2-2999-8261

In detail name the product and firmware version for which you request the source code and indicate means to contact you and send you the source code.

PLEASE NOTE WE WILL CHARGE THE COSTS OF A DATA CARRIER AND THE POSTAL CHARGES TO SEND THE DATA CARRIER TO YOU.THE AMOUNT WILL VARY ACCORDING TO YOUR LOCATION AND THE COMTREND SUPPORT TEAM WILL NOTIFY THE EXACT COSTS WHEN REVIEWING THE REQUEST.

THIS OFFER IS VALID FOR THREE YEARS FROM THE MOMENT WE DISTRIBUTED THE PRODUCT. FOR MORE INFORMATION AND THE OPEN SOURCE LIST (& RESPECTIVE LICENCES) FOR INDIVIDUAL PRODUCTS PLEASE SEE:
https://www.comtrend.com/gplcddl.html

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.

Table of Contents

Chapter 1 Introduction

PBL-6201v2 is a triple band Wi-Fi 6E Gateway with an updated silicon platform. It provides a 2.5 Giga Ethernet WAN port and four Giga Ethernet ports, supporting Wi-Fi 6 (802.11ax) Wireless solution on frequency band of 2.4GHz (4T4R) and 5GHz (4T4R). PBL-6201v2 allows central management (ACS) by following TR-069.The core design concept of PBL-6201v2 is to enhance the user experience on high speed applications with its high power wireless design, so as to provide better coverage and stable Wi-Fi services.

Chapter 2 Installation

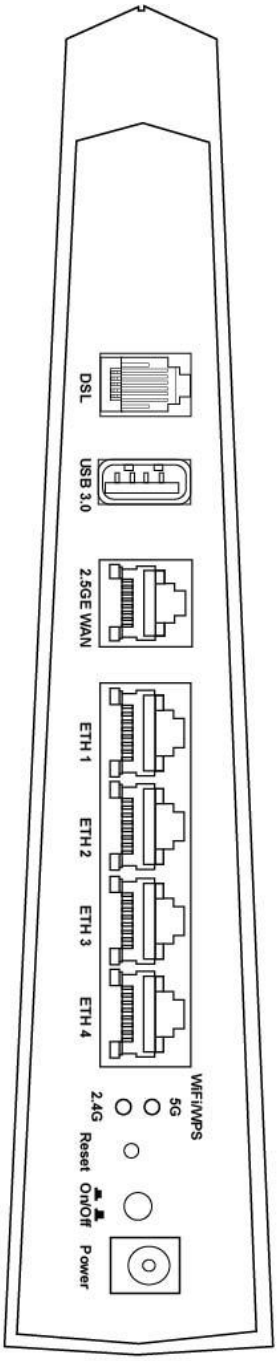
2.1 Hardware Setup

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.



DSL
Connect to the DSL port with the DSL RJ14 cable. The PBL-6201v2 supports the following DSL profiles -
ADSL : ADSL, ADSL 2, ADSL 2+.
VDSL : 8a, 8b, 8c, 8d, 12a, 12b, 17a, 30a and 35b.

USB Port
This port can be used to connect the router to a storage device. It can only be used for SAMBA(storage) and for a Printer Server. Support for other devices may be added in future firmware upgrades.

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.

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 slower networks. As these ports are auto-sensing MDI/X, either straight-through or crossover cable can be used.

WiFi On/Off/ WPS Button 5G
Press the 5G button for less than 5 seconds to enable WPS which will allow 2 minutes for WPS connection detection.
Press and hold the 5G button for more than 10 seconds to enable/disable the WiFi function.

WiFi On/Off/ WPS Button 2.4G
Press the 2.4G button for less than 5 seconds to enable WPS which will allow 2 minutes for WiFi connection.
Press and hold the 2.4G button for more than 10 seconds to enable/disable the WiFi function.

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 2.1.2 Front Panel for details).

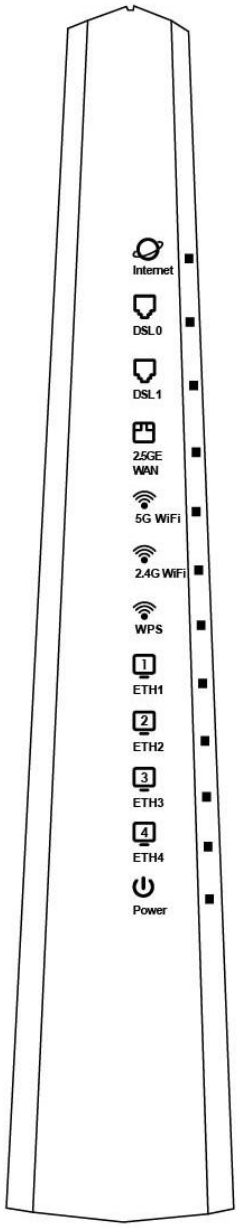
NOTE:	If pressed down for more than 60 seconds, the PBL-6201v2 will go into a firmware update state (CFE boot mode). The firmware can then be updated using an Internet browser pointed to the default IP address.

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 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 (the device has a WAN IP address from IPCP or DHCP is up or a static IP address is configured, PPP negotiation is successfully complete.
		Off	Modem power off, modem in WDS 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.)
DSL0	Green	On	xDSL (DSL0) Link is established.
		Off	xDSL (DSL0) Link is not established.
		Blink	xDSL (DSL0) Link is training.
DSL1	Green	On	xDSL (DSL1) Link is established.
		Off	xDSL (DSL1) Link is not established.
		Blink	xDSL (DSL1) Link is training.
2.5G 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. LED will stay on for three minutes.
		Off	No WPS association process ongoing.
		Blink	WPS connection in progress until client connected.
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.
		Blink	Firmware is upgrading.
	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.

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**)
- 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 PBL-6201v2 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.

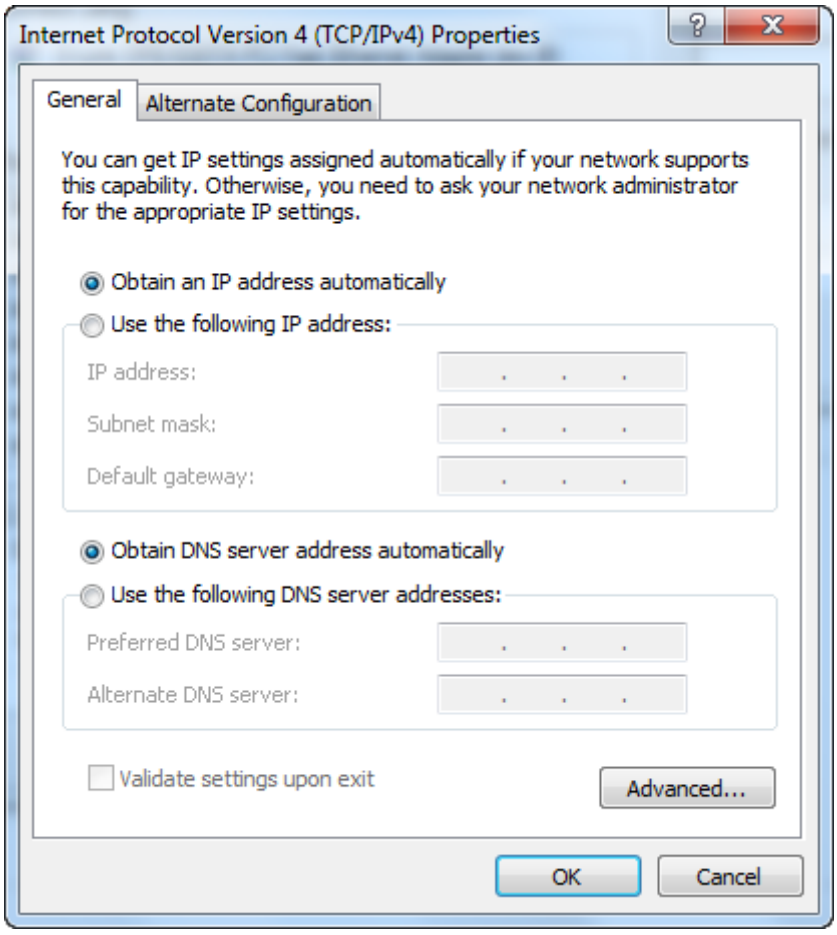
To obtain an IP address from the DCHP server, follow the steps provided below.

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.

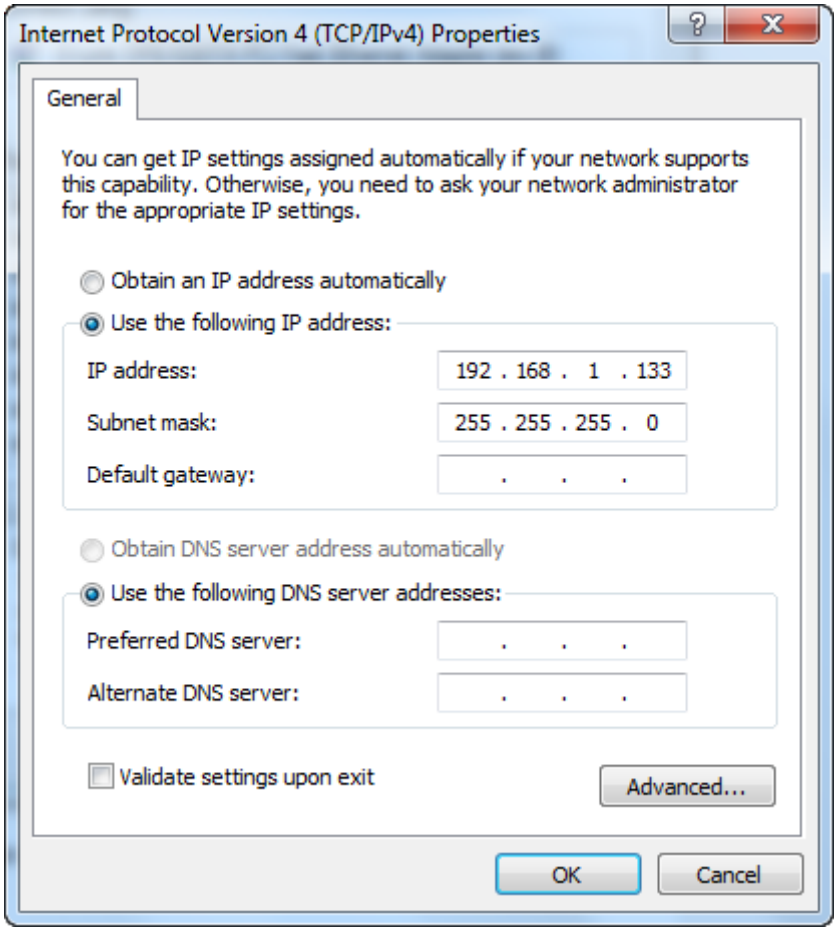
Follow these steps to configure your PC IP address to use subnet 192.168.1.x.

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

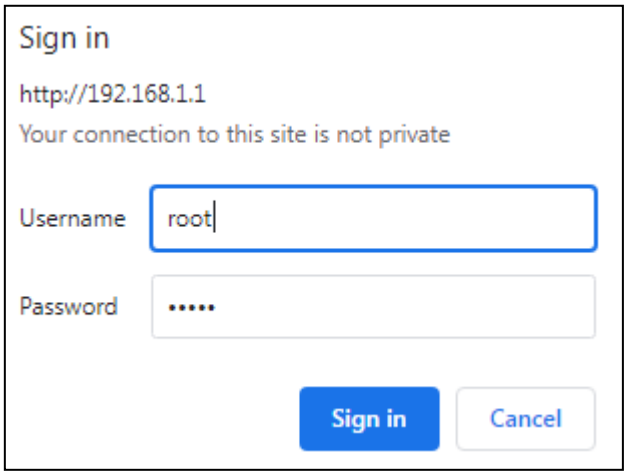
Perform the following steps to login to the web user interface.

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 Informationscreen and login with remote username and password.

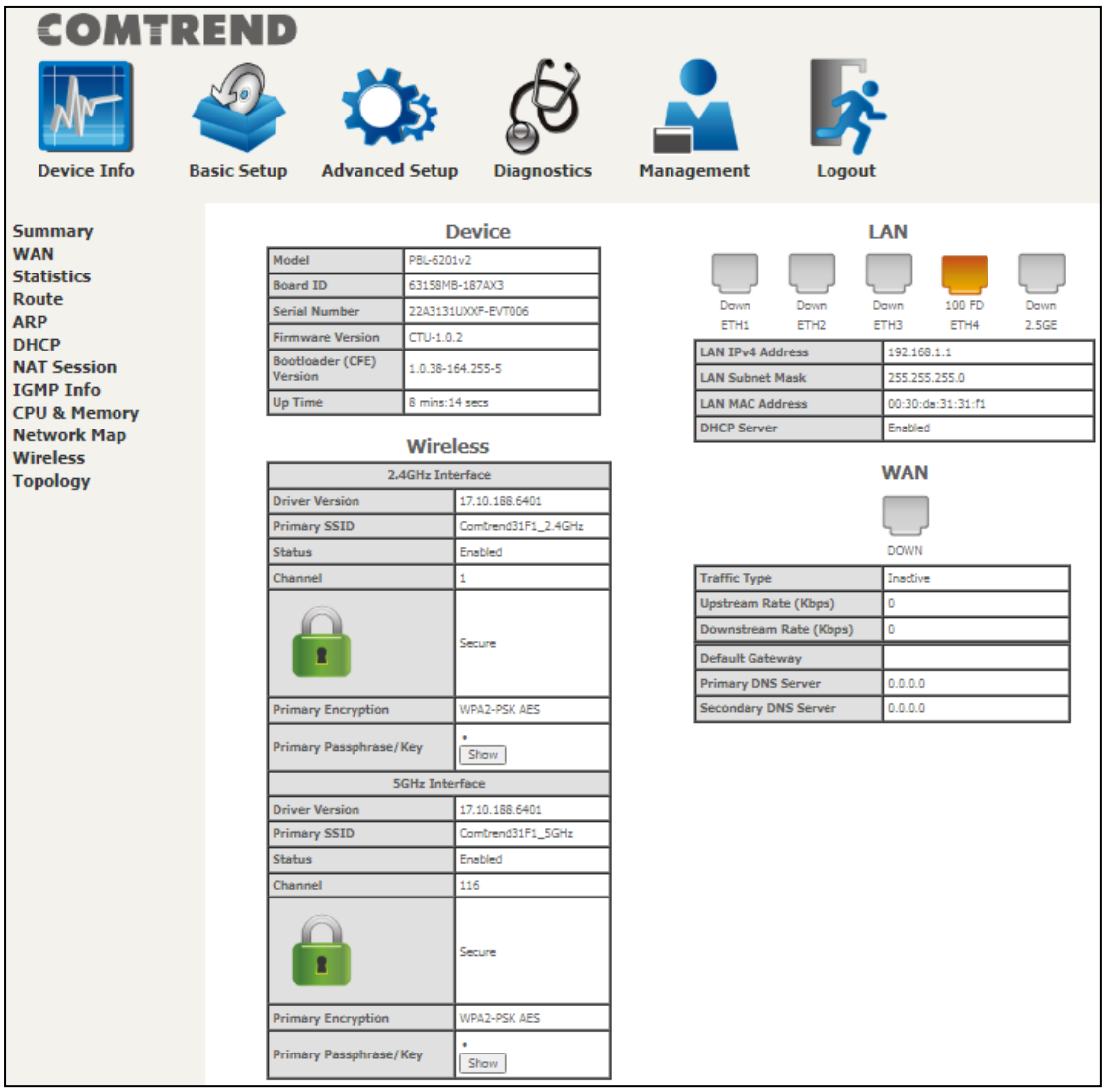
STEP 2: A dialog box will appear, such as the one below. Enter the default username and password, as defined in section 3.1 Default Settings.



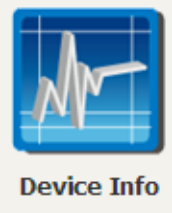
Click **OK** to continue.

NOTE:	The login password can be changed later (see section 8.7.1 Accounts).

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

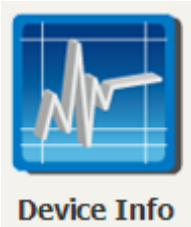


You can also reach this page by clicking on the following icon located at the top of the screen.



Chapter 4 Device Information

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

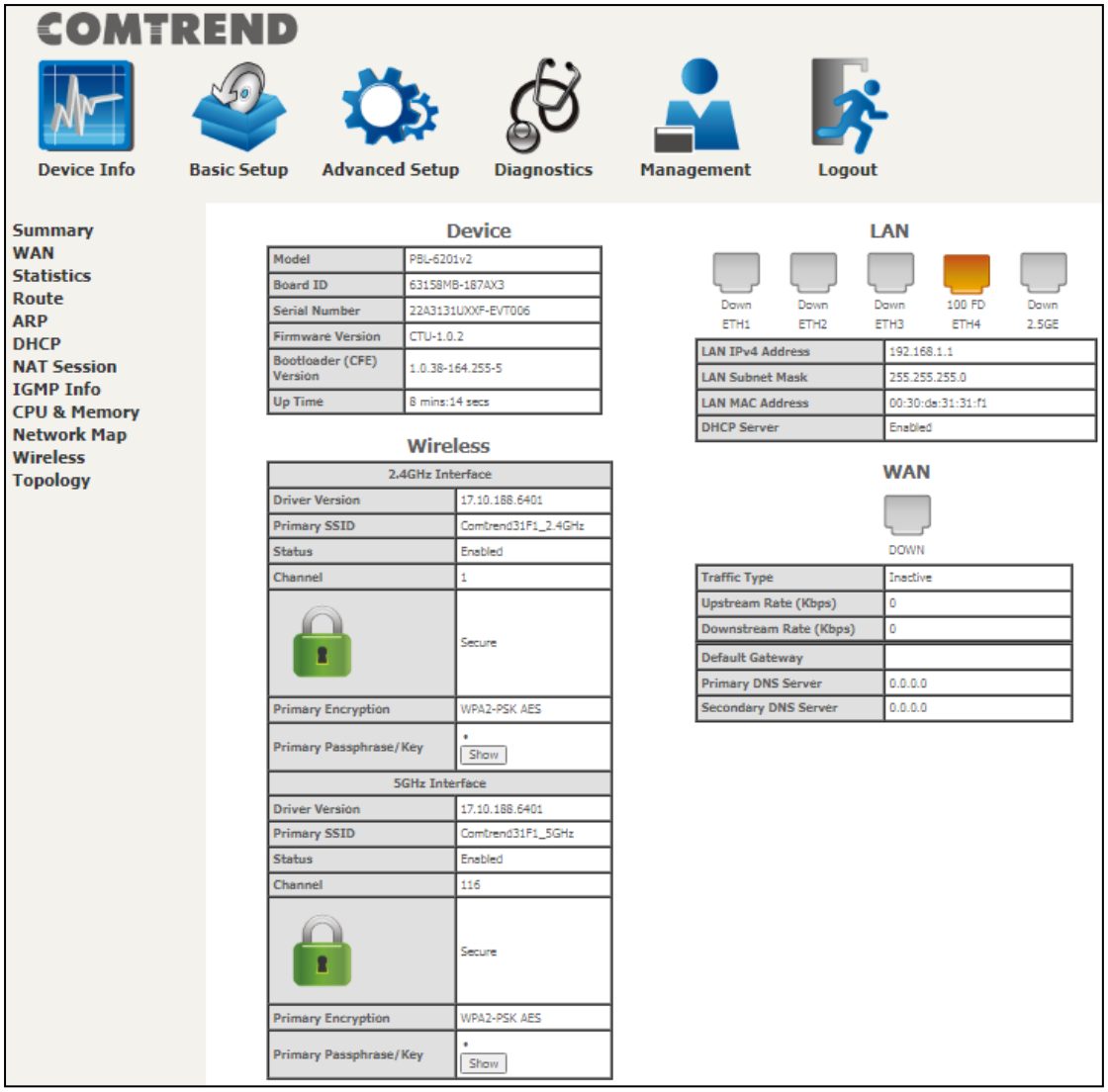


The web user interface window is divided into two frames, the main menu (on the left) and the display screen (on the right). The main menu has several options and selecting each of these options opens a submenu with more selections.

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.

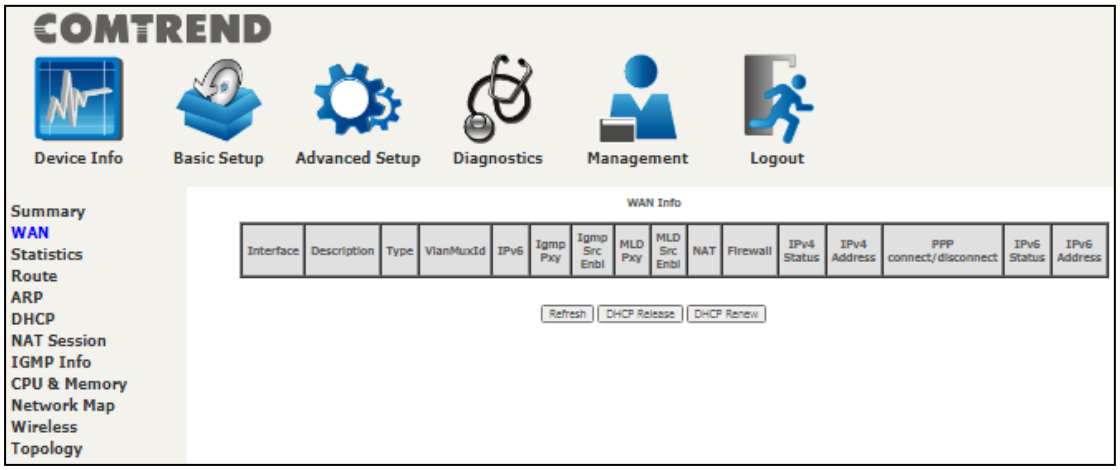
The Device Info Summary screen displays at startup.



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).



Refresh – Click this button to refresh the screen.

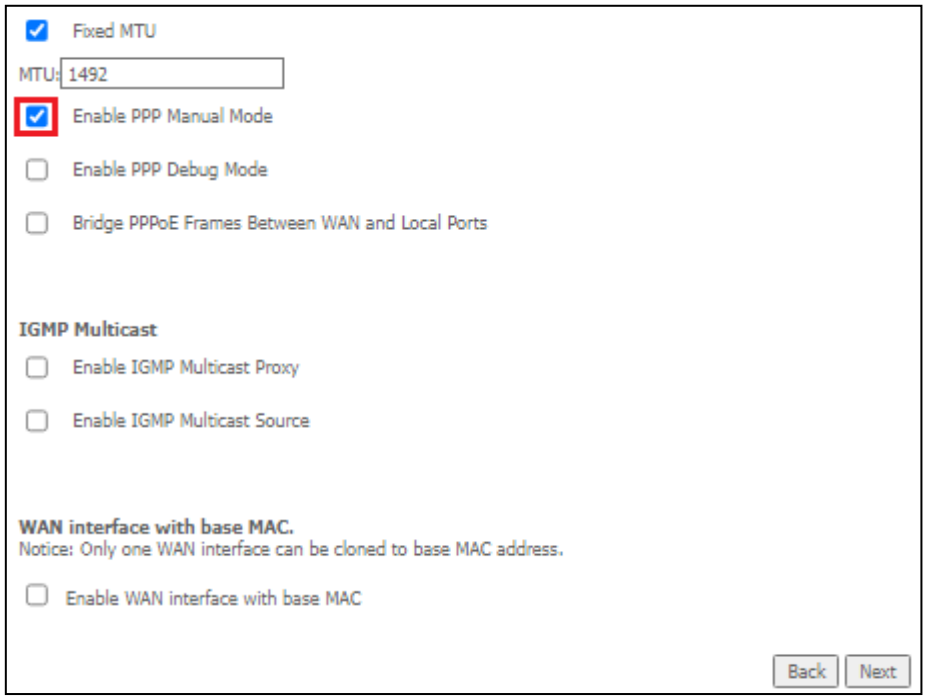
DHCP Release – Click this button to release the IP through IPoE service.

DHCP Renew - Click this button to refresh an IP through IPoE service.

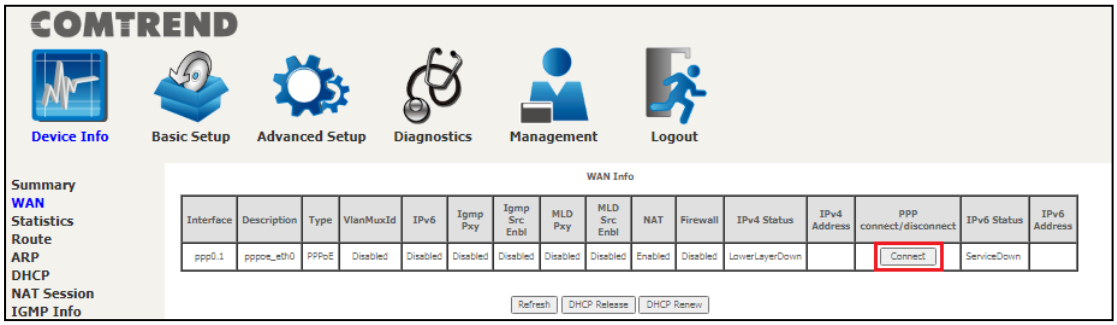
Item	Description
Interface	Name of the interface for WAN
Description	Name of the WAN connection
Type	Shows the connection type
VlanMuxId	Shows 802.1Q VLAN ID
IPv6	Shows WAN IPv6 status
Igmp Pxy	Shows Internet Group Management Protocol (IGMP) proxy status
Igmp Src Enbl	Shows the status of WAN interface 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
IPv4 Status	Lists the status of IPv4 connection if WAN enabled IPv4
IPv4 Address	Shows the WAN IPv4 address
PPP connect/disconnect	Shows the PPP connection status
IPv6 Status	Lists the status of IPv6 connection if WAN enabled IPv6
IPv6 Address	Shows the WAN IPv6 address

For your reference, if Manual Mode is enabled in PPP service as shown here.



Manual PPP connect/disconnect option will become available on the WAN Info page (as shown here).



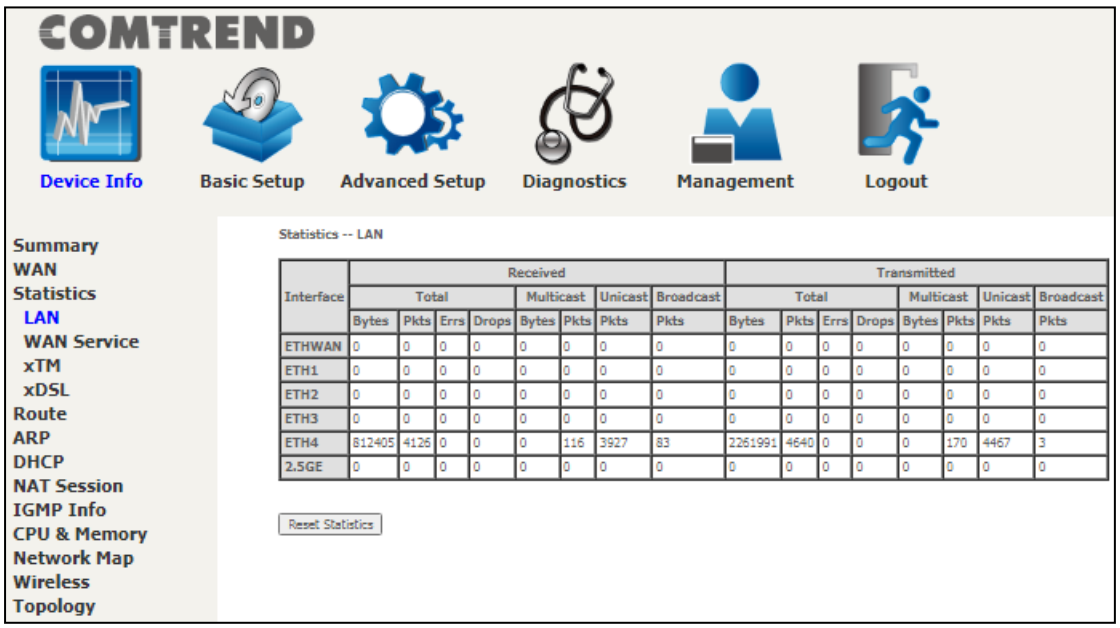
4.2 Statistics

This selection provides LAN and WAN 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.

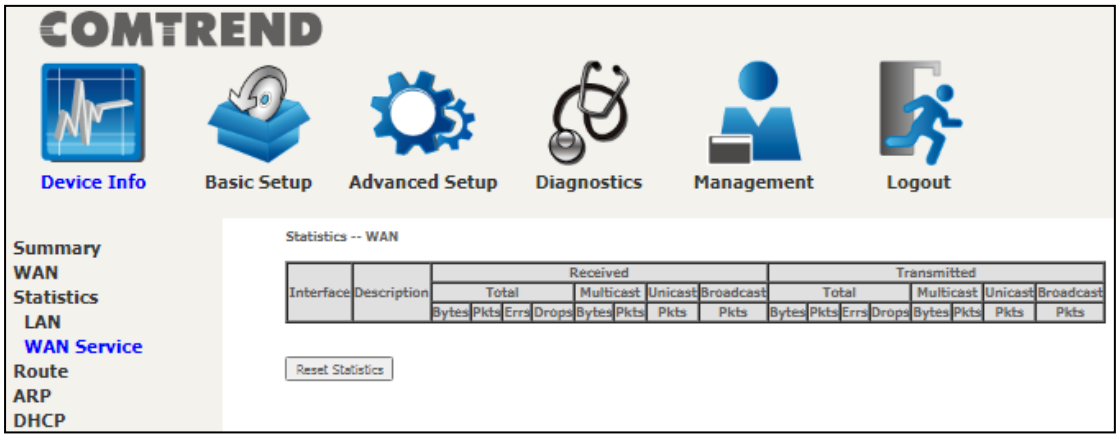


Interface	Received								Transmitted							
	Total				Multicast		Unicast	Broadcast	Total				Multicast		Unicast	Broadcast
	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts	Bytes	Pkts	Errs	Drops	Bytes	Pkts	Pkts	Pkts
ETHWAN	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ETH1	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ETH2	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ETH3	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
ETH4	812405	4126	0	0	0	116	3927	83	2261991	4640	0	0	0	170	4467	3
2.5GE	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0

Item	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

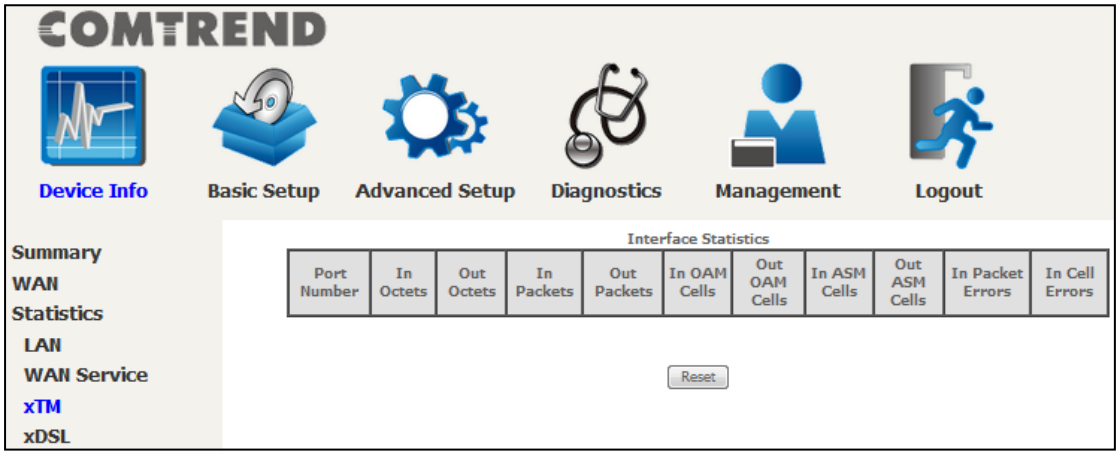
This screen shows data traffic statistics for each WAN interface.



Item	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.



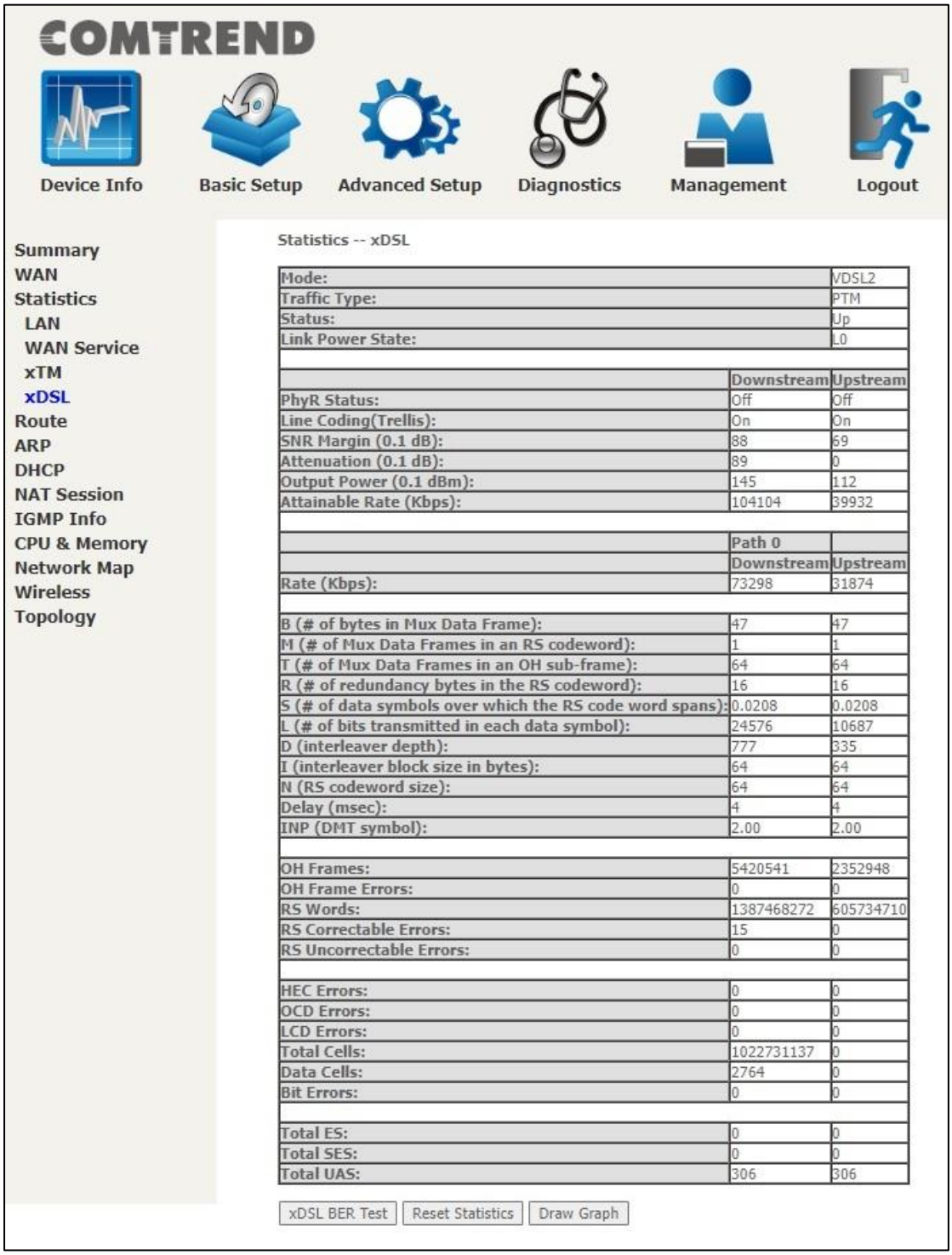
XTM Interface Statistics

Item	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

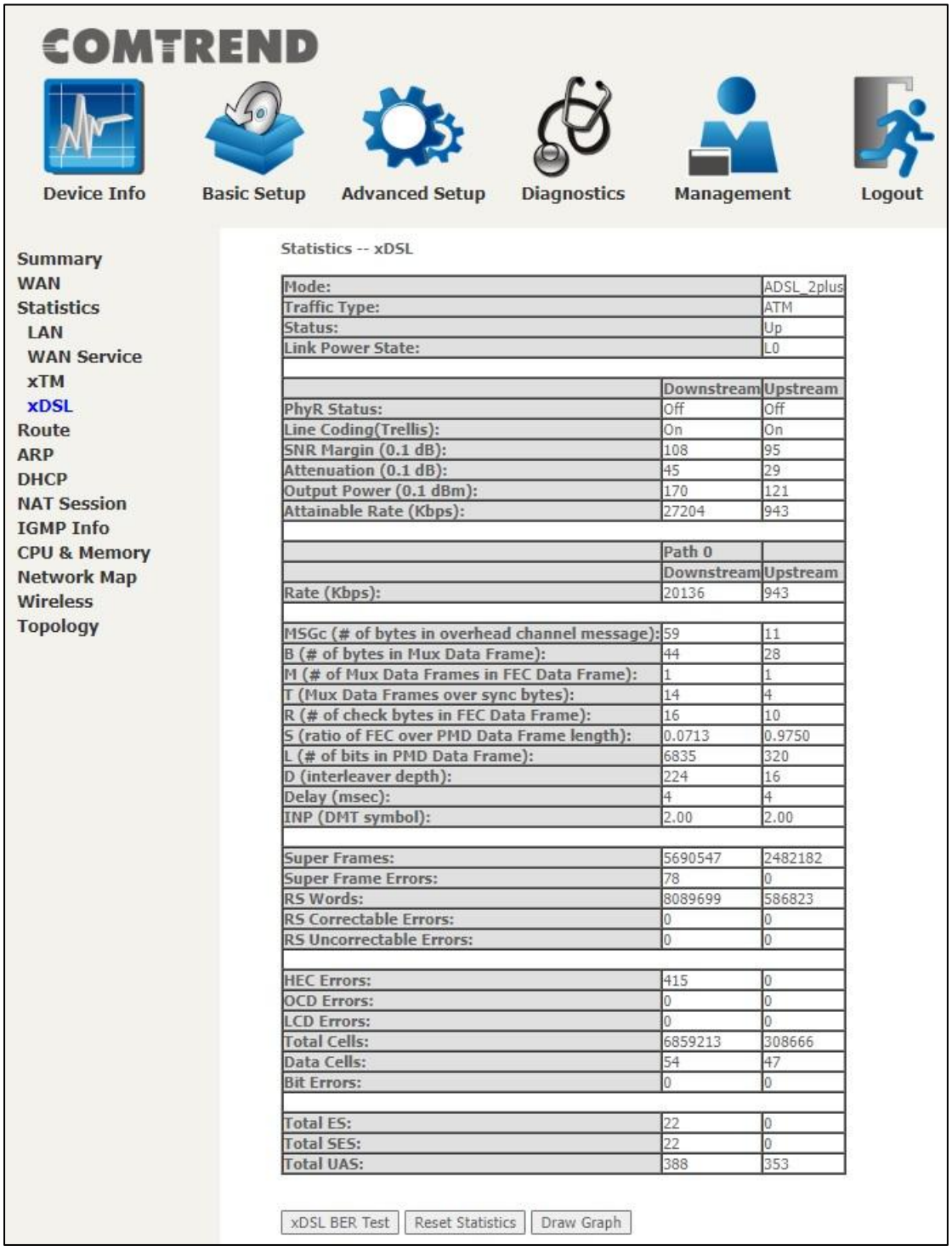
4.2.4 xDSL Statistics

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

VDSL2



ADSL2+



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

Item	Description
Mode	VDSL, VDSL2
Traffic Type	ATM, PTM

Status	Lists the status of the DSL link
Link Power State	Link output power state
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.

Item	Description
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

Item	Description
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

Item	Description
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

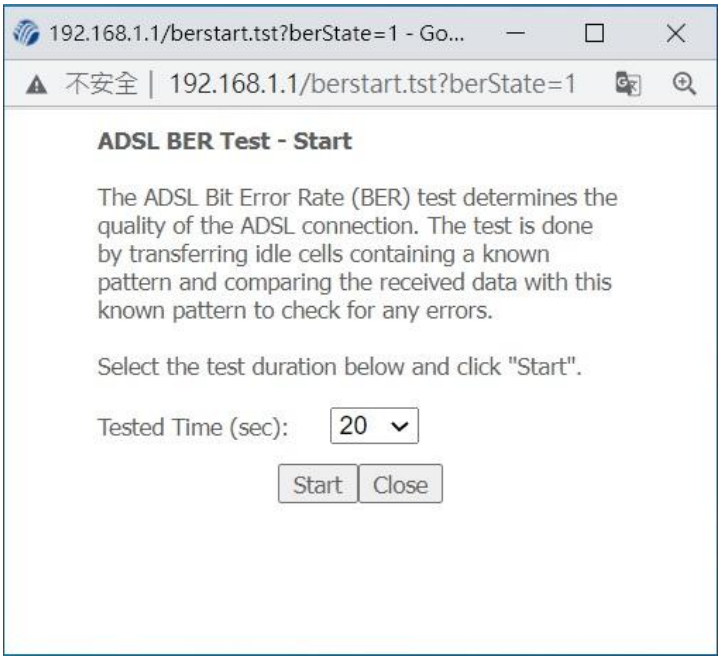
Item	Description
HEC Errors	Total Number of Header Error Checksum errors
OCD Errors	Total Number of Out-of-Cell Delineation errors
LCD Errors	Total number of Loss of Cell Delineation
Total Cells	Total number of ATM cells (including idle + data cells)
Data Cells	Total number of ATM data cells
Bit Errors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

Item	Description
Total ES	Total Number of Errored Seconds

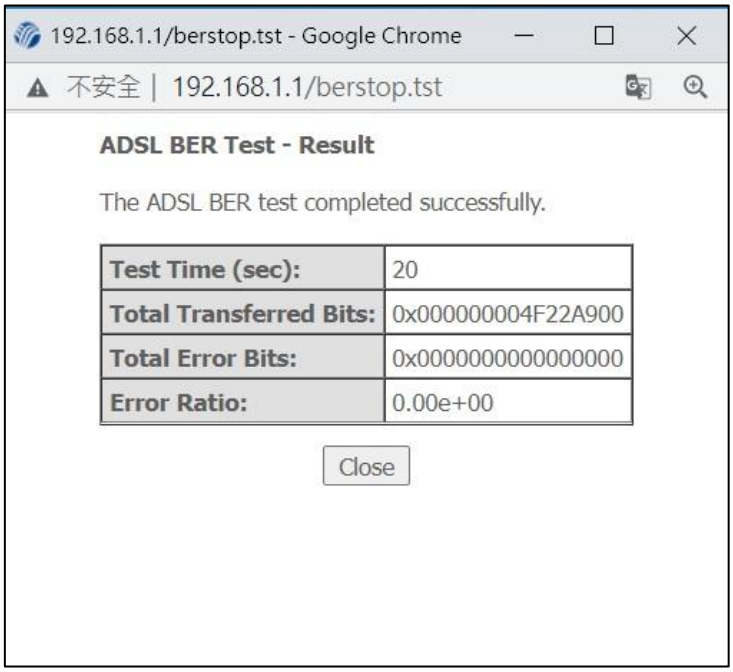
Total SES	Total Number of Severely Errored Seconds
Total UAS	Total Number of Unavailable Seconds

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.

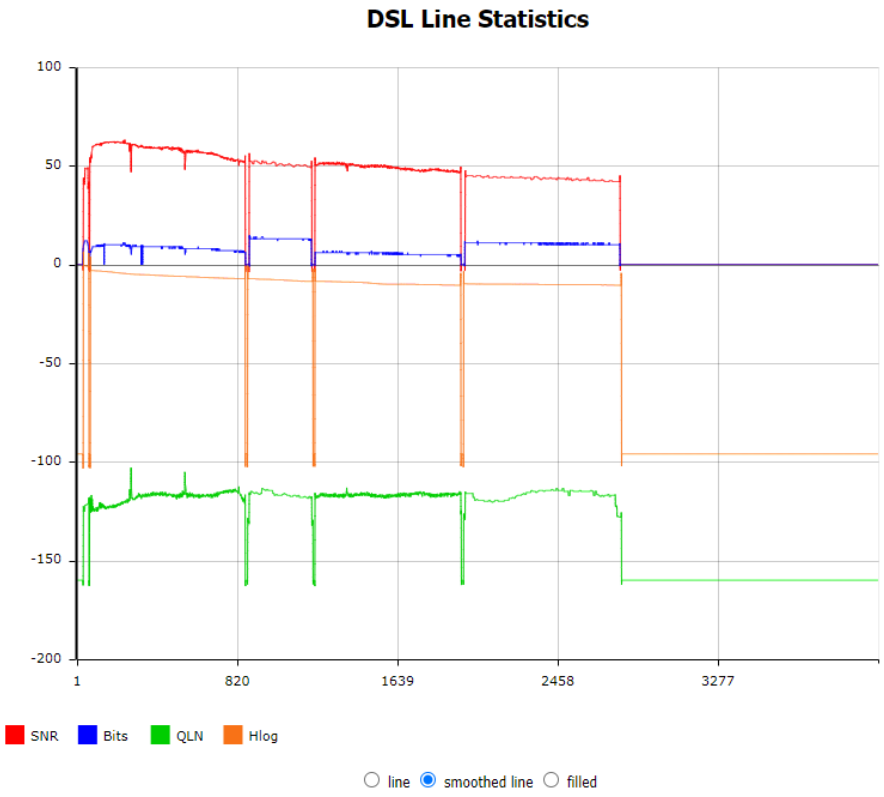


Click **Start** to start the test or click **Close** to cancel the test. After the BER testing is complete, the pop-up window will display as follows.



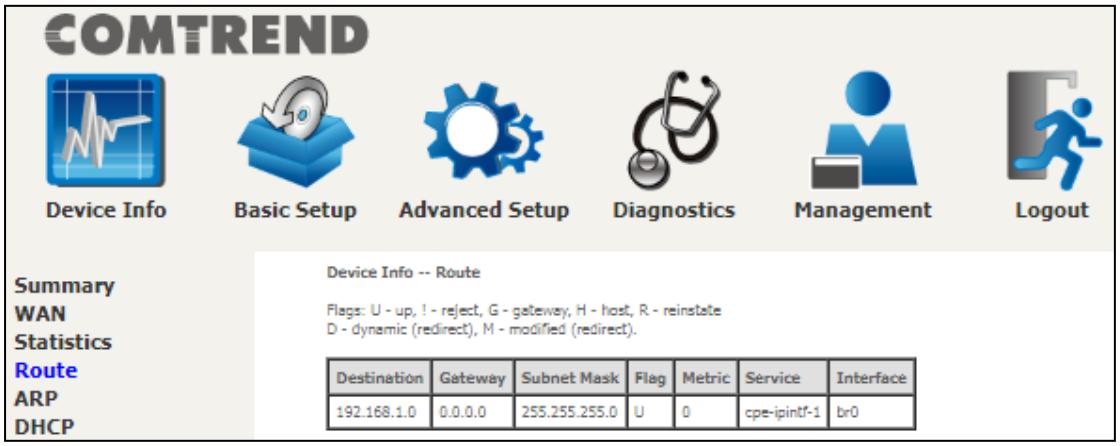
xDSL TONE GRAPH

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

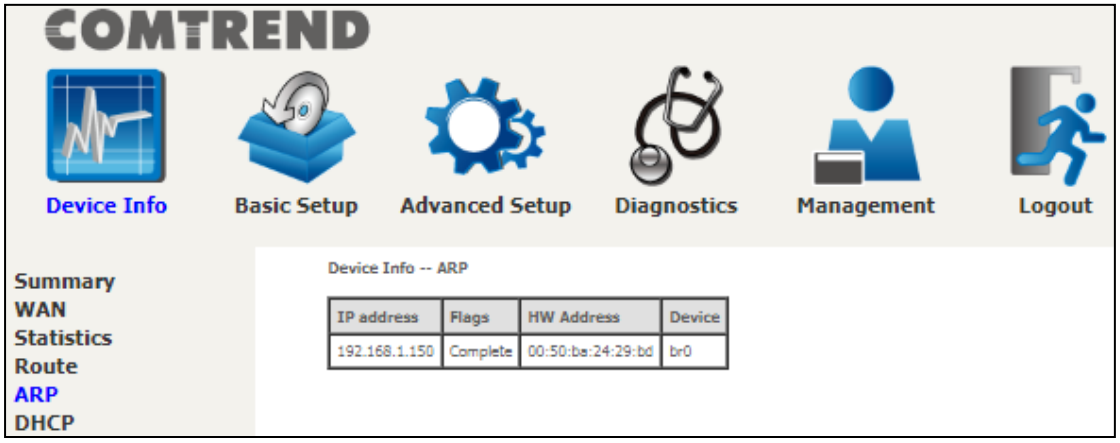
Choose **Route** to display the routes that the PBL-6201v2 has found.



Item	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

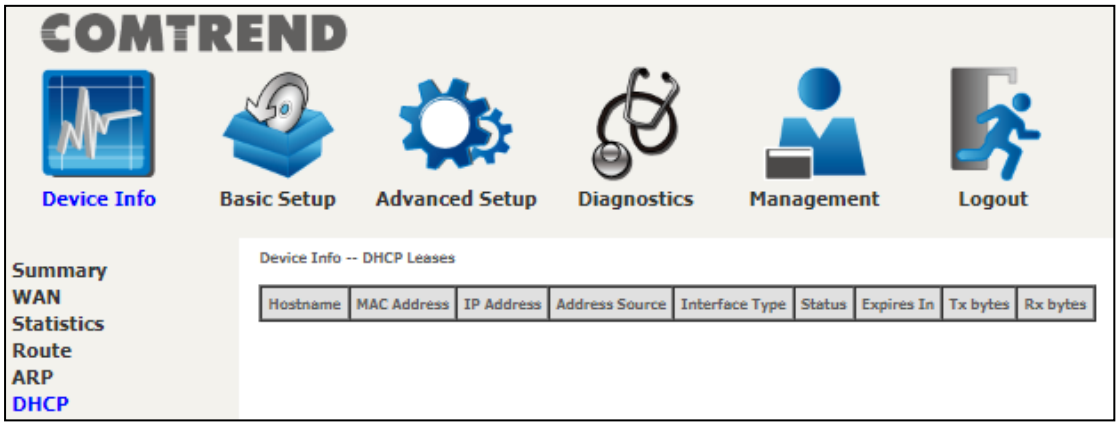
Click **ARP** to display the ARP information.



Item	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

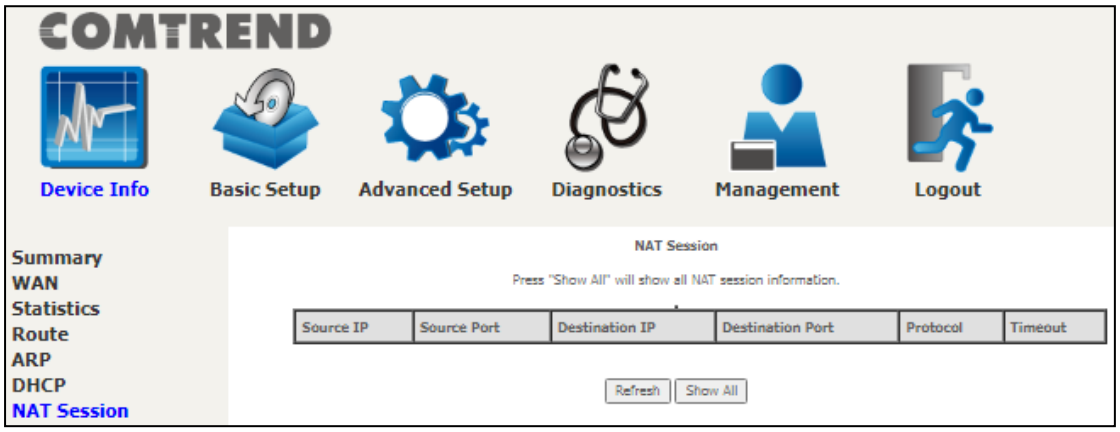
Click **DHCP** to display all DHCP Leases.



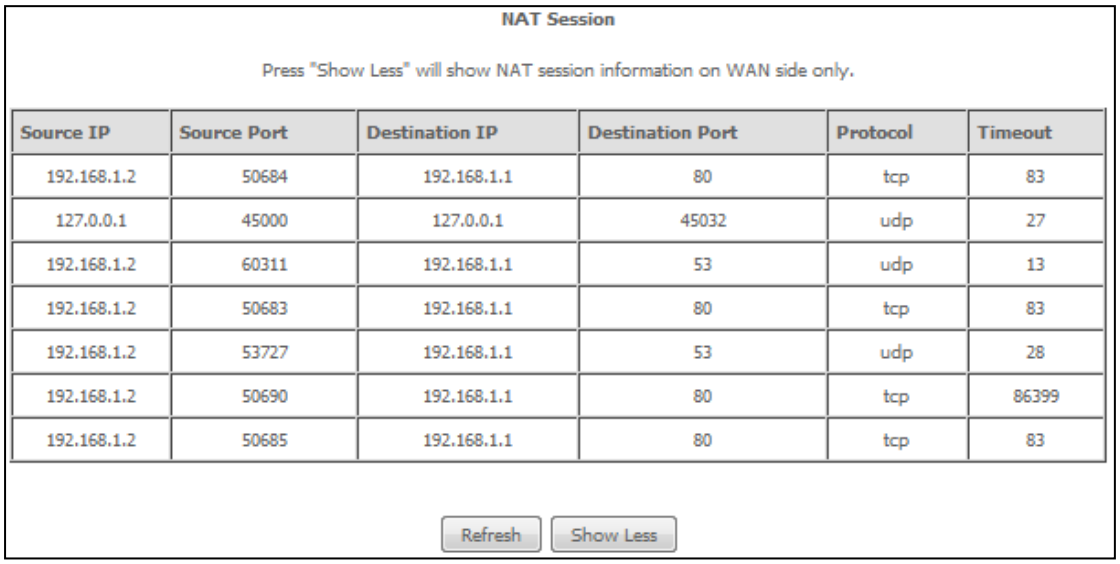
Item	Description
Hostname	Shows the device/host/PC network name
MAC Address	Shows the Ethernet MAC address of the device/host/PC
IP Address	Shows IP address of device/host/PC
Address Source	Shows IP type of device/host/PC, could be DHCP/Static
Interface Type	Shows interface type of device/host/PC, could be Ethernet/802.11
Status	Show status of device/host/PC, could be active/inactive
Expires In	Shows how much time is left for each DHCP Lease
Tx bytes	Show total Tx bytes of device/host/PC
Rx bytes	Show total Rx bytes of device/host/PC

4.6 NAT Session

This page displays all NAT connection session including both UPD/TCP protocols passing through the device.



Click the "Show All" button to display the following.



NAT Session

Press "Show Less" will show NAT session information on WAN side only.

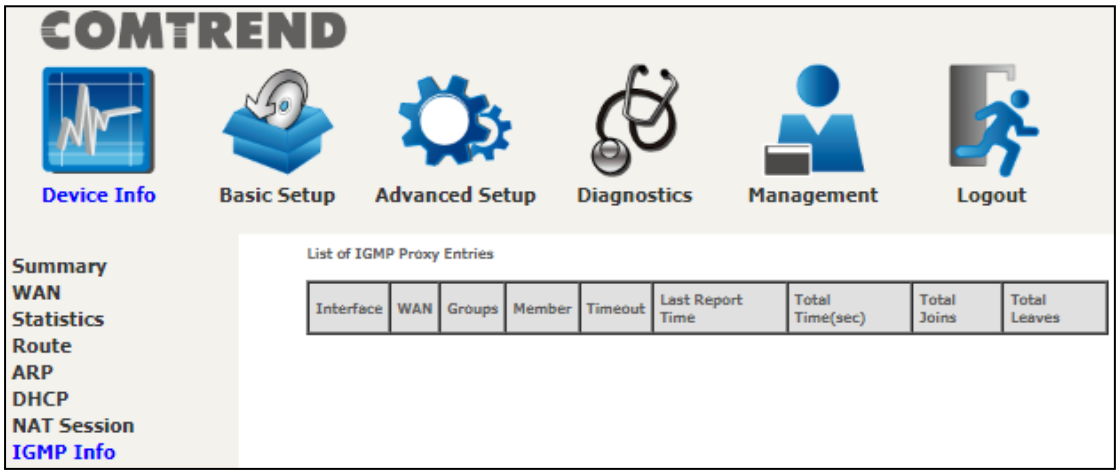
Source IP	Source Port	Destination IP	Destination Port	Protocol	Timeout
192.168.1.2	50684	192.168.1.1	80	tcp	83
127.0.0.1	45000	127.0.0.1	45032	udp	27
192.168.1.2	60311	192.168.1.1	53	udp	13
192.168.1.2	50683	192.168.1.1	80	tcp	83
192.168.1.2	53727	192.168.1.1	53	udp	28
192.168.1.2	50690	192.168.1.1	80	tcp	86399
192.168.1.2	50685	192.168.1.1	80	tcp	83

Refresh Show Less

Item	Description
Source IP	The source IP from which the NAT session is established
Source Port	The source port from which the NAT session is established
Destination IP	The IP which the NAT session was connected to
Destination Port	The port which the NAT session was connected to
Protocol	The Protocol used in establishing the particular NAT session
Timeout	The time remaining for the TCP/UDP connection to be active

4.7 IGMP Info

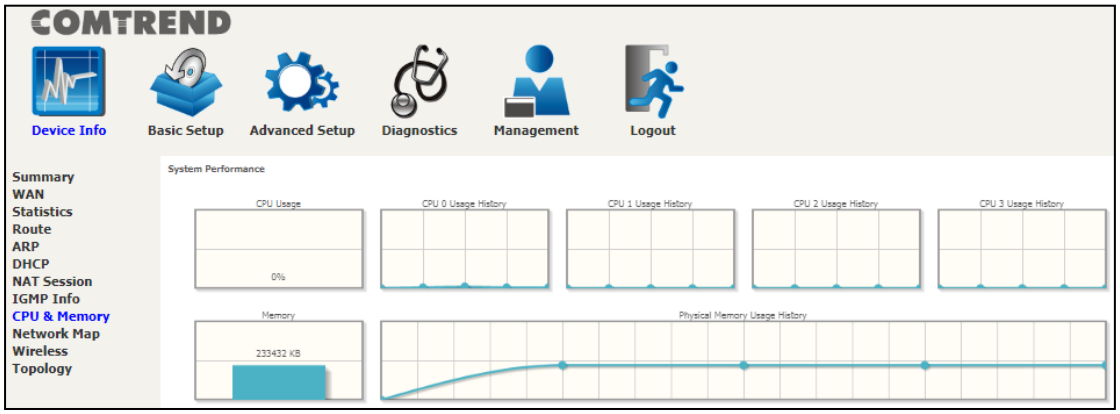
Click **IGMP Info** to display the list of IGMP entries broadcasting through the IGMP proxy enabled WAN connection.



Item	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
Last Report Time	The time of the last received IGMP report
Total Time(sec)	Total time that the IGMP stream has been played
Total Joins	Total IGMP join packets received for this IGMP address for this client
Total Leaves	Total IGMP leave packets received for this IGMP address for this client

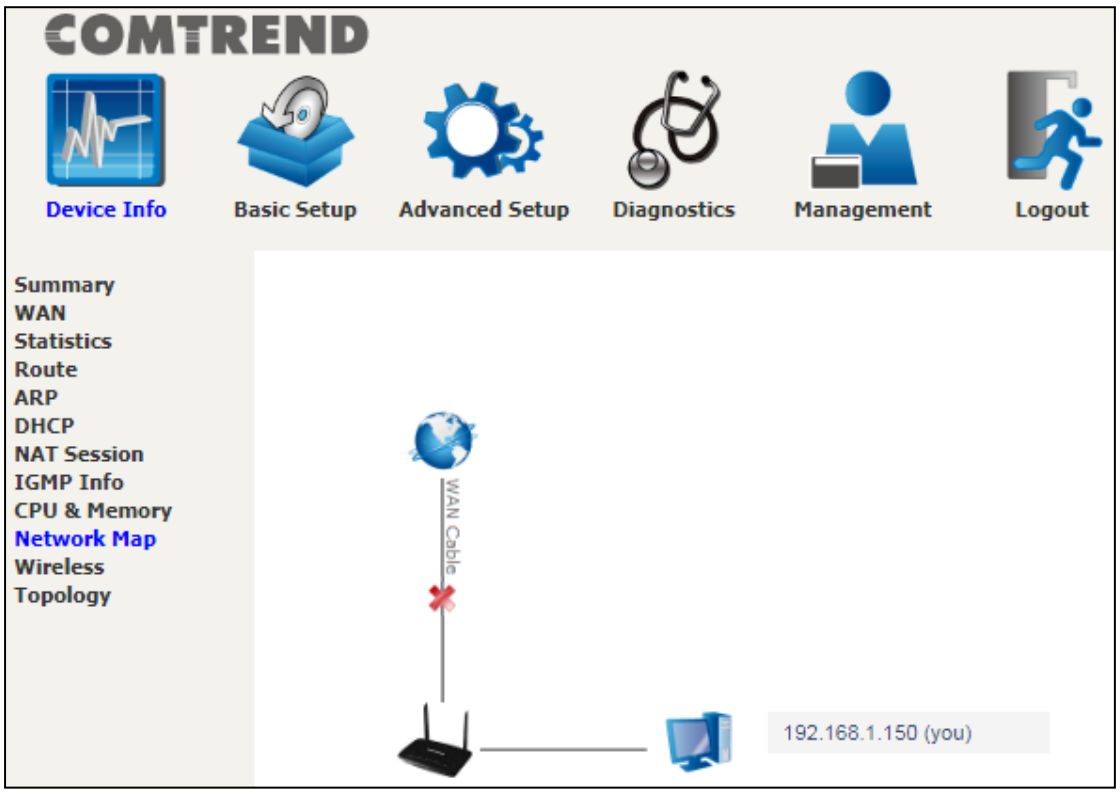
4.8 CPU & Memory

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



4.9 Network Map

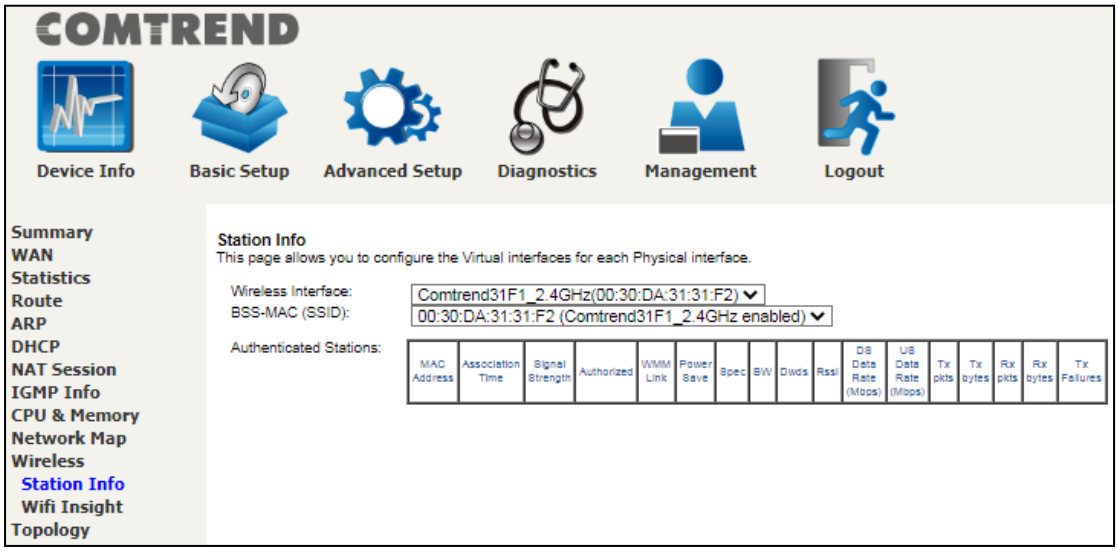
The network map is a graphical representation of router's wan status and LAN devices.



4.10 Wireless

4.10.1 Station Info

This page shows authenticated wireless stations and their status.

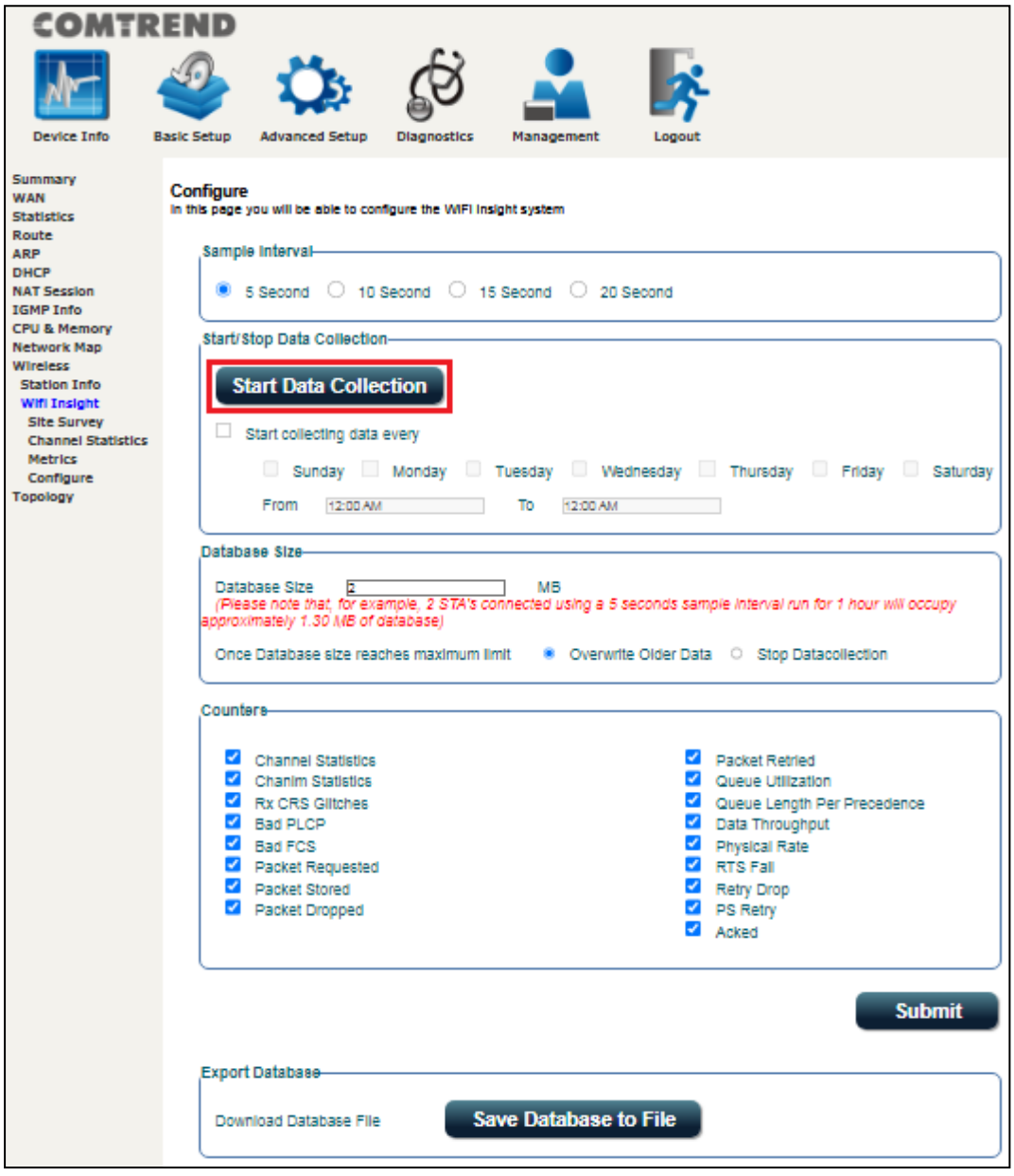


Consult the table below for descriptions of each column heading.

Item	Description
MAC Address	Lists the MAC address of all the stations.
Association Time	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
WMM Link	Lists those devices that utilize WMM
Power Save	Lists those devices that utilize the Power Save Feature
Spec	Wi-Fi Spec
BW	Bandwidth
Dwds	Lists the devices that utilize Dynamic WDS
Rssi	Received Signal Strength Indicator

4.10.2 WiFi Insight

This page allows you to configure the WiFi Insight system. The WiFi Insight system allows the wireless interface to collect beacon data from nearby devices and analyze traffic on the connected stations. This data collection requires memory storage and therefore needs to be configured prior to use. To begin, click on the "Start Data Collection" button if no change is needed.



Sample Interval
Select a desired sample interval (time interval) to collect sampling data with the WiFi insight system.

Start/Stop Data Collection
Check the checkbox of Start collecting data every (then select days & times).

Database Size
Define the dedicated database size to be used for the WiFi insight system (default is 2MB). Once the database size has reached its limit, select if you wish to **overwrite older data** or to **stop data collection.**

Counters

All counter options are selected (checked) by default. Uncheck any counters that that you do not want collected by the WiFi insight system. Click the **Submit** button to save your settings.

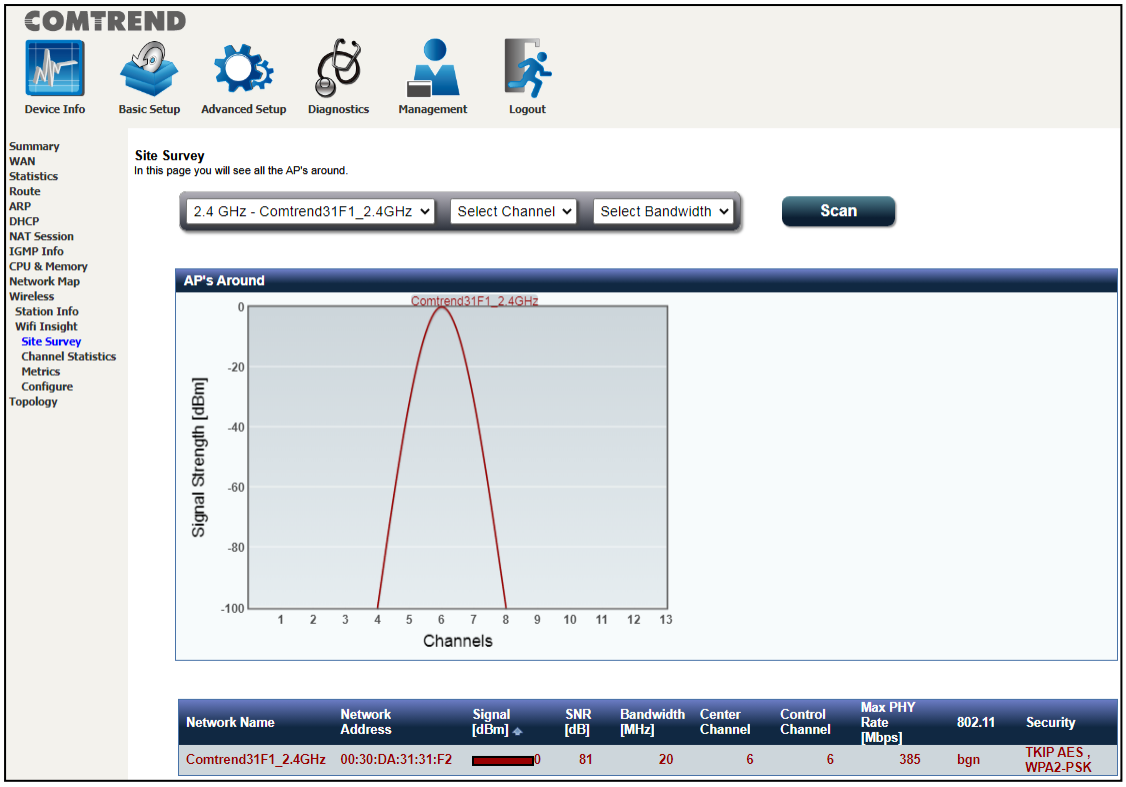
Export Database

Click the **Save Database to File** button to export and save the collected Wi-Fi data information file.

4.10.2.1 Site Survey

The graph displays wireless APs found in your neighborhood by channel collected under the WiFi insight system.

2.4GHz



Select the wireless network (2.4GHz in above example) that you wish to monitor from the drop-down menu.

1. Select the channel that you wish to monitor from the drop-down menu.
2. Select a bandwidth of the wireless network from the drop-down menu.
3. Click the Scan button to run the scan and display the results based on your selected preferences.

Consult the table below for descriptions of each column heading.

Item	Description
Network Name	SSIDs in the vicinity
Network Address	MAC address which belongs to SSIDs in the vicinity
Signal [dBm]	Signal Strength of each SSID
SNR [dB]	Signal-to-Noise Ratio of each SSID

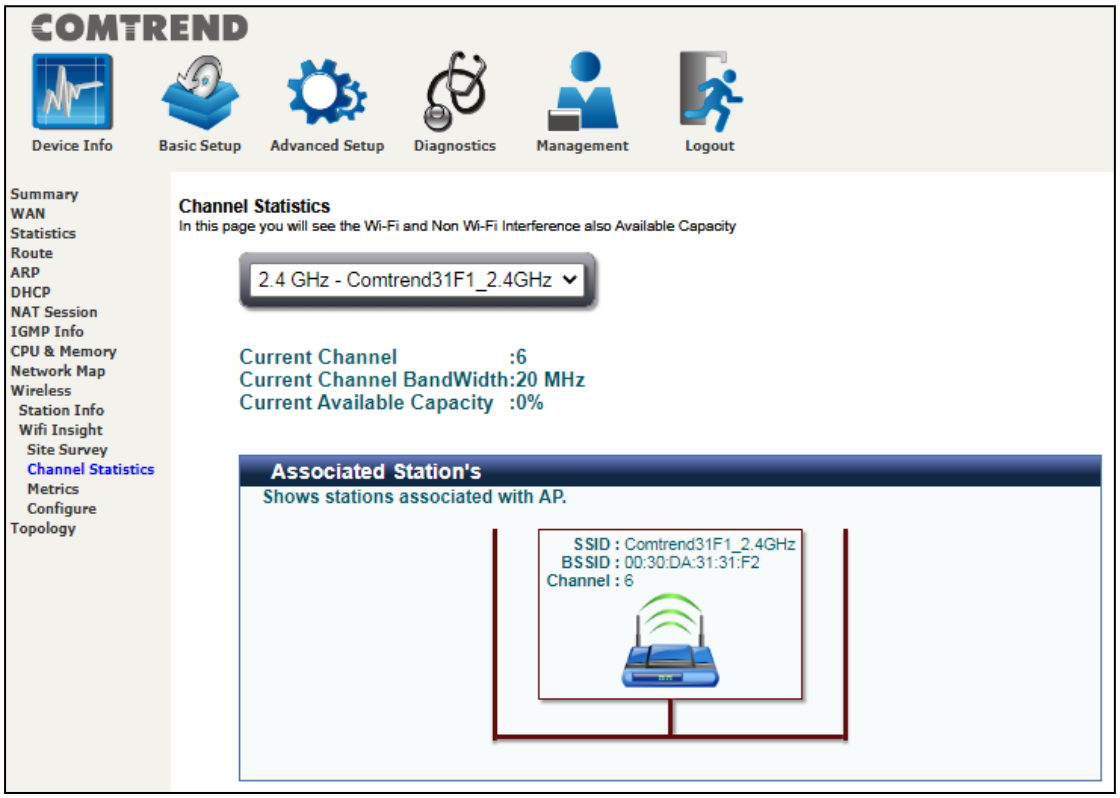
Bandwidth [MHz]	Bandwidth of each SSID
Center Channel	Center Channel of each SSID
Control Channel	Control Channel of each SSID
Max PHY Rate [Mbps]	Max PHY Rate of each SSID
802.11	802.11 type of each SSID
Security	Wi-Fi password encryption type of each SSID

4.10.2.2 Channel Statistics

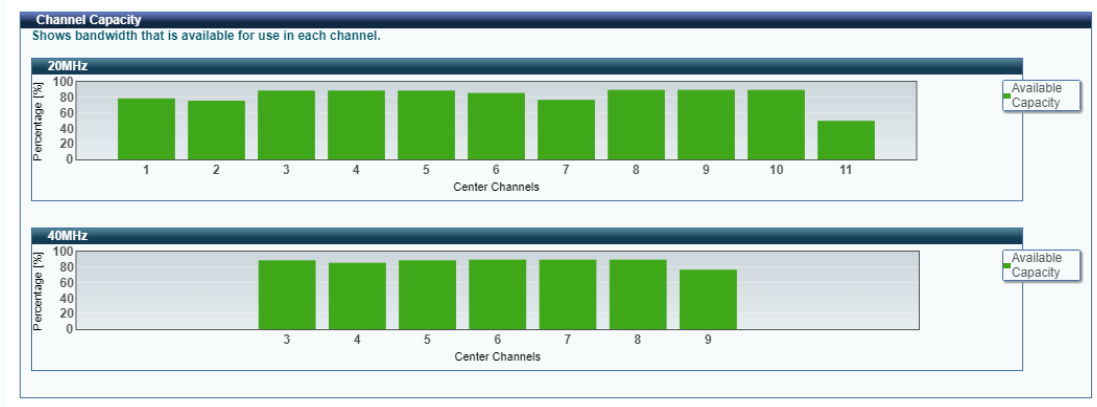
This page allows you to see the Wi-Fi and Non Wi-Fi interference, and also the available capacity. This page is broken down into individual parts below.

Click on the drop-down menu to select 2.4GHz or 5GHz interface.

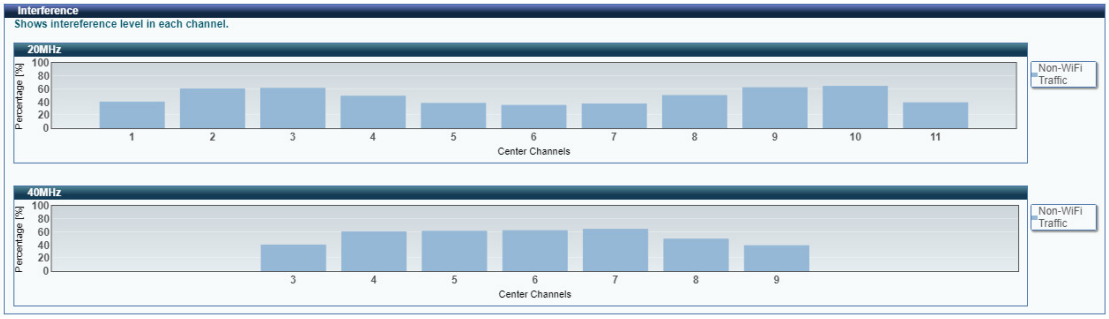
2.4 GHz



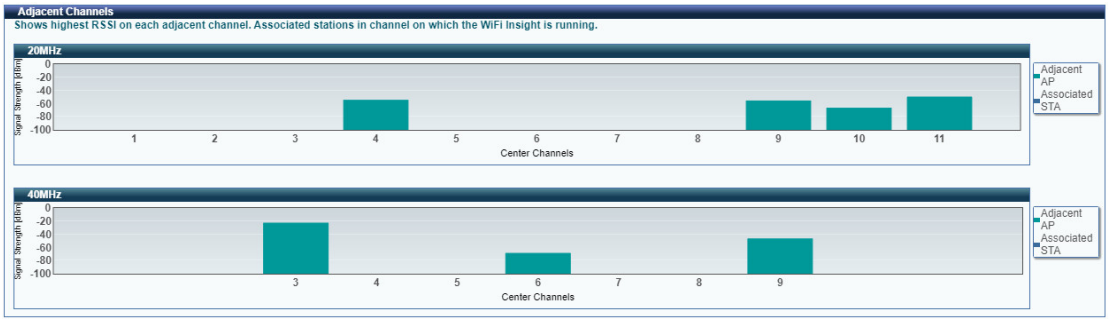
Shows the bandwidth that is available for use in each channel.



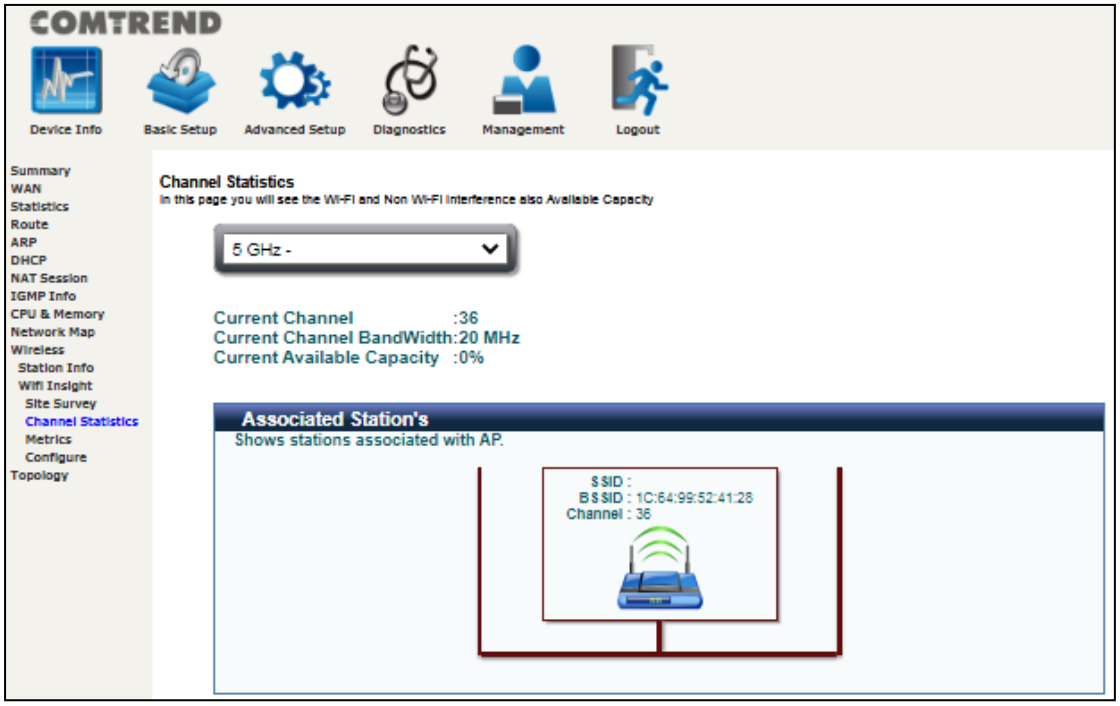
Shows interference level in each channel.



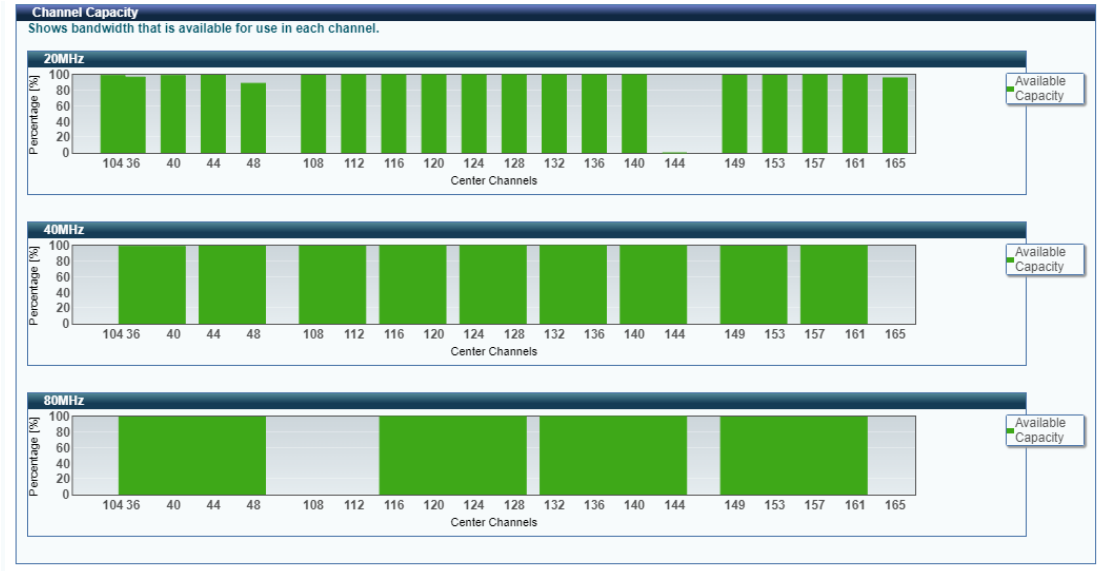
Shows the highest RSSI (Received Signal Strength Indicator) on each adjacent channel. Adjacent AP and associated stations are displayed for checking interference on those channels.



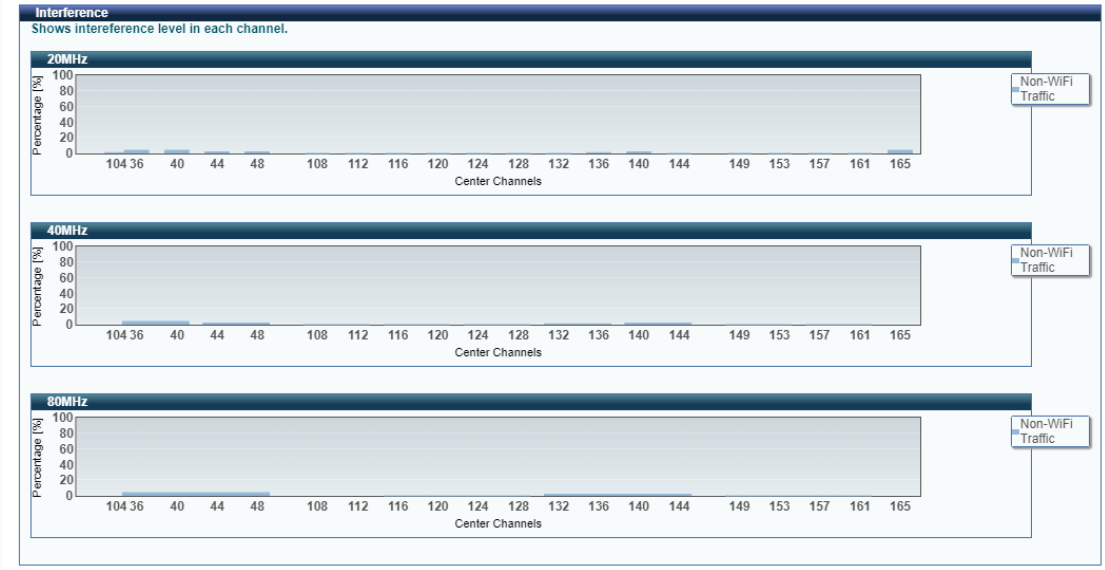
5 GHz



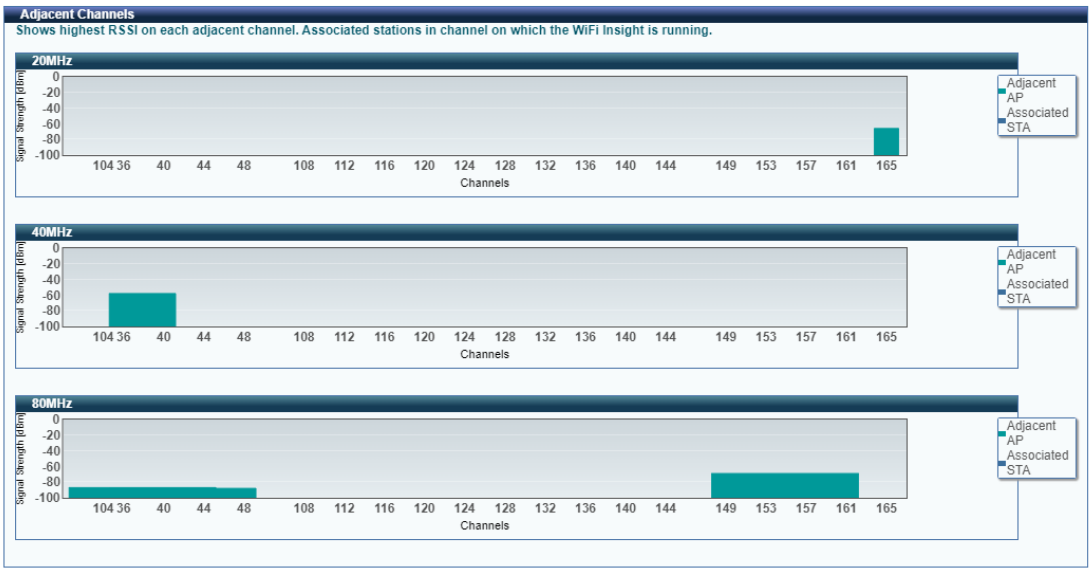
Shows the bandwidth that is available for use in each channel.



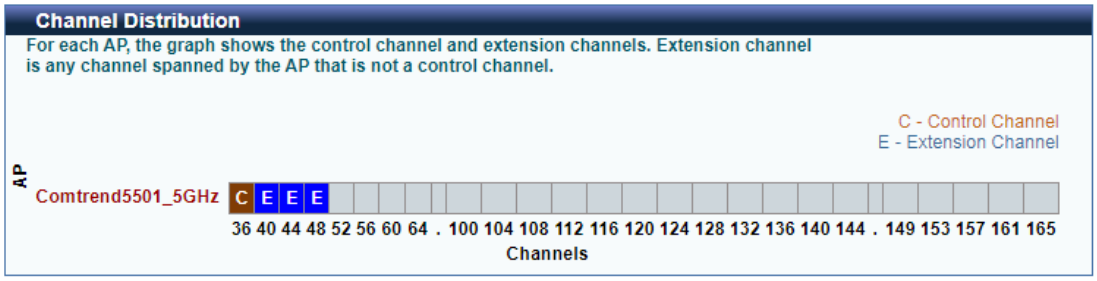
Shows interference level in each channel.



Shows the highest RSSI (Received Signal Strength Indicator) on each adjacent channel. Adjacent AP and associated stations are displayed for checking interference on those channels.

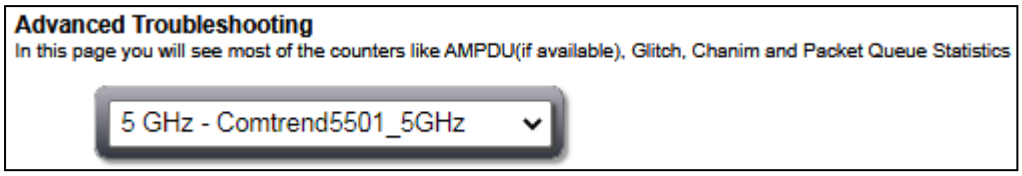


For each AP, the graph shows the control channel and extension channels. Extension channel is any channel spanned by the AP that is not a control channel.



4.10.2.3 Metrics (Advanced Troubleshooting)

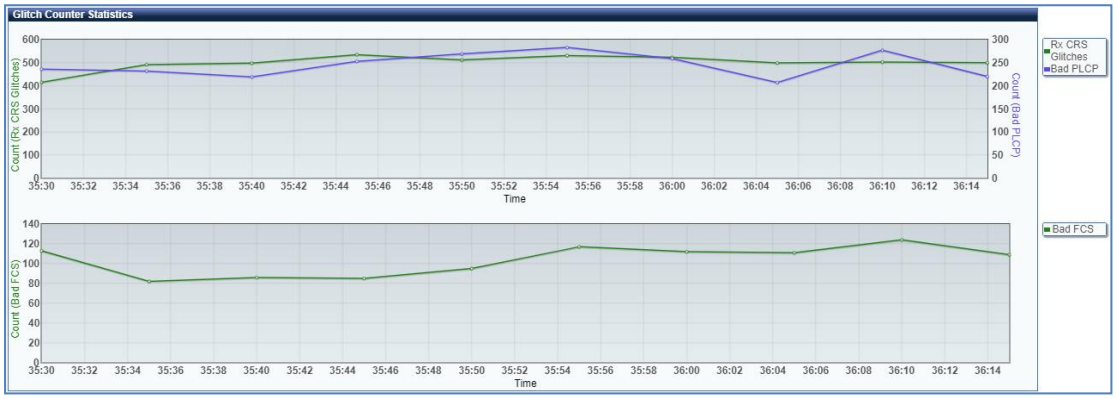
In this page you will see most of the counters like AMPDU(if available), Chanim, Glitch and Packet Queue Statistics. This page is broken down into individual parts below.



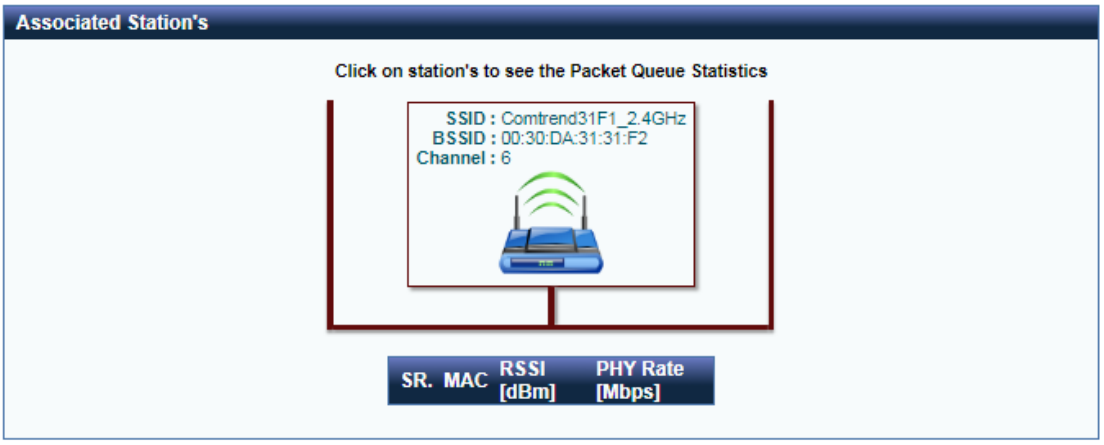
Click on the drop-down menu to select 2.4GHz or 5GHz interface.

Select the counter of interest to monitor the statistics received over time in the chanim statistics graph.

Shows the rx glitch counters, bad frame check sequence counters received from air over time.

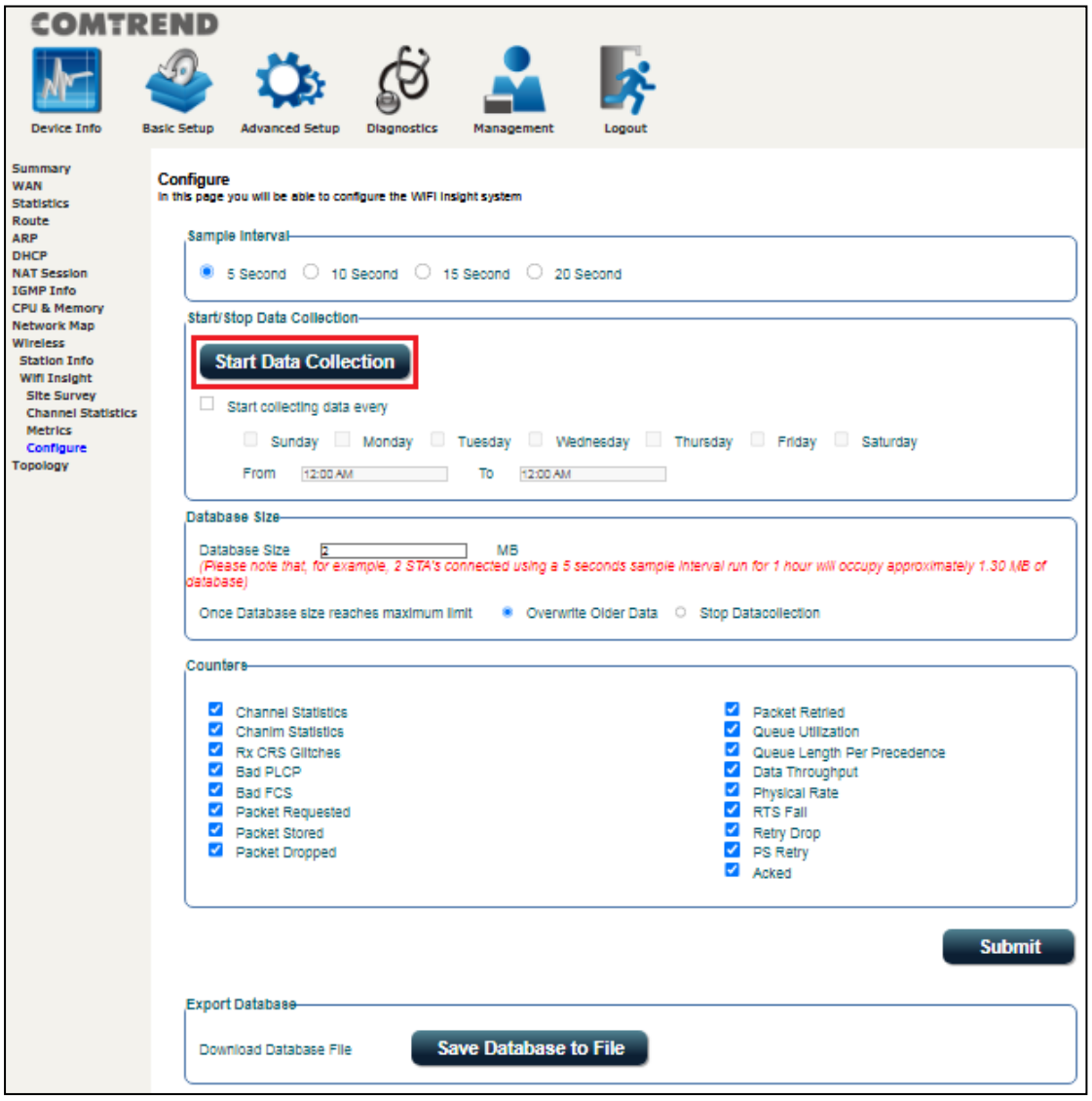


Lists the associated station to the wireless interface.



4.10.2.4 Configure

This page allows you to configure the WiFi Insight system. The WiFi Insight system allows the wireless interface to collect beacon data from nearby devices and analyze traffic on the connected stations. This data collection requires memory storage and therefore needs to be configured prior to use. To begin, click on the "Start Data Collection" button if no change is needed.



Sample Interval
Select a desired sample interval (time interval) to collect sampling data with the WiFi insight system.

Start/Stop Data Collection
Check the checkbox of Start collecting data every (then select days & times).

Database Size
Define the dedicated database size to be used for the WiFi insight system (default is 2MB). Once the database size has reached its limit, select if you wish to **overwrite older data** or to **stop data collection.**

Counters

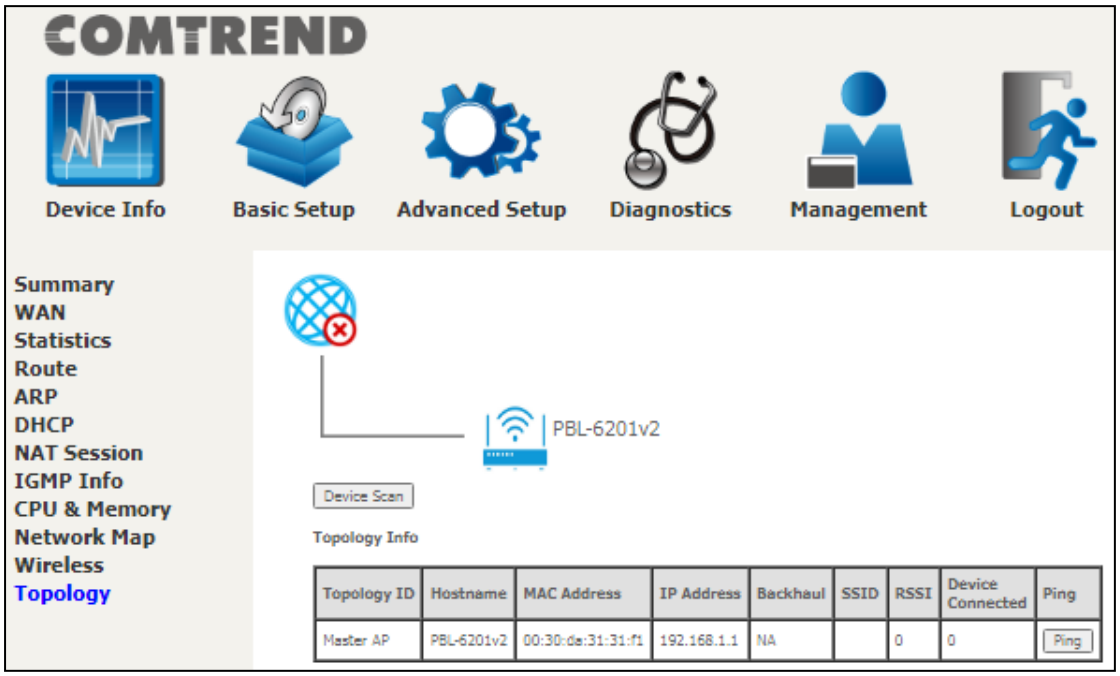
All counter options are selected (checked) by default. Uncheck any counters that that you do not want collected by the WiFi insight system. Click the **Submit** button to save your settings.

Export Database

Click the **Save Database to File** button to export and save the collected Wi-Fi data information file.

4.11 Topology

This displays the arrangement of devices of the communication network.
The dotted line represents a wireless connection, whereas a solid line represents a wired connection.



Click the **Device Scan** button to scan for the network topology.

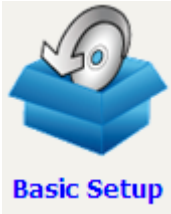
Consult the table below for descriptions of each column heading.

Item	Description
Topology ID	This shows different IDs for different host devices: Master AP: Host device is a gateway Node AP: Slave AP And it remains empty for Client devices
Hostname	Displays the name of the device
MAC Address	Displays the MAC address of the device
IP Address	Displays the IP address of the device
Backhaul	Shows the type of link for only Node AP; Ethernet: Connected by wired Ethernet PLC: Connected by Power Line WLan802.11: Connected by 802.11
SSID	Displays the SSID of the device
RSSI	Displays the received signal strength indicator (signal strength) for the device

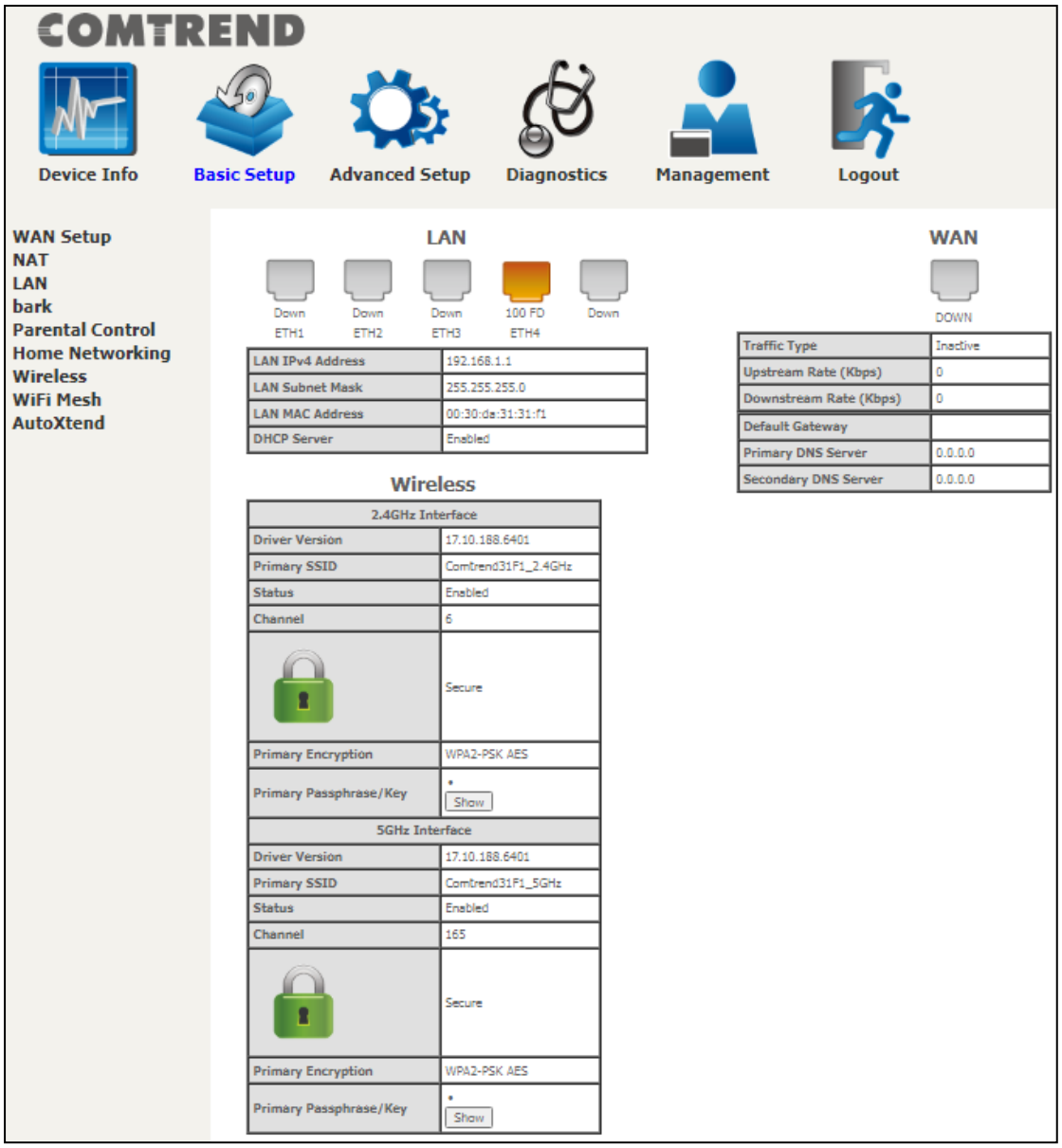
Device Connected	Displays the number of devices connected
Ping	Click the button and follow the onscreen instructions to ping a device.

Chapter 5 Basic Setup

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

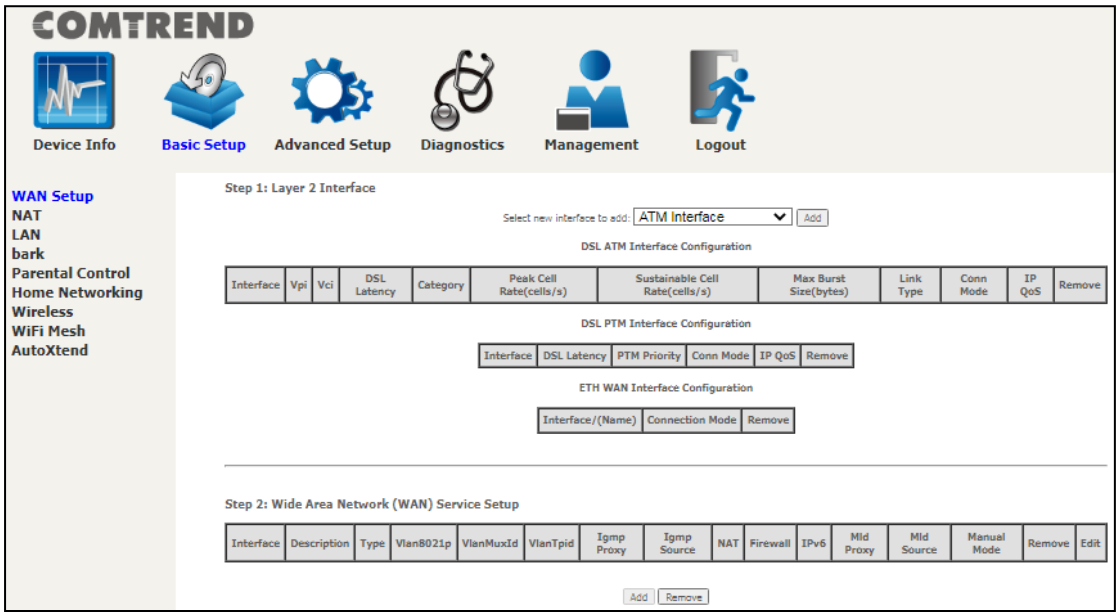


This will bring you to the following screen.



5.1 WAN Setup

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

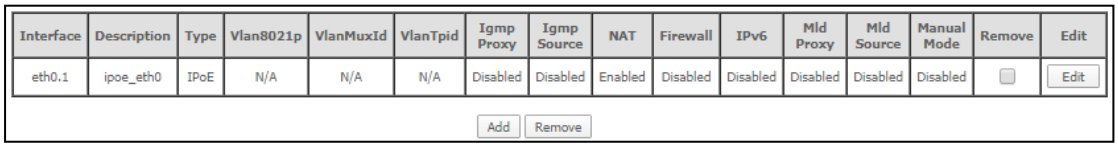


Click **Add** to create a new Layer 2 Interface (see Appendix F - Connection Setup).

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.**

Item	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
Manual Mode	Indicates the status of the PPP manual connect/disconnect button
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.**

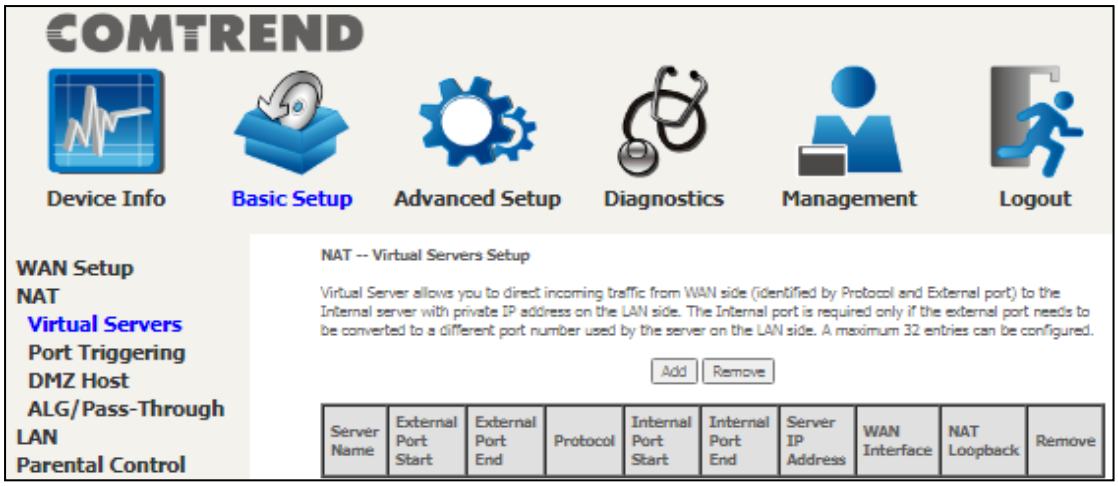
NOTE: Up to 16 PVC profiles can be configured and saved in flash memory.

5.2 NAT

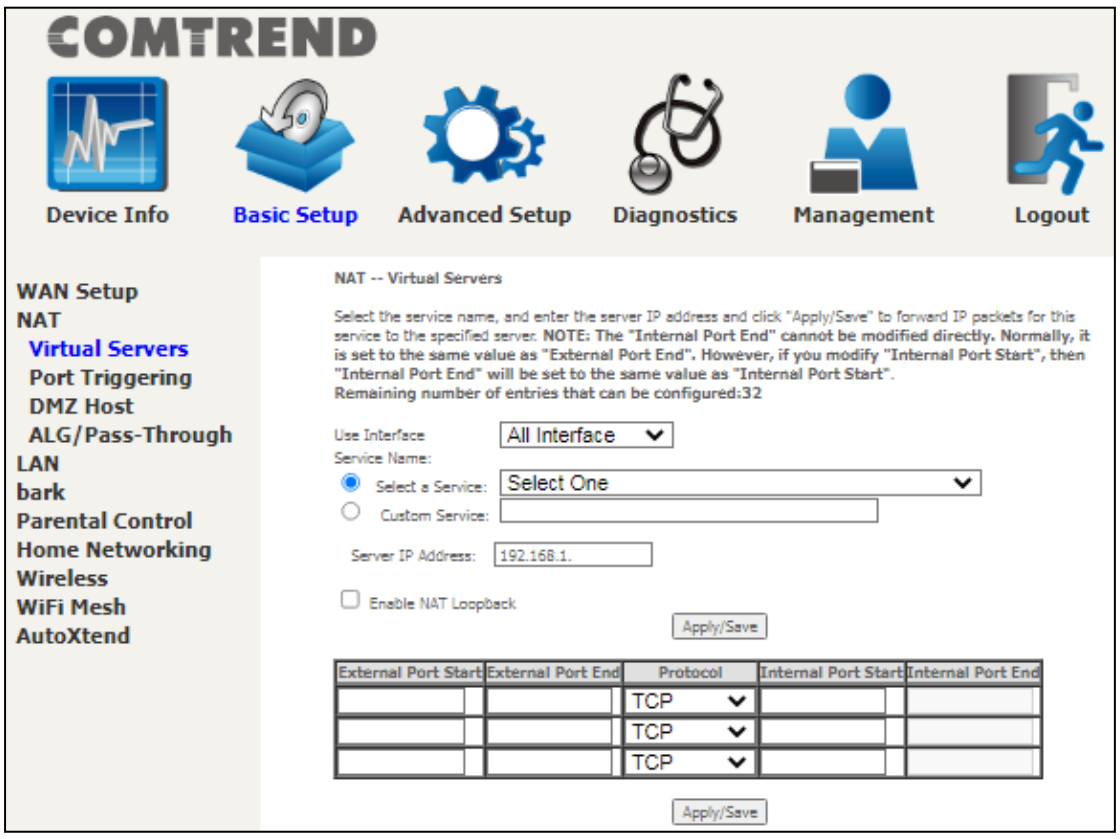
For NAT features under this section to work, NAT must be enabled in at least one PVC.

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.



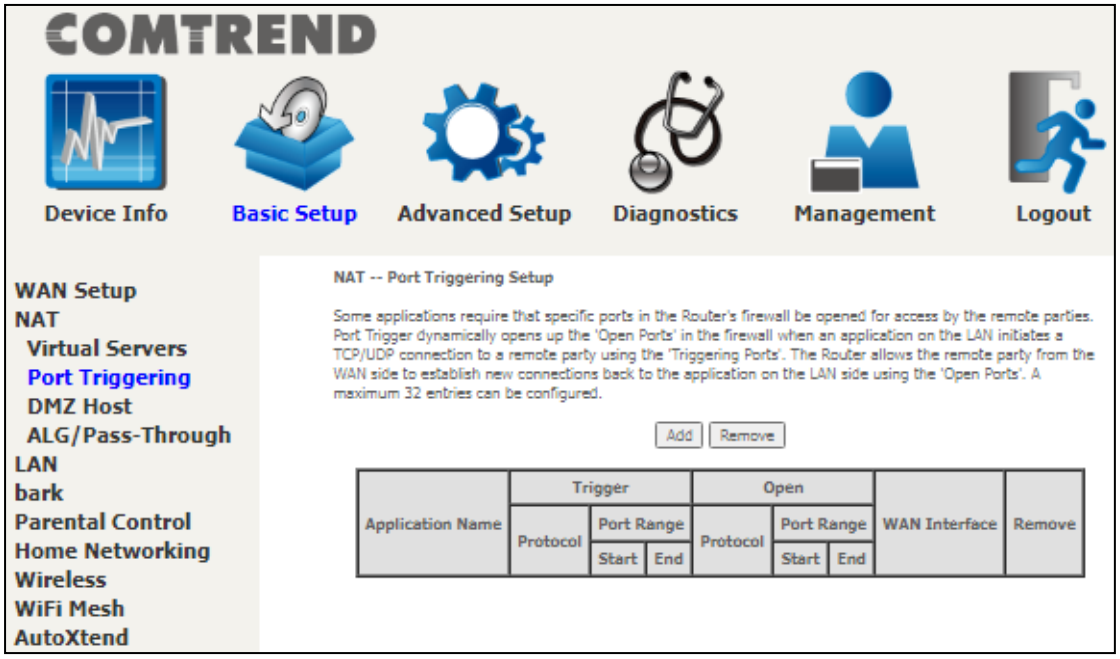
Click **Apply/Save** to apply and save the settings.

Consult the table below for item descriptions.

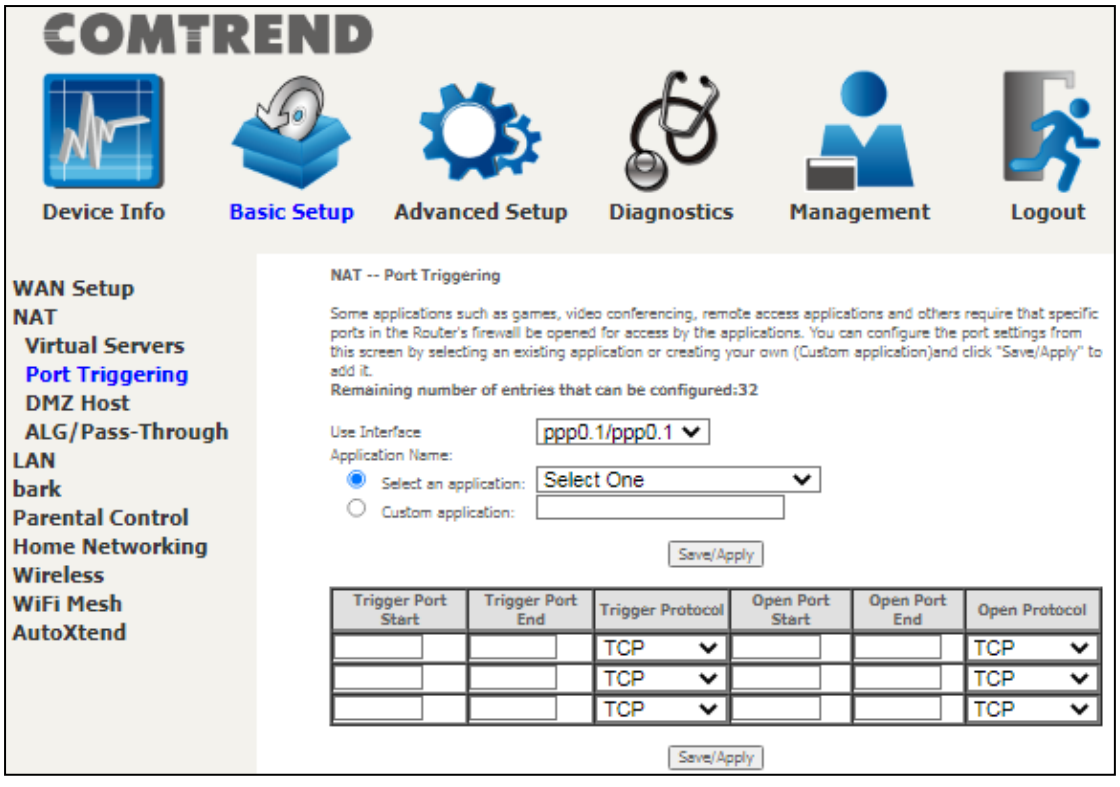
Item	Description
Use Interface	Select a WAN interface from the drop-down menu. If you choose All Interface, server rules will be created for all WAN interfaces.
Select a Service **Or** Custom Service	User should select the service from the list. **Or** User can enter the name of their choice.
Server IP Address	Enter the IP address for the server.
Enable NAT Loopback	Allows local machines to access virtual server via WAN IP Address
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.



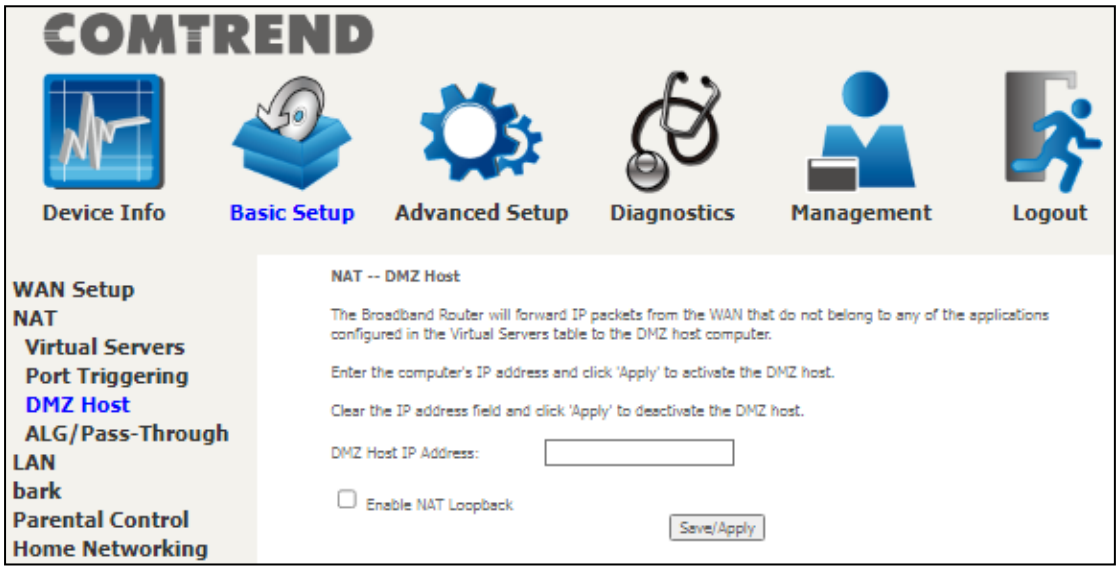
Click **Save/Apply** to save and apply the settings.

Consult the table below for item descriptions.

Item	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.
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.



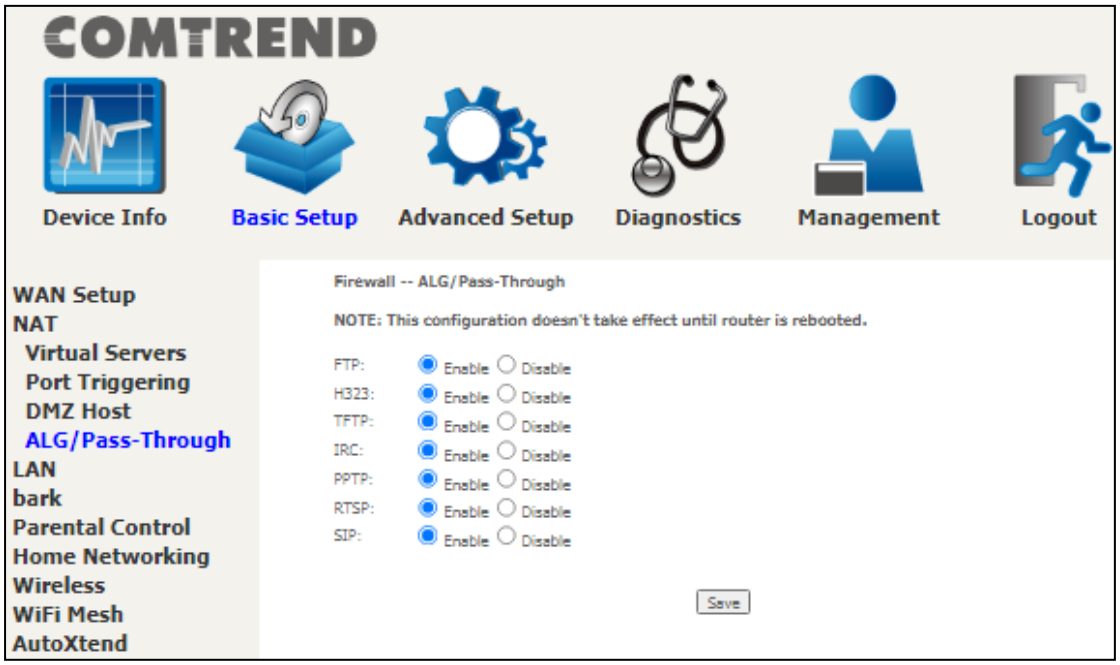
To **Activate** the DMZ host, enter the DMZ host IP address and click **Save/Apply**.

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

Enable NAT Loopback: Check the checkbox to allow local machines to access virtual server via WAN IP Address.

5.2.4 ALG/Pass-Through

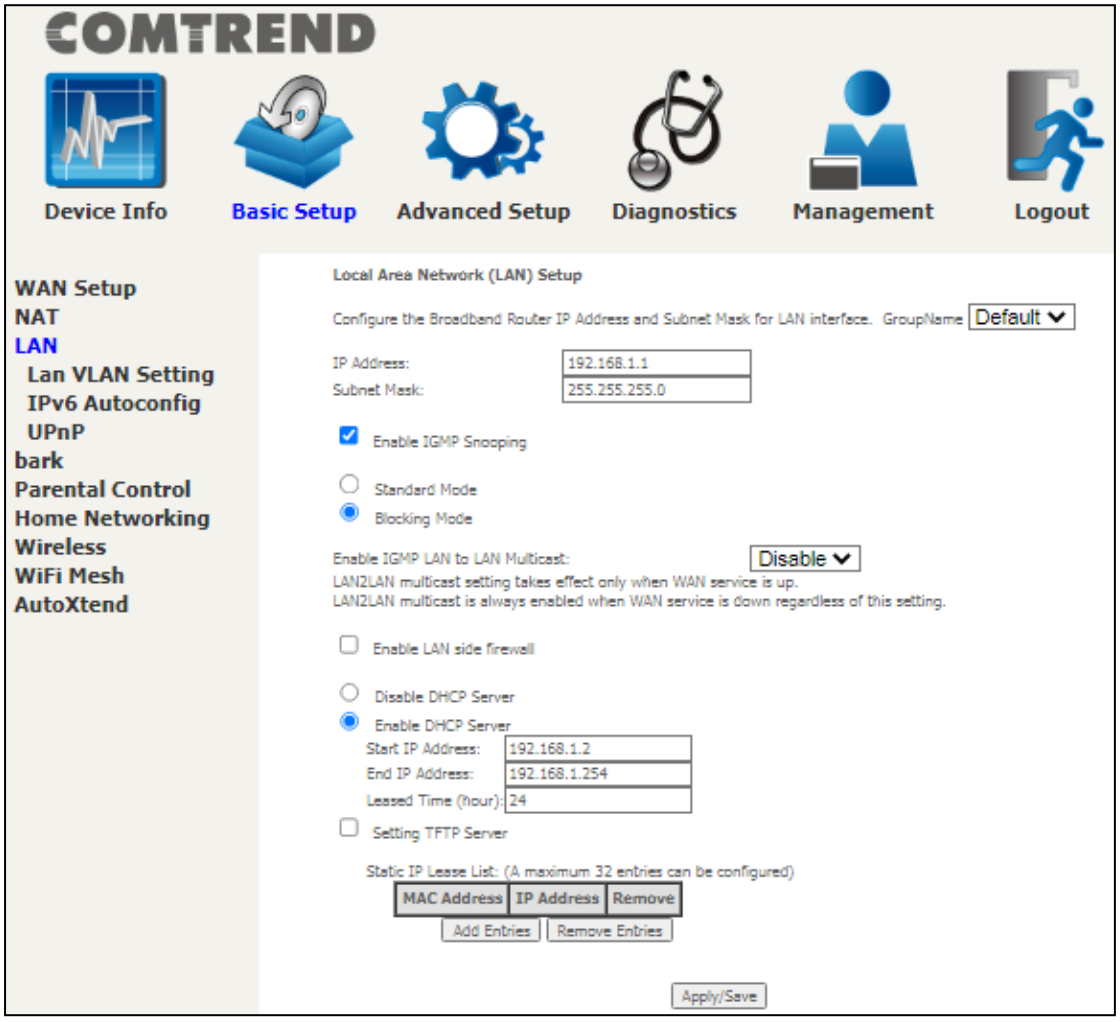
Support ALG Pass-through for the listed protocols.



To allow/deny the corresponding ALG protocol, select Enable / Disable and then click the **Save** button. After reboot, the protocol will be added/removed to/from the system module.

5.3 LAN

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



The settings shown above are described below.

GroupName: Select an Interface Group.

1st LAN INTERFACE

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

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

Enable IGMP Snooping: Enable by checking the checkbox ☑.

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.

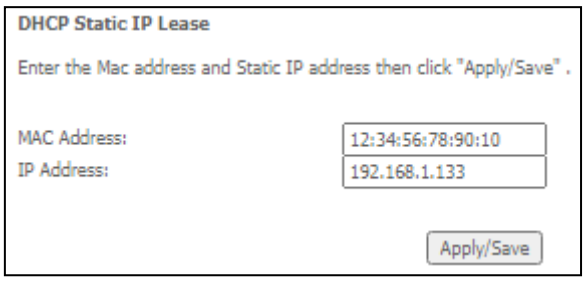
Enable LAN side firewall: Enable by ticking the checkbox ☑.

DHCP Server: To enable DHCP, select **Enable DHCP server** and enter Start and End IP addresses and the Leased Time. This setting configures the router to automatically assign IP, default gateway and DNS server addresses to every PC on your LAN.

Setting TFTP Server: Enable by ticking the checkbox ☑. Then, input the TFTP server address or an IP address.

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

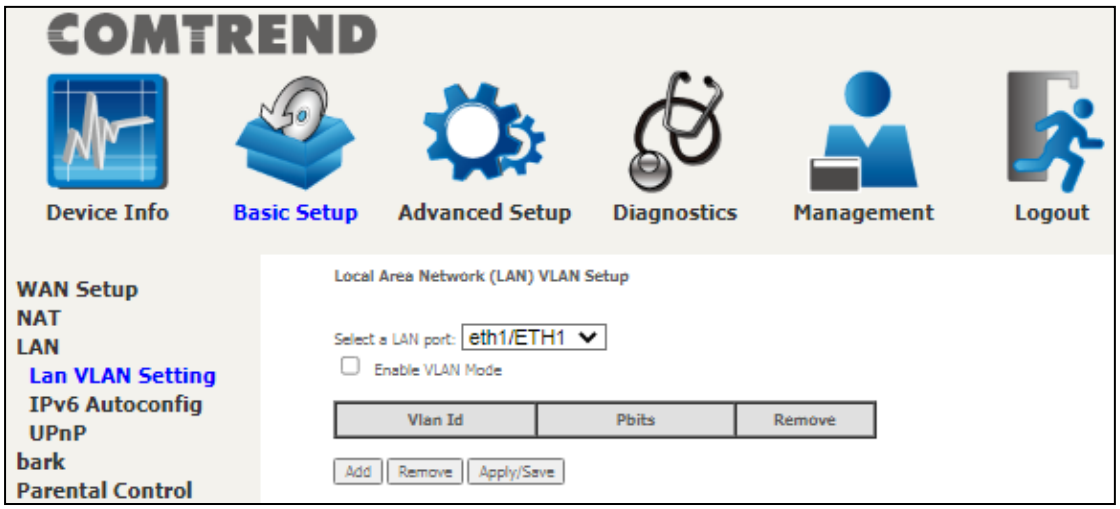
To add an entry, enter MAC address and Static IP and then click **Apply/Save**.



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

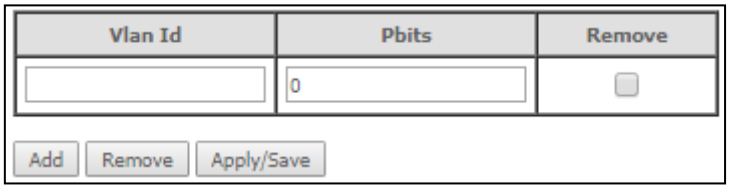
5.3.1 Lan VLAN Setting

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



To enable VLAN Mode, check the checkbox and click the **Apply/Save** button.

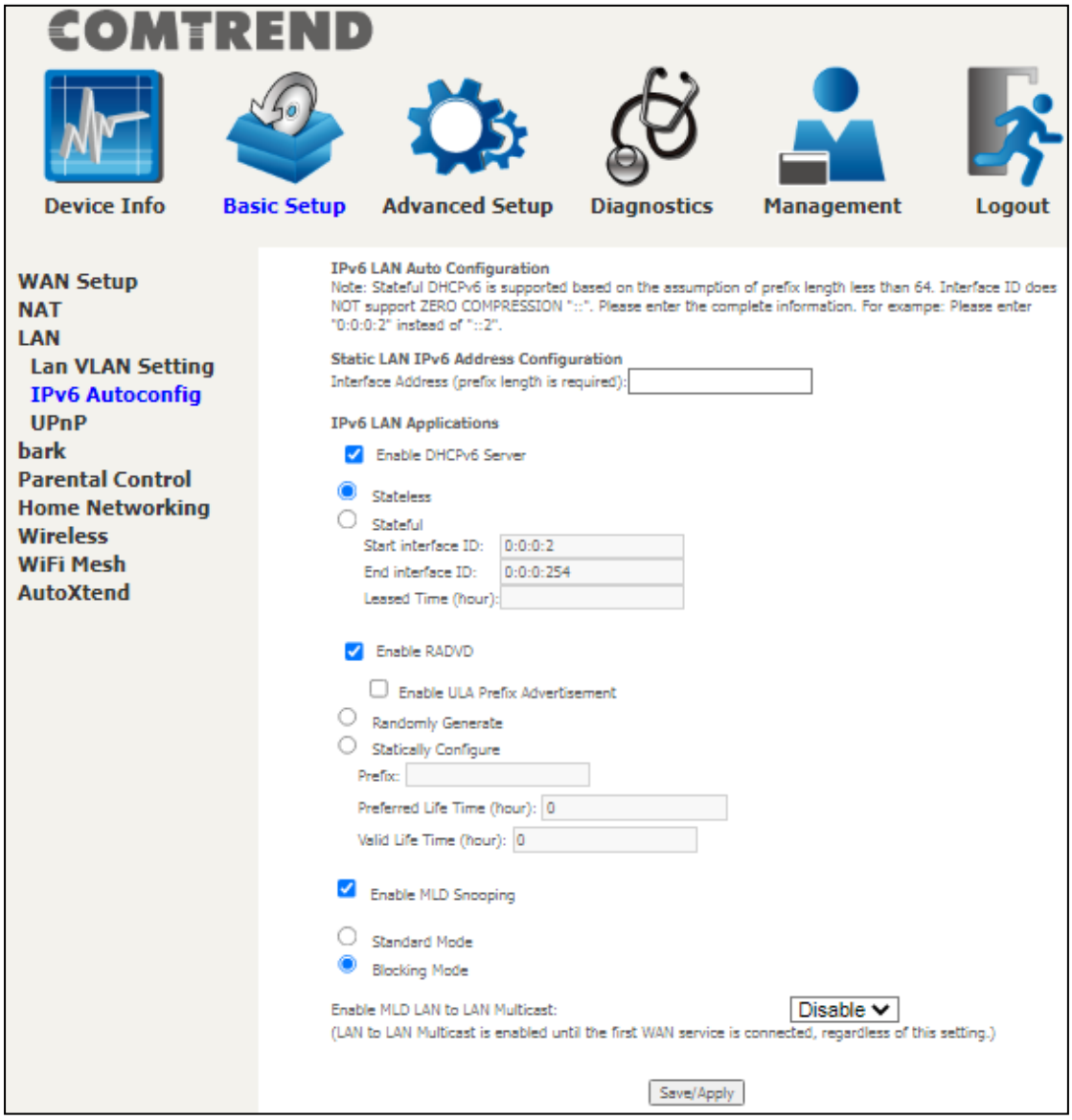
Click the **Add** button to display the following.



Item	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**.



The settings shown above are described below.

Static LAN IPv6 Address Configuration

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

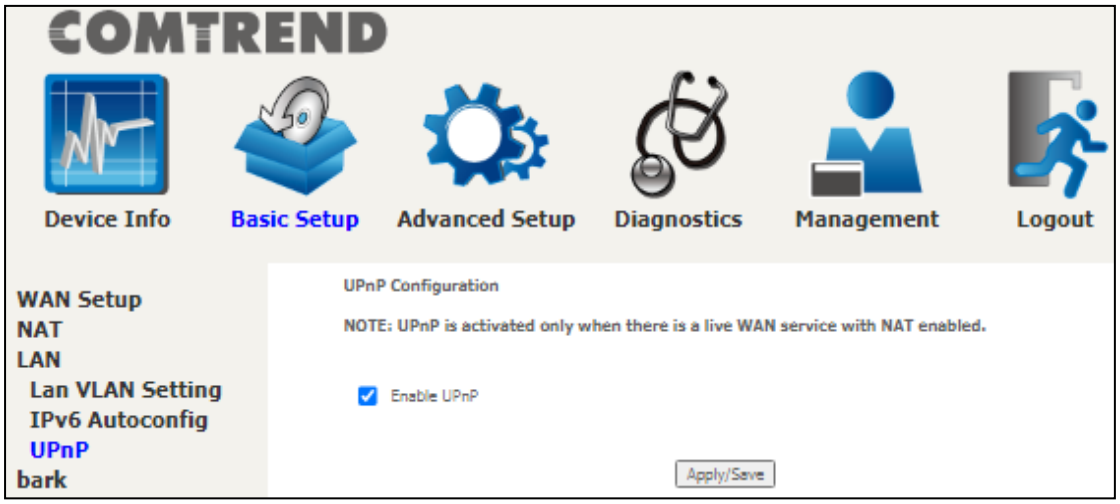
IPv6 LAN Applications

Item	Description
Stateless	Use stateless configuration
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

Item	Description
Enable RADVD	Enable use of router advertisement daemon
Enable ULA Prefix Advertisement	Allow RADVD to advertise Unique Local Address Prefix
Randomly Generate	Use a Randomly Generated Prefix
Statically Configure Prefix	Specify 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	LAN to LAN Multicast is automatically enabled until the first WAN service is configured. Once there is a WAN service, the ability to operate LAN to LAN multicasts is controlled by setting the pull down menu option to Enable or Disable on the LAN page.

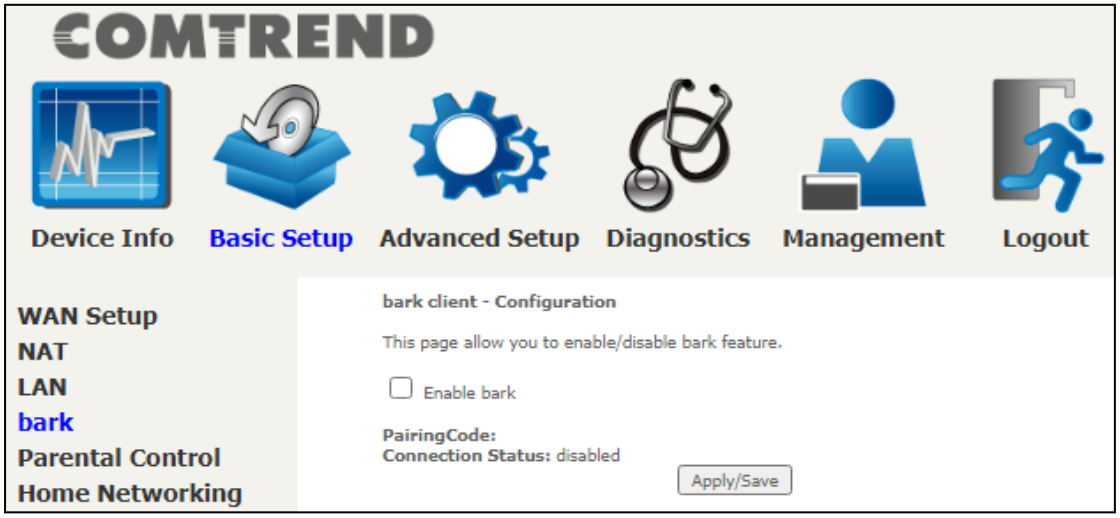
5.3.3 UPnP

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

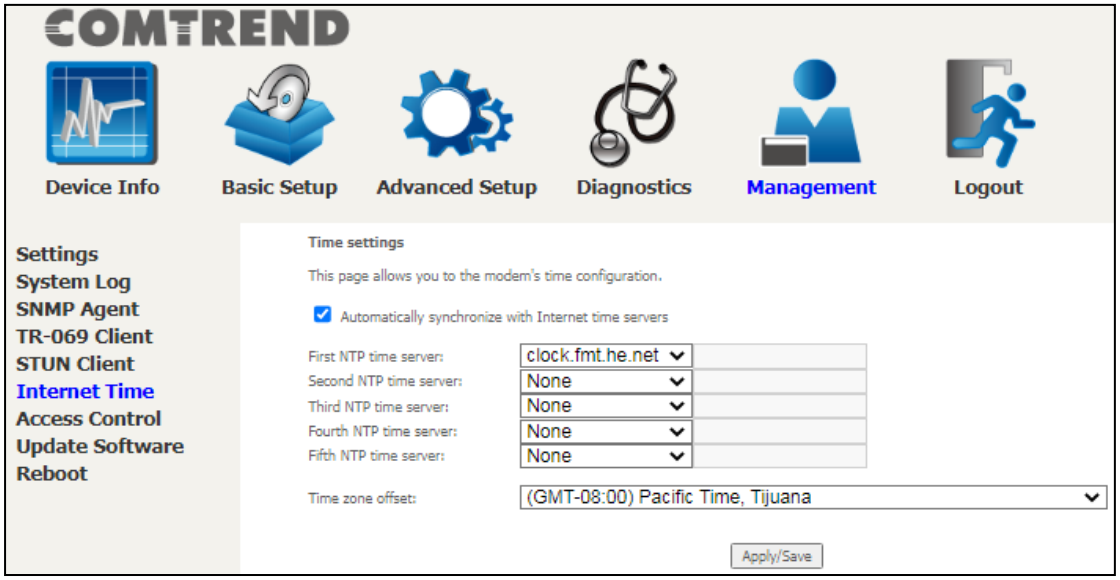


5.4 Bark

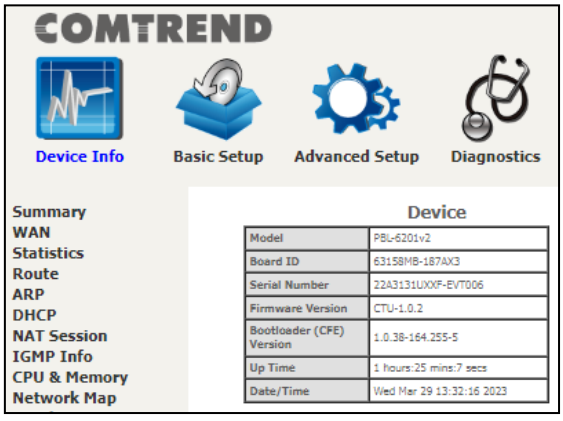
This page allows you to enable/disable bark feature. Bark has parental control features to provide online safety for kids.



Step 1: Check the checkbox and click the **Apply/Save** button to enable this feature.



Step 2: Click **Management/Internet Time**, and check the "Automatically synchronize with Internet time servers" checkbox. Then click the **Apply/Save** button.



Step 3: Click **Device Info/Summary** to check that the CPE date and time are correct.

Note: For more information, contact your local ISP / Comtrend support about Bark options.

https://www.bark.us/faq/

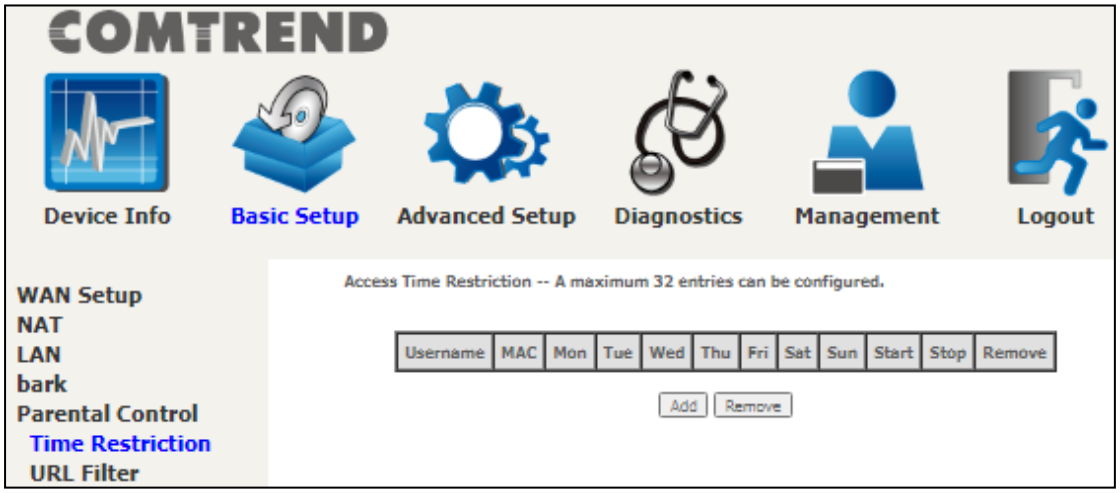
5.5 Parental Control

This selection provides WAN access control functionality.

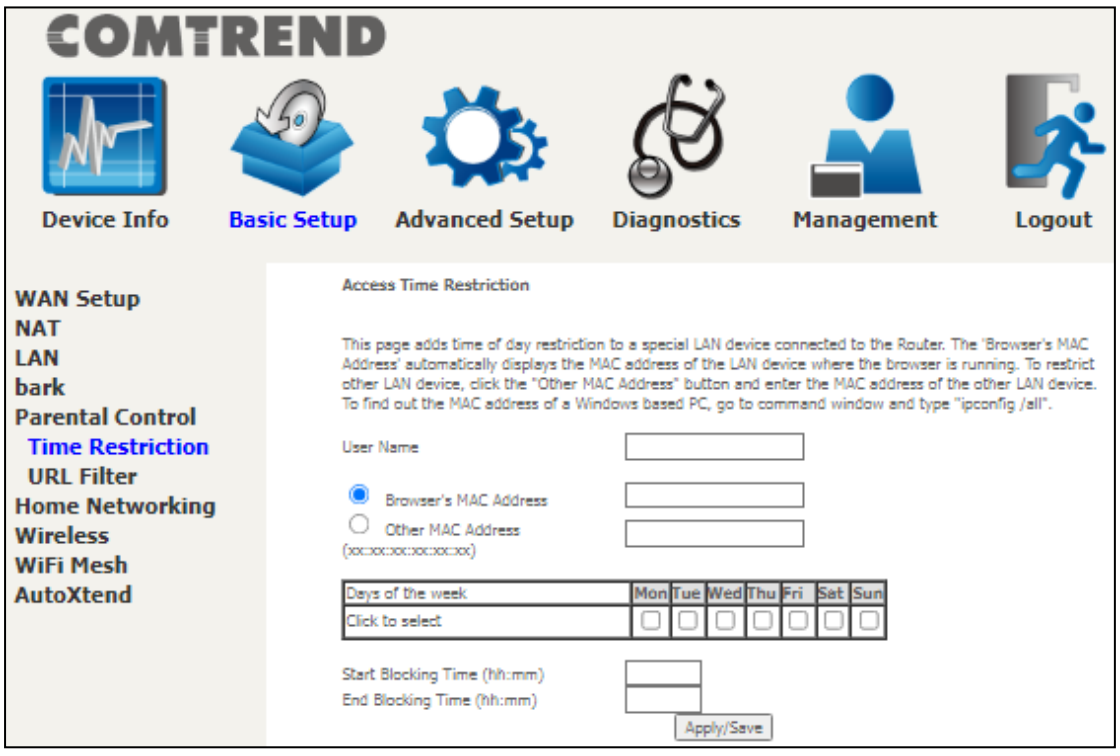
5.5.1 Time Restriction

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 8.6 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.

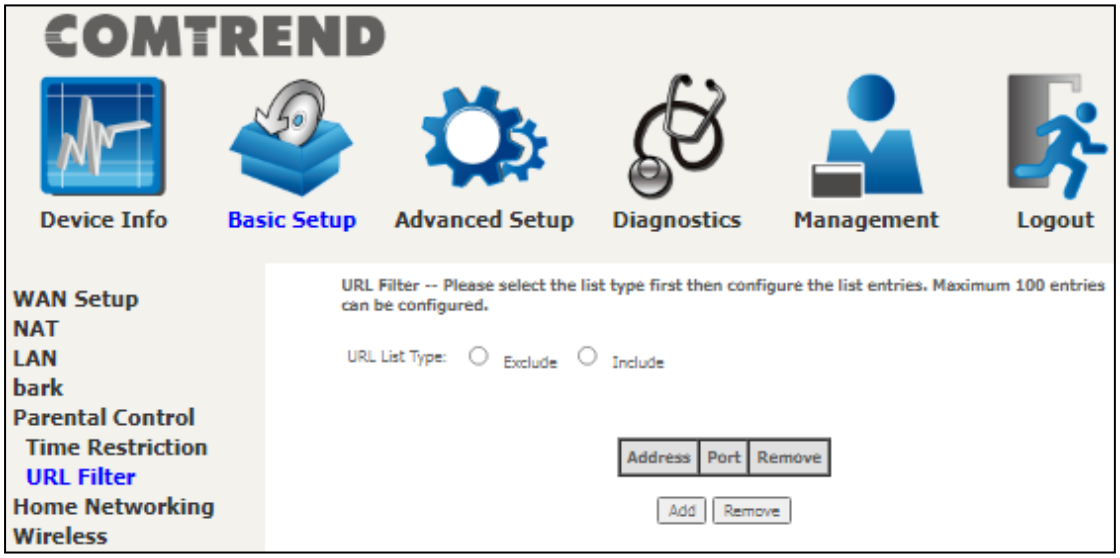


See below for item descriptions. Click **Apply/Save** to add a time restriction.

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.



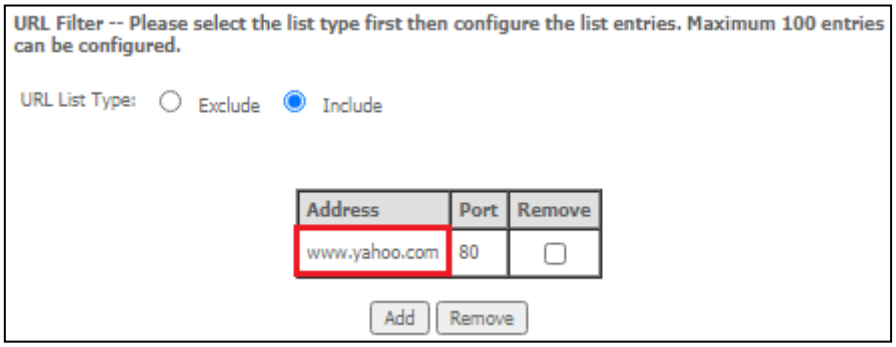
Select URL List Type: Exclude or Include.

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 **Apply/Save** to add the entry to the URL filter. URL Addresses begin with "www", as shown in this example.

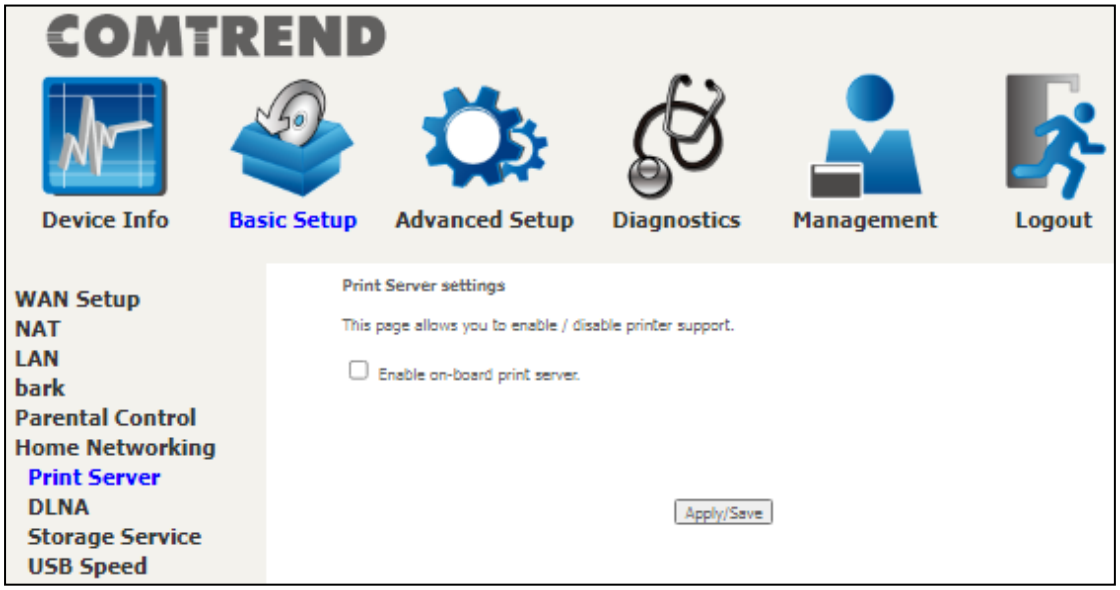


A maximum of 100 entries can be added to the URL Filter list.

5.6 Home Networking

5.6.1 Print Server

This page allows you to enable or disable printer support.

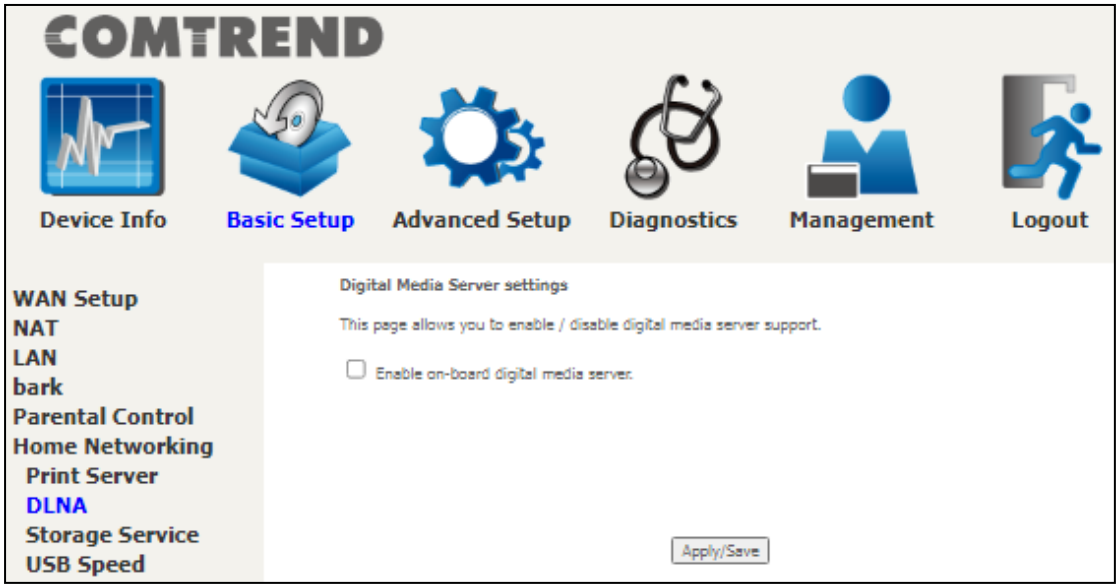


Please reference **Appendix E** to see the procedure for enabling the Printer Server.

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 **Apply/Save** to enable the DLNA media server.

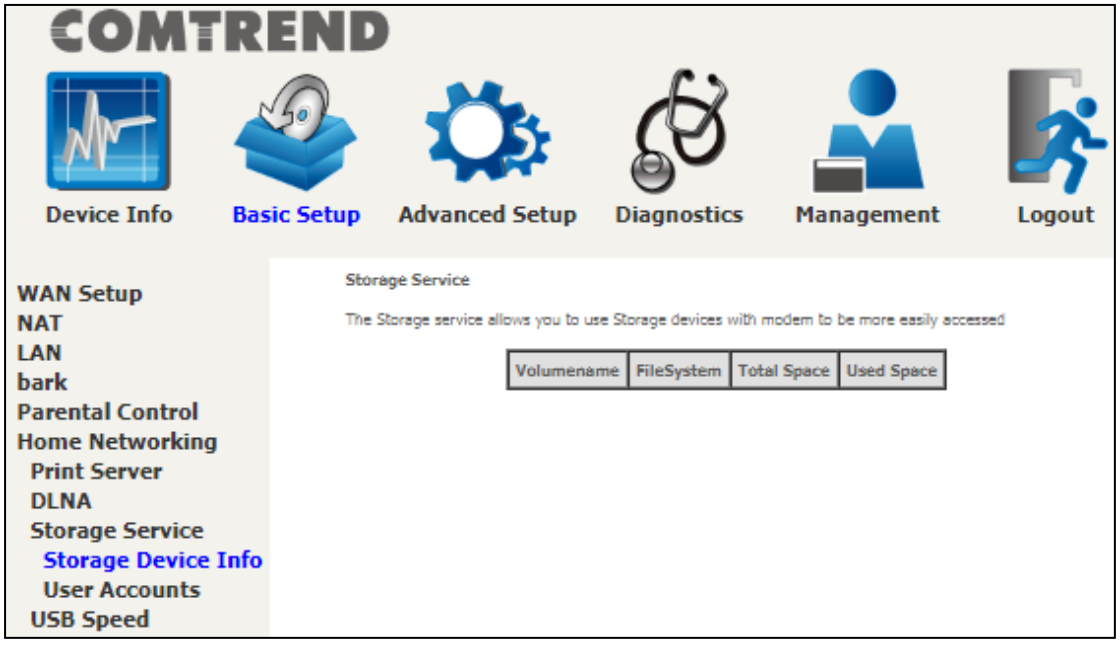


5.6.3 Storage Service

The Storage service allows you to use Storage devices with modem to be more easily accessed.

5.6.3.1 Storage Device Info

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

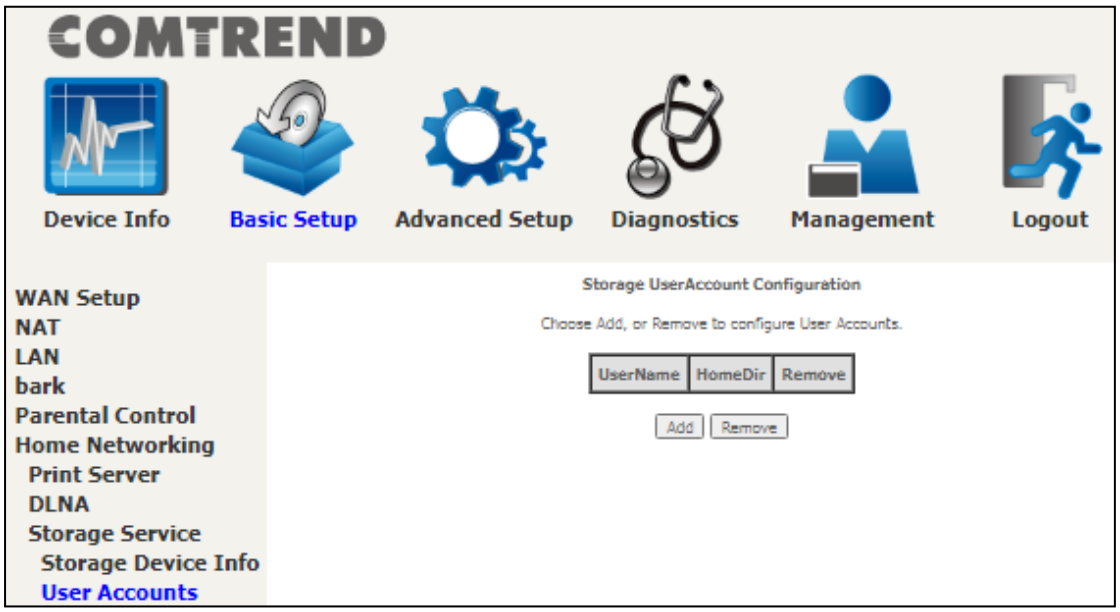


Display after storage device attached (for your reference).

Volumename	FileSystem	Total Space	Used Space
disk1_1	fat	962	6

5.6.3.2 Storage User Accounts

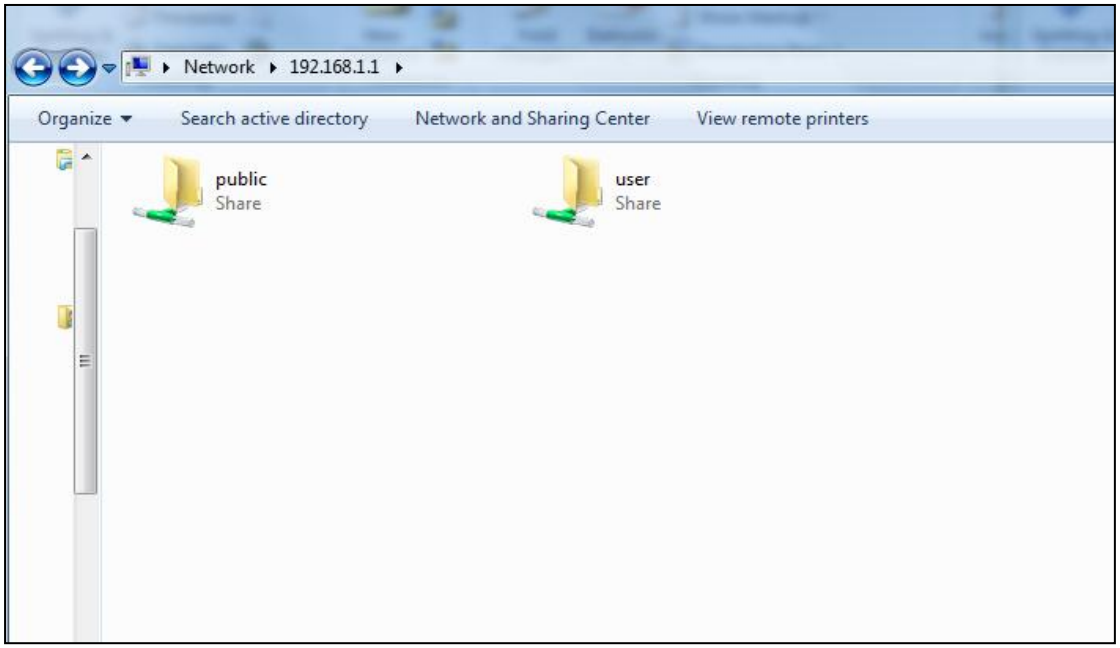
Add a storage account to access the USB device for the samba access system.



Click the **Add** button to display the following. volumeName would be disk1_1 if only 1 USB has been plugged into the device.

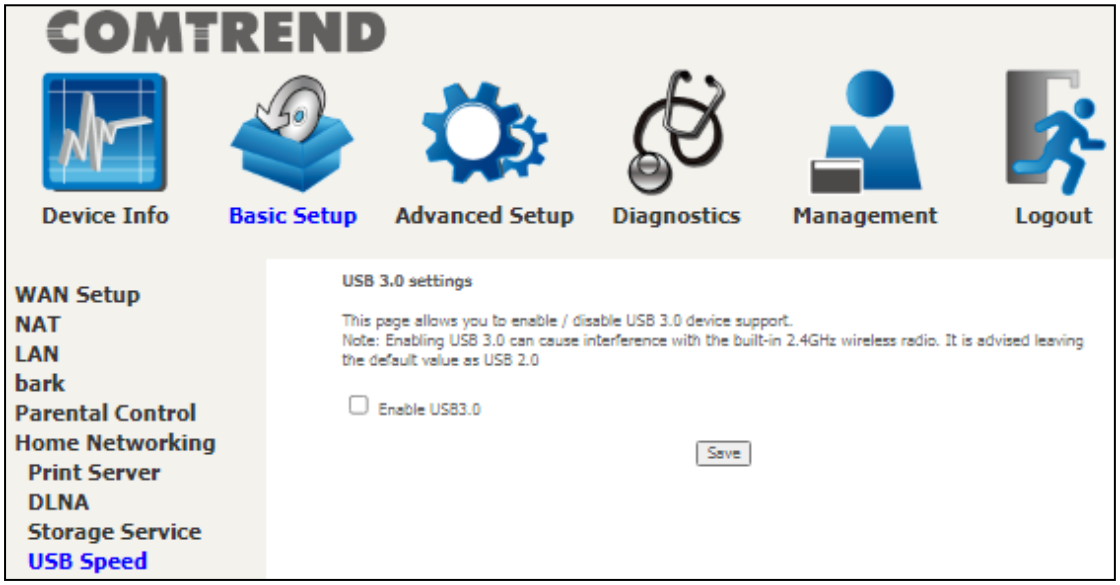
In the boxes provided, enter the user name, password and volume name on which the home directory is to be created. Then click the **Apply/Save** button.

In any windows folder, enter the address \\192.168.1.1 to access the samba folder created. A password prompt will show. Enter username password as configured. Access \\192.168.1.1 again (or refresh the screen), the user folder will now be available for access.



5.6.4 USB Speed

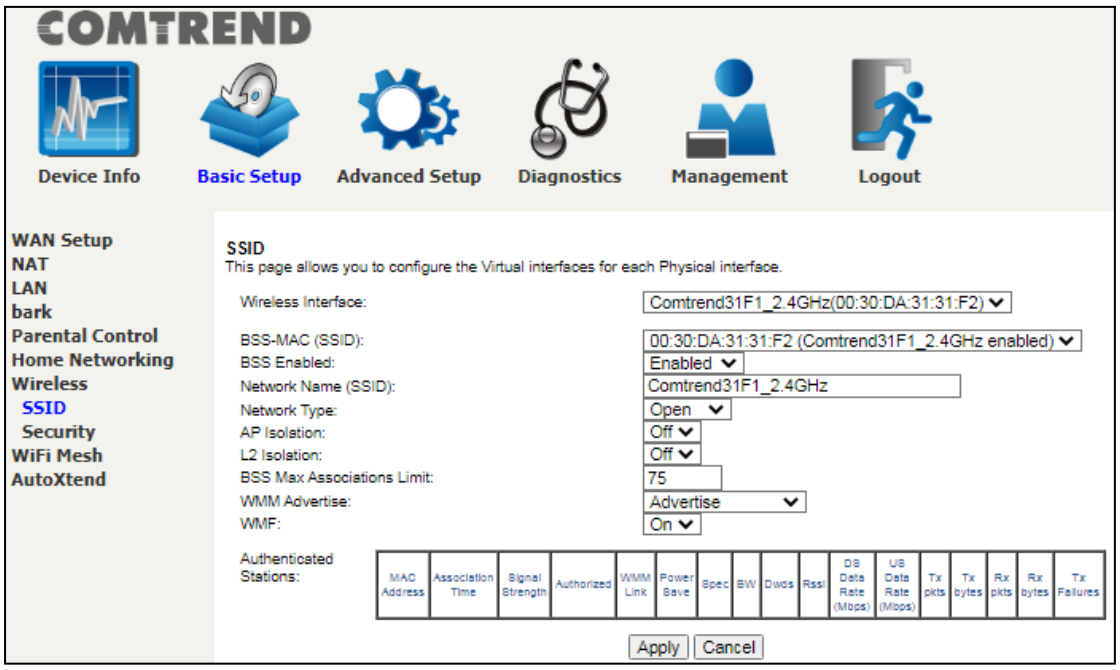
This page allows you to enable / disable USB 3.0 device support.
Note: Enabling USB 3.0 can cause interference with the built-in 2.4GHz wireless radio. It is advised leaving the default value as USB 2.0



5.7 Wireless

5.7.1 SSID

This page allows you to configure the Virtual interfaces for each Physical interface.



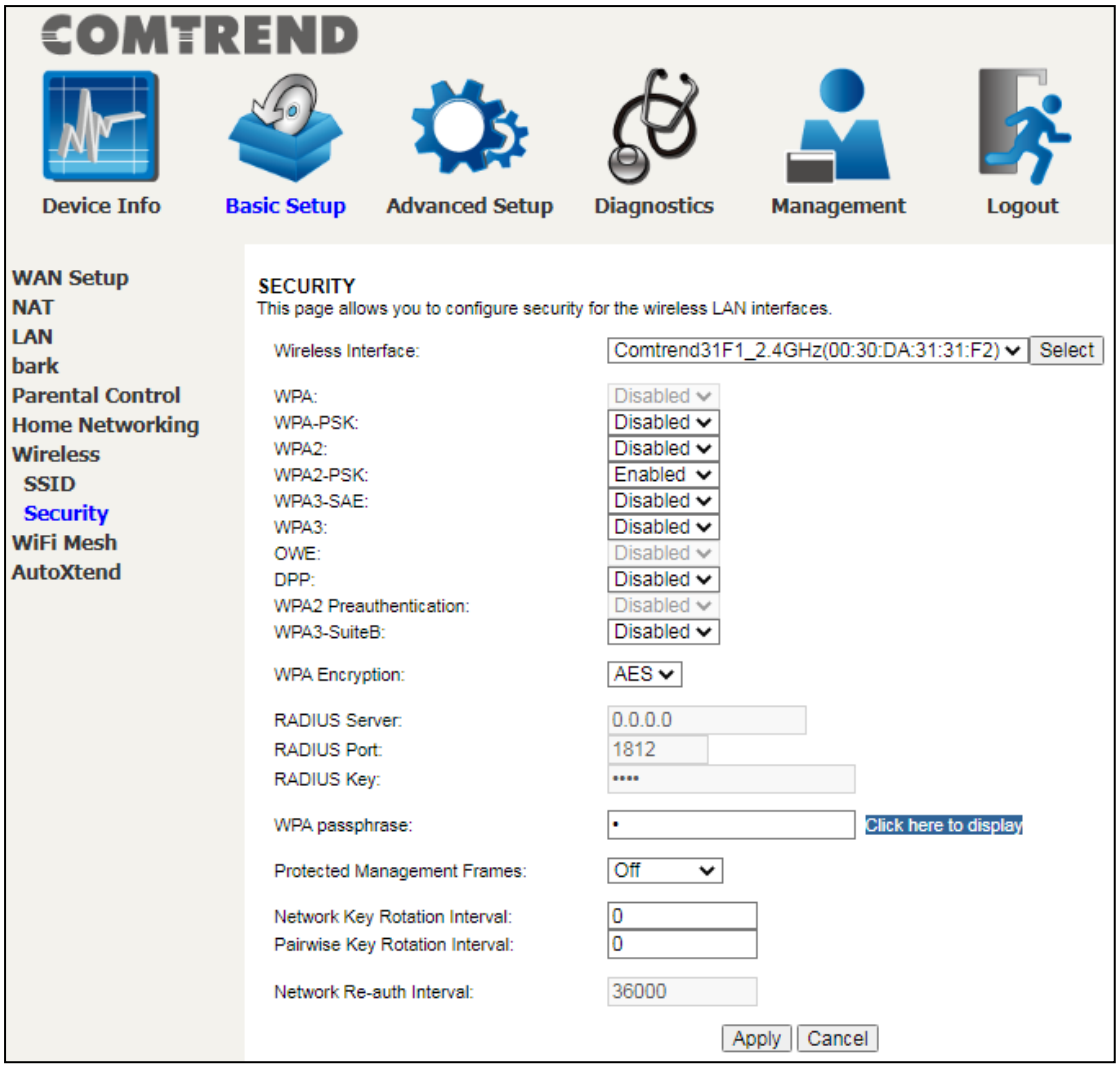
Click the **Apply** button to apply your changes. The settings shown above are described below.

Item	Description
Wireless Interface	Select which wireless interface to configure
BSS-MAC (SSID)	Select desired BSS to configure
BSS Enabled	Enable or disable this SSID
Network Name (SSID)	Sets the network name (also known as SSID) of this network
Network Type	Selecting **Closed** hides the network from active scans. Selecting **Open** reveals the network from active scans.
AP Isolation	Selecting **On** enables AP Isolation mode. When enabled, STAs associated with the AP will not be able to communicate with each other.
L2 Isolation	Wireless clients on the guest network cannot access hardwired LAN clients

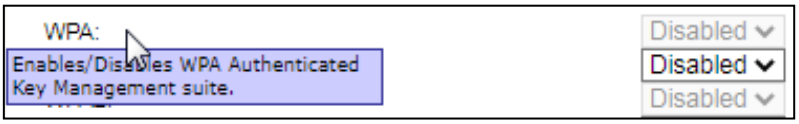
BSS Max Associations Limit	Sets the maximum associations for this BSS
WMM Advertise	When WMM is enabled for the radio, selecting **On** allows WMM to be advertised in beacons and probes for this BSS. **Off** disables advertisement of WMM in beacons and probes.
WMF	Choose **On** to enable Wireless Multicast Forwarding on this BSS. **Off** disables this feature.
MAC Address	Lists the MAC address of all the stations.
Association Time	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.
Signal Strength	Wi-Fi connection signal strength icon
Authorized	Lists those devices with authorized access
WMM Link	Lists those devices that utilize WMM
Power Save	Lists those devices that utilize the Power Save Feature
Spec	Wi-Fi Spec
BW	Bandwidth
Dwds	Lists the devices that utilize Dynamic WDS
Rssi	Received Signal Strength Indicator
DS Data Rate (Mbps)	Receive Rate
US Data Rate (Mbps)	Transmit Rate
Tx pkts	Shows total Tx packets
Tx bytes	Shows total Tx bytes
Rx pkts	Shows total Rx packets
Rx bytes	Shows total Rx bytes
Tx Failures	Shows total Tx packets failed

5.7.2 Security

This page allows you to configure security for the wireless LAN interfaces.



Click the **Apply** button to apply your changes. For information on each parameter, move the cursor over the parameter that you are interested in (as shown here).



Item	Description
Wireless Interface	Select which wireless interface to configure
WPA	Enable/disable WPA authenticated key management suite
WPA-PSK	Enable/disable WPA-PSK authenticated key management suite

WPA2	Enable/disable WPA2 authenticated key management suite
WPA2-PSK	Enable/disable WPA2-PSK authenticated key management suite
WPA3-SAE	Enable/disable WPA3-SAE authenticated key management suite
WPA3	Enable/disable WPA3 authenticated key management suite
OWE	Enable/disable OWE authenticated key management suite
DPP	Enable/disable DPP authenticated key management suite
WPA2 Preauthentication	Enable/disable WPA2 Preauthenticated key management suite
WPA3-SuiteB	Enable/disable WPA3-SuiteB key management suite
WPA Encryption	Select the WPA encryption algorithm
RADIUS Server	Set the IP of the RADIUS (Remote Authentication Dial In User Service) to use for authentication and dynamic key derivation
RADIUS Port	Set the UDP port number of the RADIUS server. The port number is usually 1812 or 1645 and depends upon the server.
RADIUS Key	Set the shared secret for the RADIUS connection
WPA passphrase	Set the WPA passphrase
Protected Management Frames	Wi-Fi CERTIFIED WPA2 with Protected Management Frames provides a WPA2-level of protection for unicast and multicast management action frames.
Network Key Rotation Interval	Set the Network Key Rotation interval in seconds. Leave blank or set to zero to disable the rotation.
Pairwise Key Rotation Interval	Set the Pairwise Key Rotation interval in seconds. Leave blank or set to zero to disable the rotation.

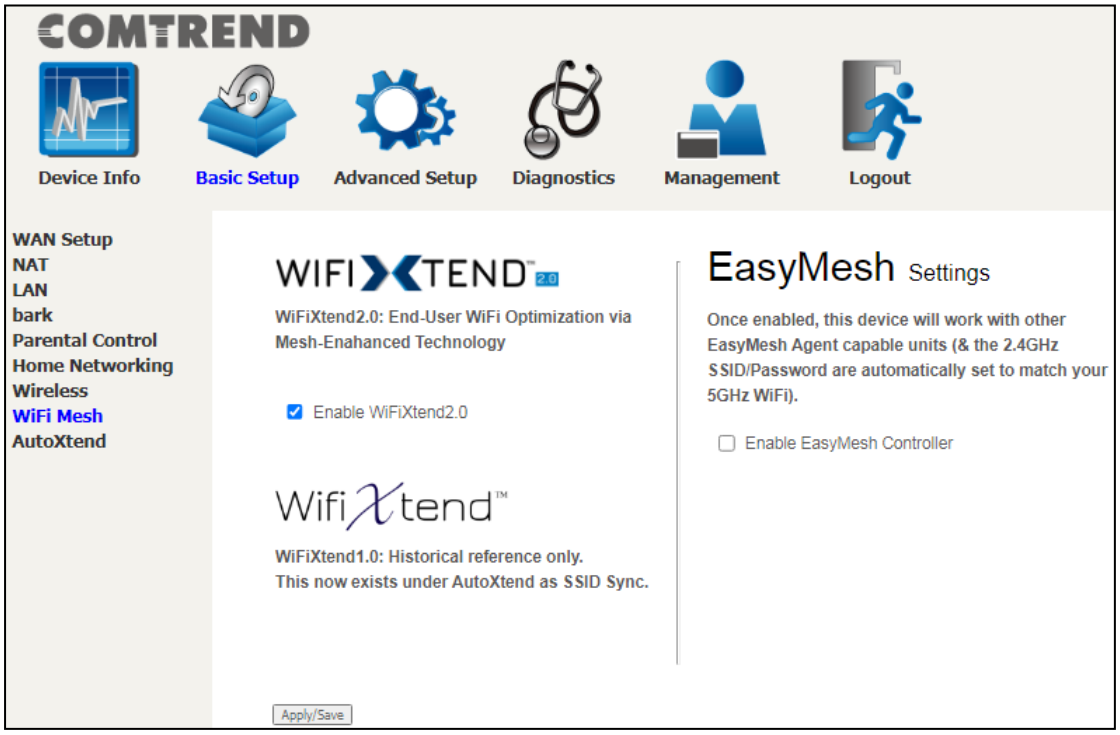
Network Re-auth Interval	Set the Network Key Re-authentication interval in seconds. Leave blank or set to zero to disable periodic network re-authentication.

5.8 WiFi Mesh

WiFiXtend
A Comtrend proprietary WiFi Mesh solution that makes the slave devices automatically synchronize, and makes slave devices choose the best uplink path in a covered network environment.

EasyMesh
The Wi-Fi EasyMesh defines the control protocols between APs, mechanisms to route traffic within the network, and the data objects necessary to enable easy onboarding, provisioning, control, and automated management of APs in a Wi-Fi EasyMesh network.

Wi-Fi EasyMesh networks use a controller to manage the network, with agent APs connected to it.



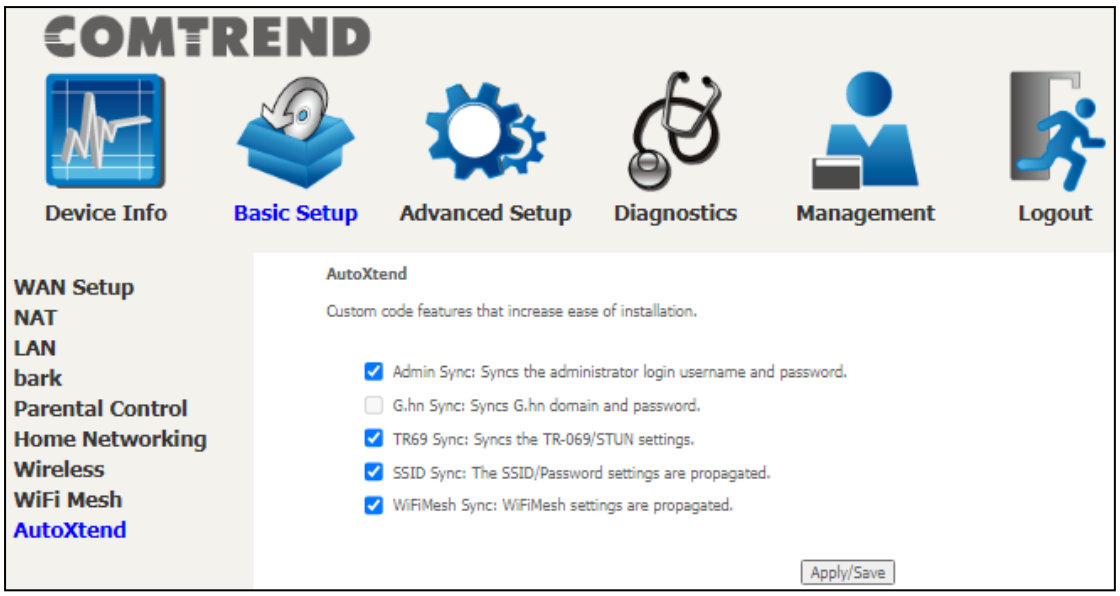
Once you have decided to use **WifiXtend** or **EasyMesh** follow the instructions below.

Check the checkbox and click the **Apply/Save** button to enable **WifiXtend.**

To enable **EasyMesh**, check the checkbox and click the **Apply/Save** button. Once enabled, this device will work with other EasyMesh Agent capable units (& the 2.4GHz SSID/Password are automatically set to match your 5GHz WiFi).

5.9 AutoXtend

AutoXtend is a function to construct and optimize a mesh-network. To select information to synchronize with all mesh-network nodes, please check the desired item and click the **Apply/Save** button.



To enable the AutoXtend features, check the required checkboxes and click the **Apply/Save** button.

Chapter 6 Advanced Setup

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

6.1 Security

For detailed descriptions, with examples, please consult Appendix A - Firewall.

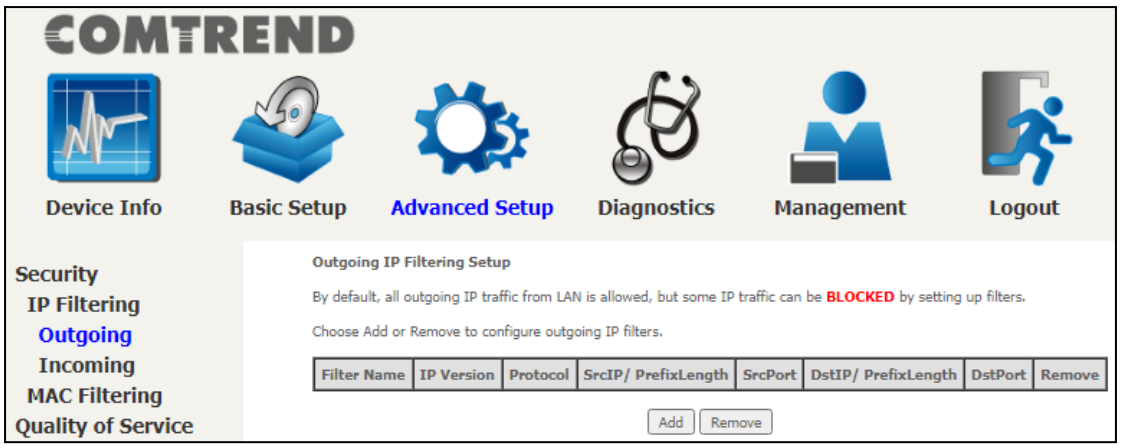
6.1.1 IP Filtering

This screen sets filter rules that limit IP traffic (Outgoing/Incoming). Multiple filter rules can be set and each applies at least one limiting condition. For individual IP packets to pass the filter all conditions must be fulfilled.

NOTE:	This function is not available when in WDS mode. Instead, MAC Filtering performs a similar function.

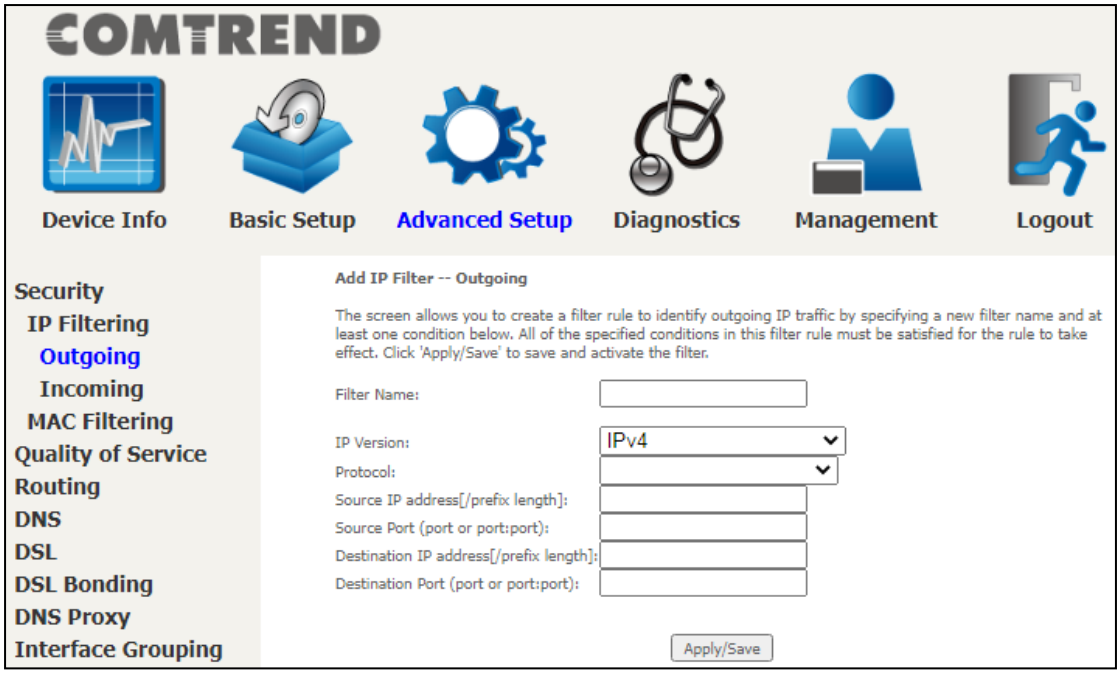
OUTGOING IP FILTER

By default, all outgoing IP traffic is allowed, but IP traffic can be blocked with filters.



To add a filter (to block some outgoing IP traffic), click the **Add** button.

On the following screen, enter your filter criteria and then click **Apply/Save**.



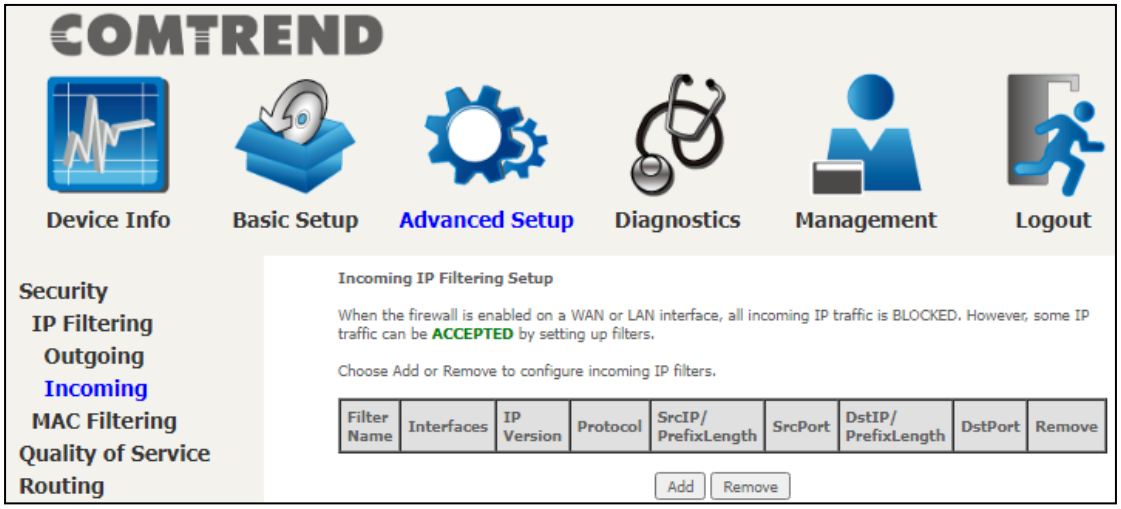
Click the **Apply/Save** button to apply and save your changes.

Consult the table below for item descriptions.

Item	Description
Filter Name	The filter rule label (user defined)
IP Version	Select from the drop down menu
Protocol	Set the traffic type (TCP, TCP/UDP, UDP, or ICMP) that the rule will apply to
Source IP address	Enter source IP address for the IP filter
Source Port (port or port:port)	Enter source port number or range for the IP filter
Destination IP address	Enter destination IP address for the IP filter
Destination Port (port or port:port)	Enter destination port number or range for the IP filter

INCOMING IP FILTER

By default, all incoming IP traffic is blocked, but IP traffic can be allowed with filters.



To add a filter (to allow incoming IP traffic), click the **Add** button.

On the following screen, enter your filter criteria and then click **Apply/Save**.

Consult the table below for item descriptions.

Item	Description
Filter Name	The filter rule label (user defined)
IP Version	Select from the drop down menu
Protocol	Set the traffic type (TCP, TCP/UDP, UDP, or ICMP) that the rule will apply to
Source IP address	Enter source IP address for the IP filter
Source Port (port or port:port)	Enter source port number or range for the IP filter
Destination IP address	Enter destination IP address for the IP filter
Destination Port (port or port:port)	Enter destination port number or range for the IP filter

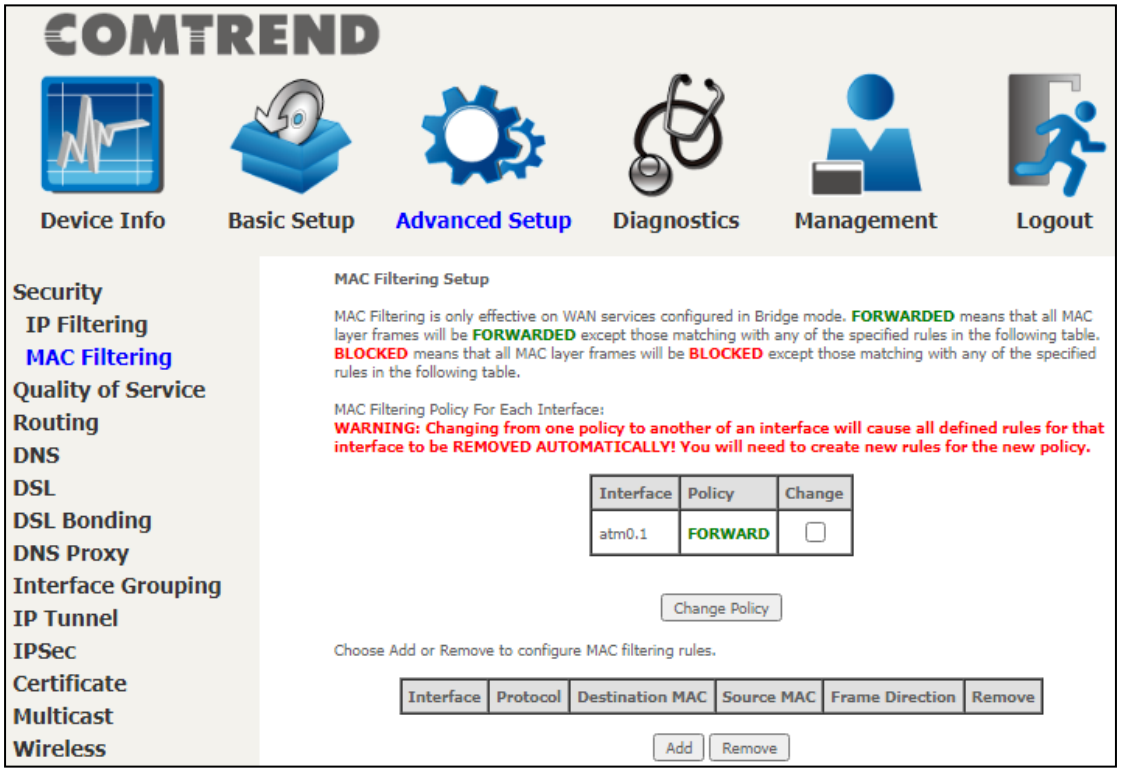
At the bottom of this screen, select the WAN and LAN Interfaces to which the filter rule will apply. You may select all or just a subset. WAN interfaces in WDS mode or without firewall enabled are not available.

6.1.2 MAC Filtering

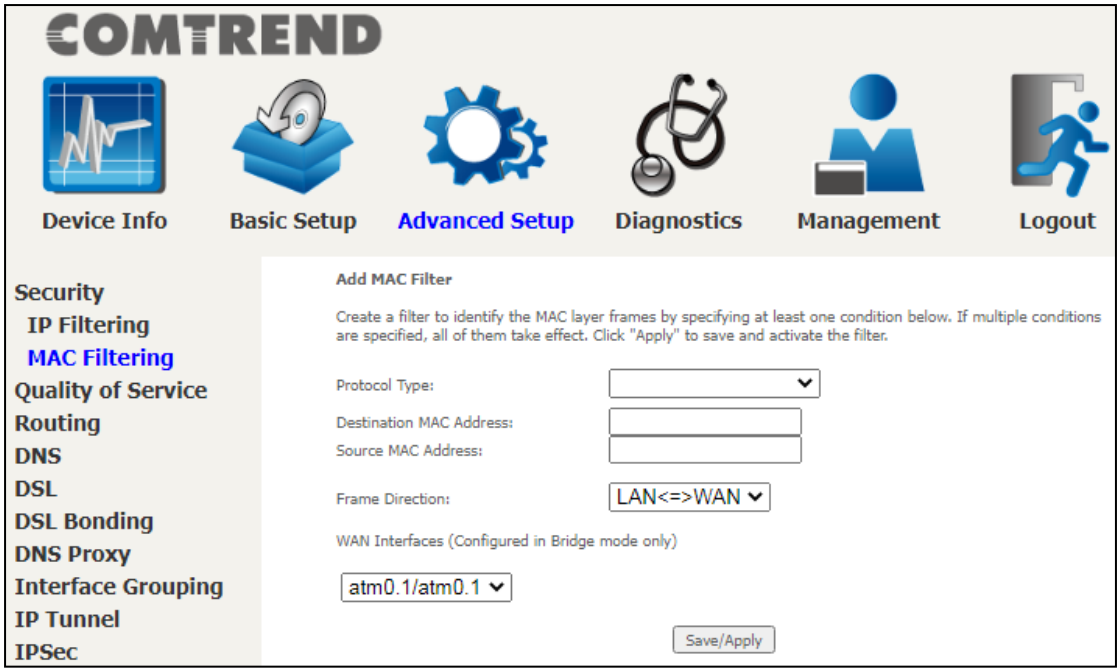
NOTE:	This option is only available in WDS mode. Other modes use IP Filtering to perform a similar function.

Each network device has a unique 48-bit MAC address. This can be used to filter (block or forward) packets based on the originating device. MAC filtering policy and rules for the PRT-6302 can be set according to the following procedure.

The MAC Filtering Global Policy is defined as follows. **FORWARDED** means that all MAC layer frames will be **FORWARDED** except those matching the MAC filter rules. **BLOCKED** means that all MAC layer frames will be **BLOCKED** except those matching the MAC filter rules. The default MAC Filtering Global policy is **FORWARDED**. It can be changed by clicking the **Change Policy** button.



Choose **Add** or **Remove** to configure MAC filtering rules. The following screen will appear when you click **Add**. Create a filter to identify the MAC layer frames by specifying at least one condition below. If multiple conditions are specified, all of them must be met.



Click **Save/Apply** to save and activate the filter rule.

Consult the table below for detailed item descriptions.

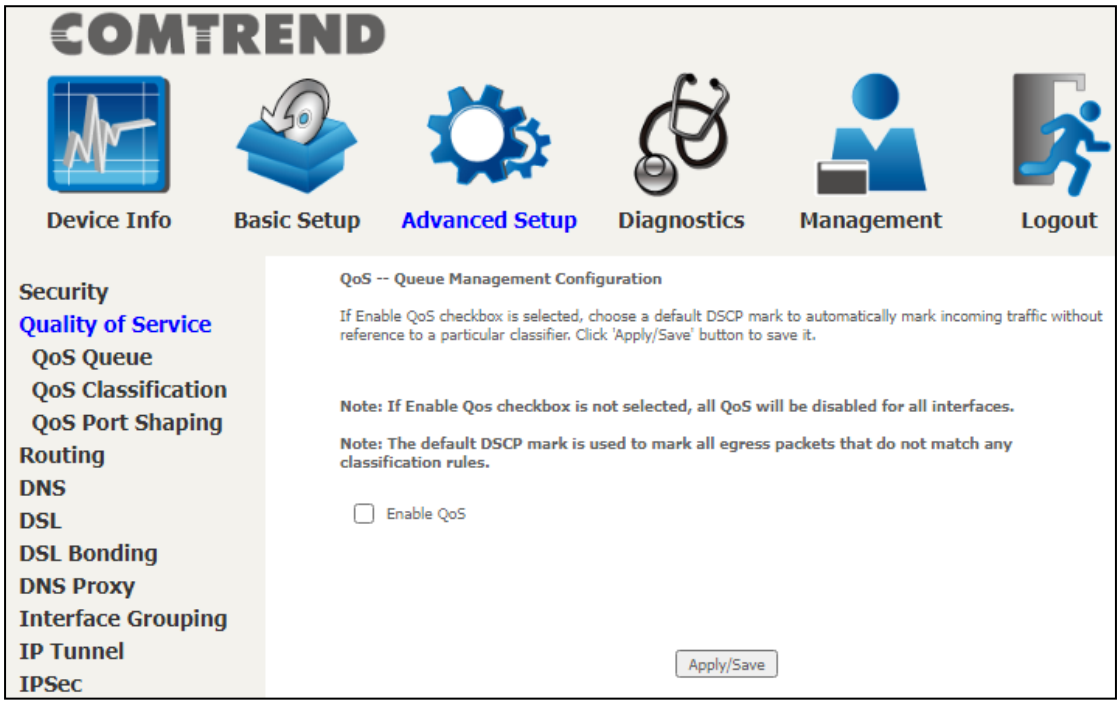
Item	Description
Protocol Type	Select from the drop down menu the protocol (PPPoE, IPv4, IPv6, AppleTalk, IPX, NetBEUI, IGMP) that will apply to this rule.
Destination MAC Address	Defines the destination MAC address
Source MAC Address	Defines the source MAC address
Frame Direction	Select the incoming/outgoing packet interface
WAN Interfaces	Applies the filter to the selected bridge interface

6.2 Quality of Service (QoS)

NOTE: QoS must be enabled in at least one PVC to display this option.
(See Appendix F - Connection Setup for detailed PVC setup instructions).

To Enable QoS tick the checkbox ☑ and select a Default DSCP Mark.

Click **Apply/Save** to activate QoS.



QoS and DSCP Mark are defined as follows:

Quality of Service (QoS): This provides different priority to different users or data flows, or guarantees a certain level of performance to a data flow in accordance with requests from Queue Prioritization.

Default Differentiated Services Code Point (DSCP) Mark: This specifies the per hop behavior for a given flow of packets in the Internet Protocol (IP) header that do not match any other QoS rule.

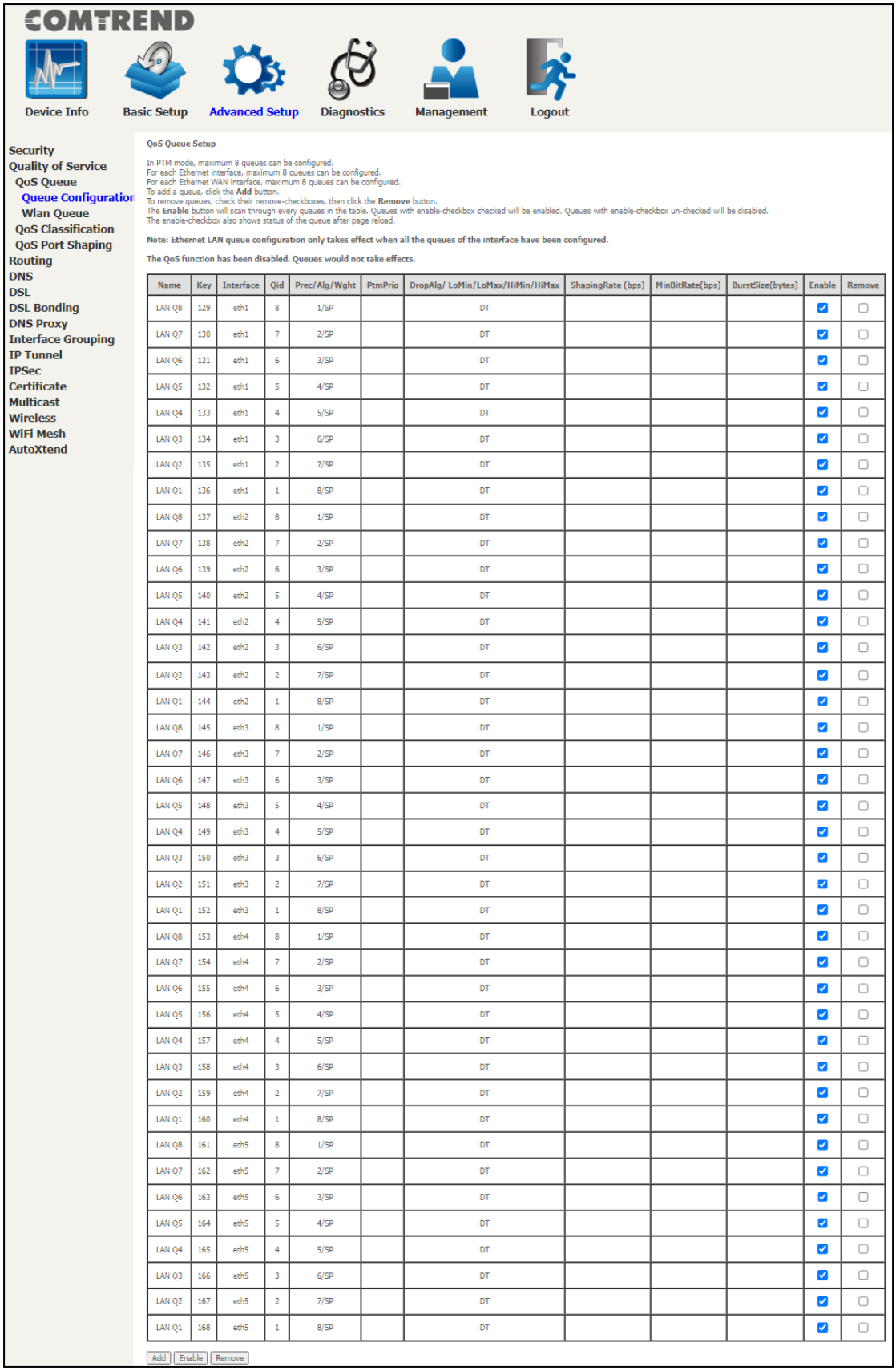
6.2.1 QoS Queue

6.2.1.1 QoS Queue Configuration

Configure queues with different priorities to be used for QoS setup.

In ATM mode, a maximum of 16 queues can be configured.
In PTM mode, a maximum of 8 queues can be configured.
For each Ethernet interface, a maximum of 8 queues can be configured.
For each Ethernet WAN interface, a maximum of 8 queues can be configured.

(Please see the screen on the following page).



Name	Key	Interface	Qid	Prec/Alg/Wght	PtmPrio	DropAlg/ LoMin/LoMax/HiMin/HiMax	ShapingRate (bps)	MinBitRate(bps)	BurstSize(bytes)	Enable	Remove
LAN Q8	129	eth1	8	1/SP		DT				☑	☐
LAN Q7	130	eth1	7	2/SP		DT				☑	☐
LAN Q6	131	eth1	6	3/SP		DT				☑	☐
LAN Q5	132	eth1	5	4/SP		DT				☑	☐
LAN Q4	133	eth1	4	5/SP		DT				☑	☐
LAN Q3	134	eth1	3	6/SP		DT				☑	☐
LAN Q2	135	eth1	2	7/SP		DT				☑	☐
LAN Q1	136	eth1	1	8/SP		DT				☑	☐
LAN Q8	137	eth2	8	1/SP		DT				☑	☐
LAN Q7	138	eth2	7	2/SP		DT				☑	☐
LAN Q6	139	eth2	6	3/SP		DT				☑	☐
LAN Q5	140	eth2	5	4/SP		DT				☑	☐
LAN Q4	141	eth2	4	5/SP		DT				☑	☐
LAN Q3	142	eth2	3	6/SP		DT				☑	☐
LAN Q2	143	eth2	2	7/SP		DT				☑	☐
LAN Q1	144	eth2	1	8/SP		DT				☑	☐
LAN Q8	145	eth3	8	1/SP		DT				☑	☐
LAN Q7	146	eth3	7	2/SP		DT				☑	☐
LAN Q6	147	eth3	6	3/SP		DT				☑	☐
LAN Q5	148	eth3	5	4/SP		DT				☑	☐
LAN Q4	149	eth3	4	5/SP		DT				☑	☐
LAN Q3	150	eth3	3	6/SP		DT				☑	☐
LAN Q2	151	eth3	2	7/SP		DT				☑	☐
LAN Q1	152	eth3	1	8/SP		DT				☑	☐
LAN Q8	153	eth4	8	1/SP		DT				☑	☐
LAN Q7	154	eth4	7	2/SP		DT				☑	☐
LAN Q6	155	eth4	6	3/SP		DT				☑	☐
LAN Q5	156	eth4	5	4/SP		DT				☑	☐
LAN Q4	157	eth4	4	5/SP		DT				☑	☐
LAN Q3	158	eth4	3	6/SP		DT				☑	☐
LAN Q2	159	eth4	2	7/SP		DT				☑	☐
LAN Q1	160	eth4	1	8/SP		DT				☑	☐
LAN Q8	161	eth5	8	1/SP		DT				☑	☐
LAN Q7	162	eth5	7	2/SP		DT				☑	☐
LAN Q6	163	eth5	6	3/SP		DT				☑	☐
LAN Q5	164	eth5	5	4/SP		DT				☑	☐
LAN Q4	165	eth5	4	5/SP		DT				☑	☐
LAN Q3	166	eth5	3	6/SP		DT				☑	☐
LAN Q2	167	eth5	2	7/SP		DT				☑	☐
LAN Q1	168	eth5	1	8/SP		DT				☑	☐

To remove queues, check their remove-checkboxes (for user created queues), then click the **Remove** button.

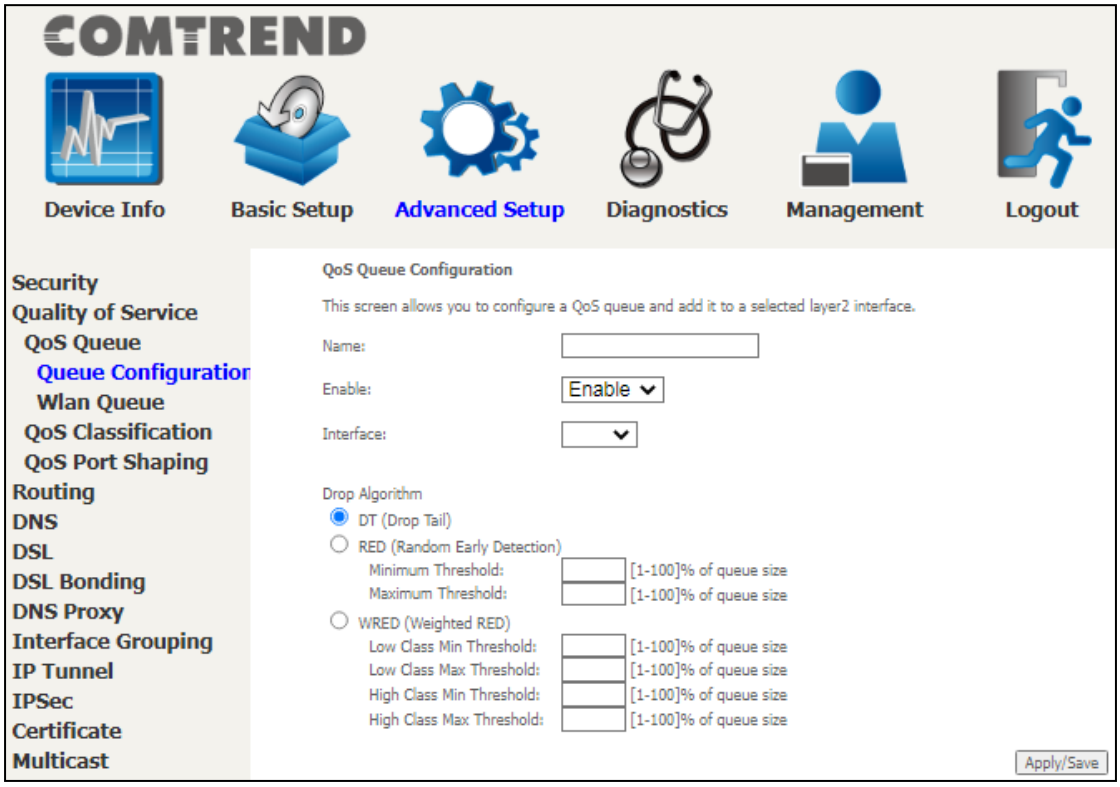
The **Enable** button will scan through every queue in the table. Queues with the enable-checkbox checked will be enabled. Queues with the enable-checkbox un-checked will be disabled.

The enable-checkbox also shows status of the queue after page reload.

Note that if WMM function is disabled in the Wireless Page, queues related to wireless will not take effect. This function follows the Differentiated Services rule of IP QoS.

Enable and assign an interface and precedence on the next screen. Click **Apply/Save** on this screen to activate it.

To add a queue, click the **Add** button to display the following screen.



Name: Identifier for this Queue entry.

Enable: Enable/Disable the Queue entry.

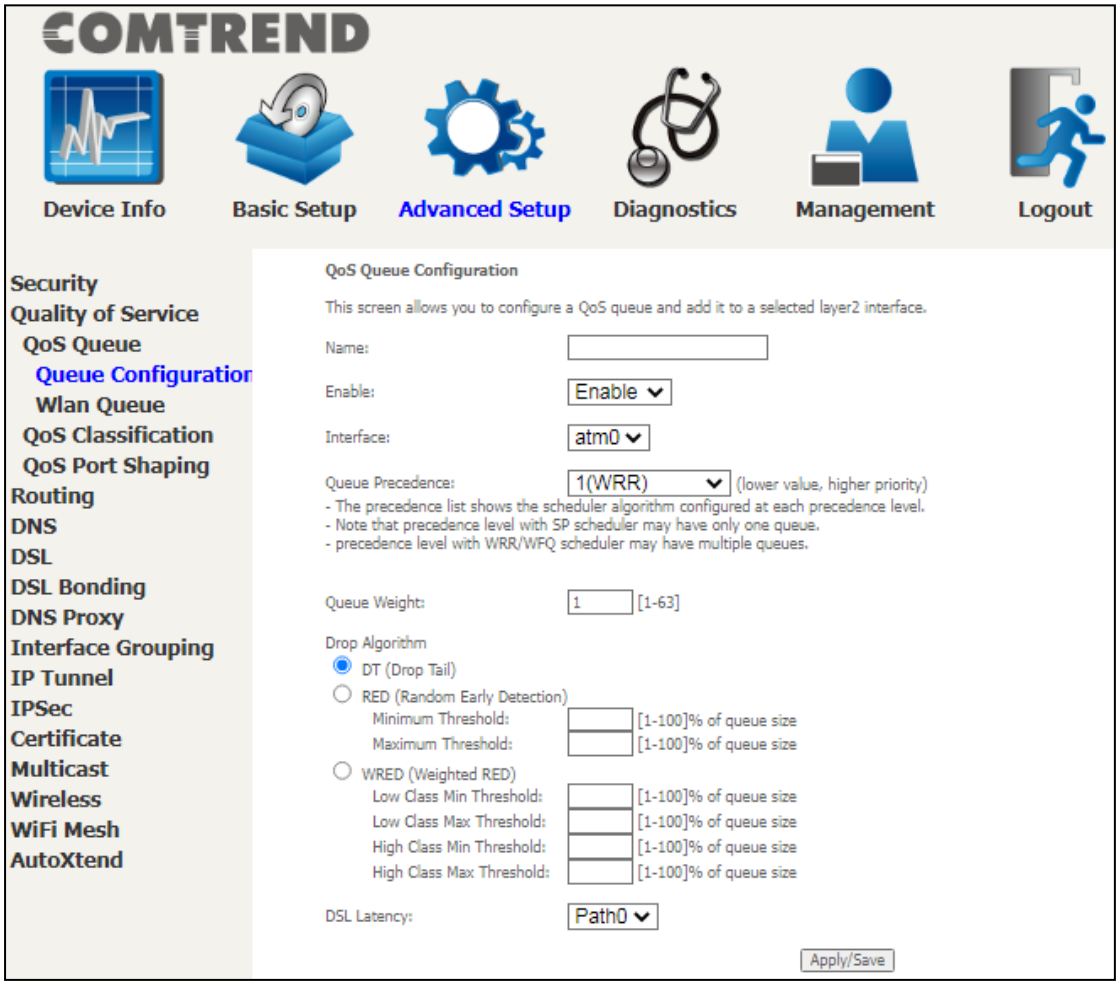
Interface: Assign the entry to a specific network interface (QoS enabled).

Drop Algorithm: Select the algorithm to be used to ensure that the QoS rule is enforced if the traffic exceeds the configured limit.

Drop Tail: Packets are sent in first come first serve fashion, the tailing traffic would be dropped if they exceed the handling limit.

Random Early Detection: Packets are monitored by configured queue threshold and serving proportion.

WRED: Weighted RED, the assigned monitoring queue would be given different priority and threshold to ensure various priority queues would be served fairly. After selecting an Interface the following will be displayed.



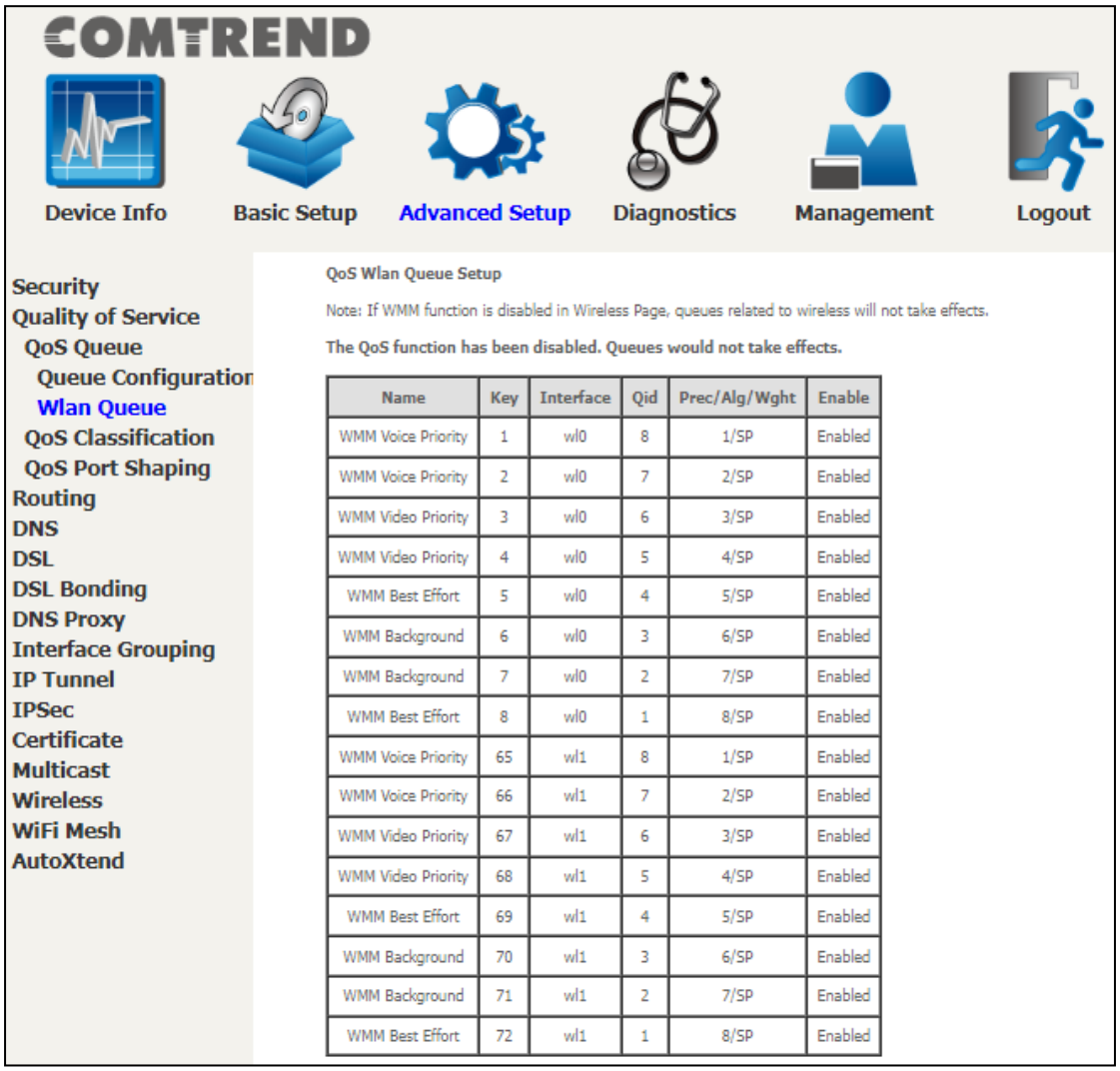
The precedence list shows the scheduler algorithm for each precedence level. Queues of equal precedence will be scheduled based on the algorithm. Queues of unequal precedence will be scheduled based on SP.

Shaping Rate: Specify a shaping rate limit to the defined queue.

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

6.2.1.2 Wlan Queue

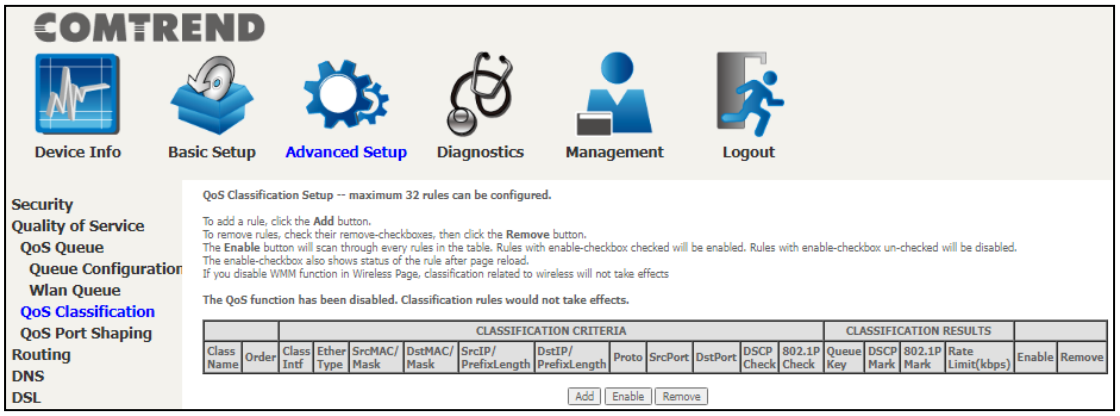
Displays the list of available wireless queues for WMM and wireless data transmit priority.



Name	Key	Interface	Qid	Prec/Alg/Wght	Enable
WMM Voice Priority	1	wl0	8	1/SP	Enabled
WMM Voice Priority	2	wl0	7	2/SP	Enabled
WMM Video Priority	3	wl0	6	3/SP	Enabled
WMM Video Priority	4	wl0	5	4/SP	Enabled
WMM Best Effort	5	wl0	4	5/SP	Enabled
WMM Background	6	wl0	3	6/SP	Enabled
WMM Background	7	wl0	2	7/SP	Enabled
WMM Best Effort	8	wl0	1	8/SP	Enabled
WMM Voice Priority	65	wl1	8	1/SP	Enabled
WMM Voice Priority	66	wl1	7	2/SP	Enabled
WMM Video Priority	67	wl1	6	3/SP	Enabled
WMM Video Priority	68	wl1	5	4/SP	Enabled
WMM Best Effort	69	wl1	4	5/SP	Enabled
WMM Background	70	wl1	3	6/SP	Enabled
WMM Background	71	wl1	2	7/SP	Enabled
WMM Best Effort	72	wl1	1	8/SP	Enabled

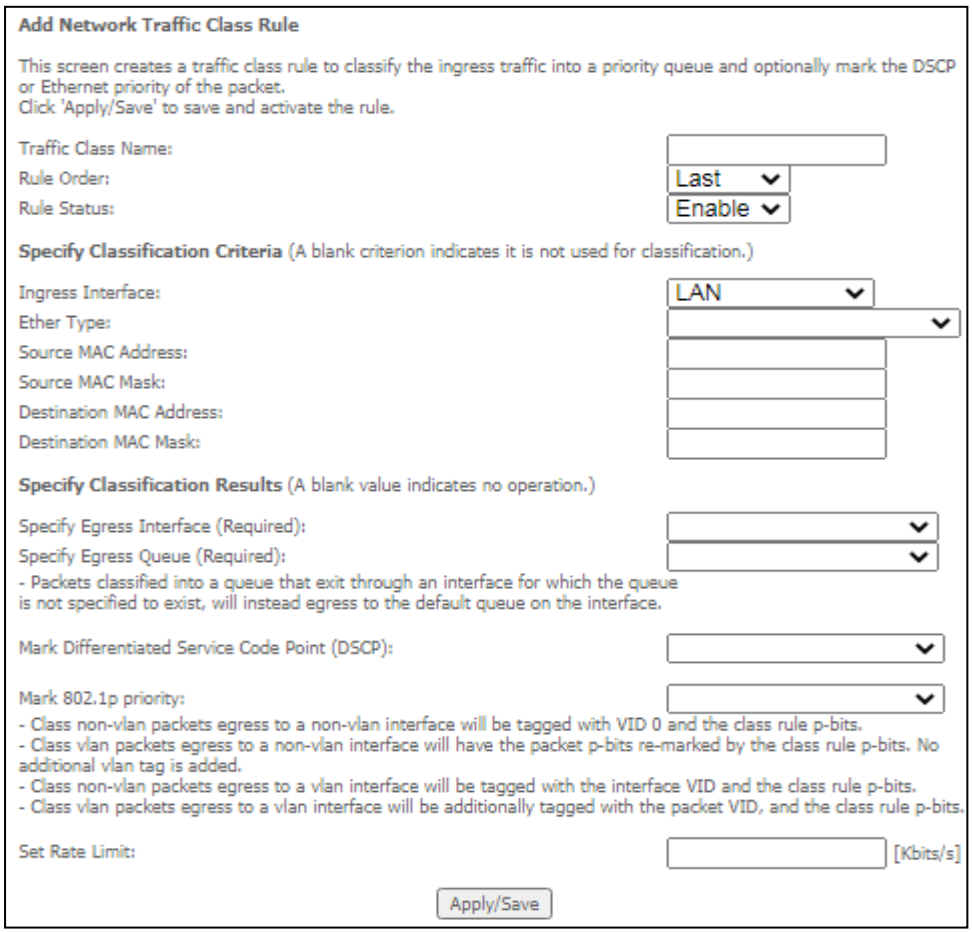
6.2.2 QoS Classification

The network traffic classes are listed in the following table.



Click **Add** to configure a network traffic class rule and **Enable** to activate it. To delete an entry from the list, click **Remove**.

This screen creates a traffic class rule to classify the upstream traffic, assign queuing priority and optionally overwrite the IP header DSCP byte. A rule consists of a class name and at least one logical condition. All the conditions specified in the rule must be satisfied for it to take effect.



Click **Apply/Save** to save and activate the rule.

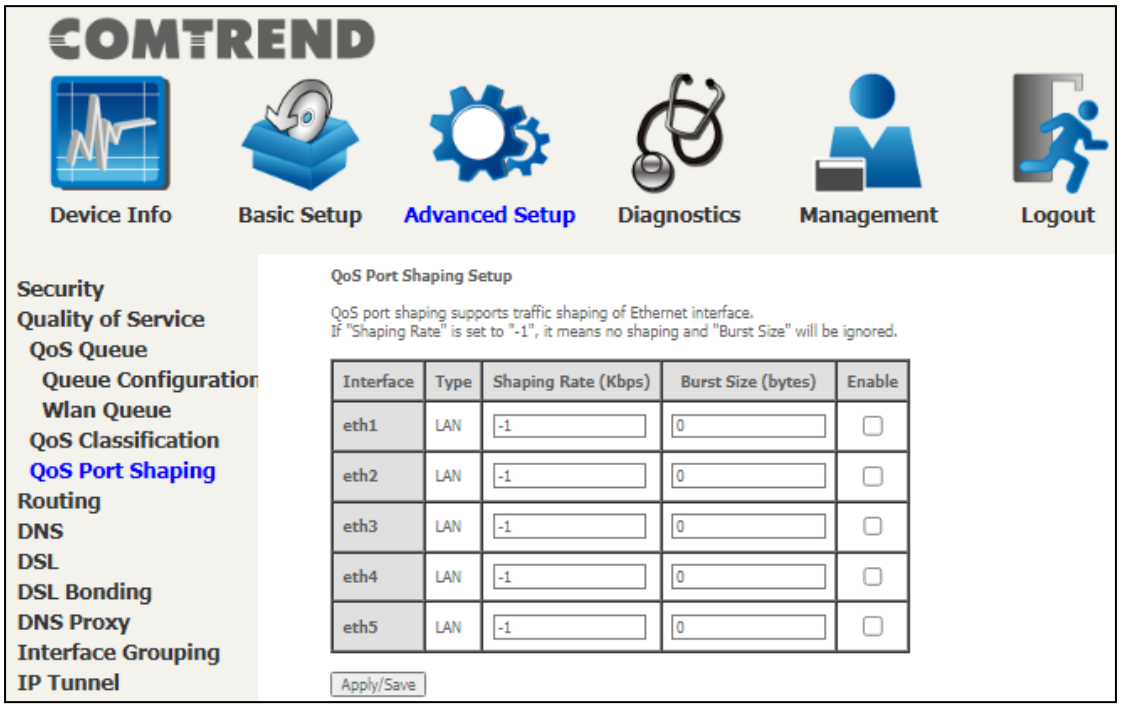
Consult the table below for detailed item descriptions.

Item	Description
Traffic Class Name	Enter a name for the traffic class.
Rule Order	Last is the only option.
Rule Status	Disable or enable the rule.
Classification Criteria	
Ingress Interface	Select an interface: (i.e. LAN, WAN, local, ETH1, ETH2, ETH3, wl0)
Ether Type	Set the Ethernet type (e.g. IP, ARP, IPv6).
Source MAC Address	A packet belongs to SET-1, if a binary-AND of its source MAC address with the Source MAC Mask is equal to the binary-AND of the Source MAC Mask and this field.
Source MAC Mask	This is the mask used to decide how many bits are checked in Source MAC Address.
Destination MAC Address	A packet belongs to SET-1 then the result that the Destination MAC Address of its header binary-AND to the Destination MAC Mask must equal to the result that this field binary-AND to the Destination MAC Mask.
Destination MAC Mask	This is the mask used to decide how many bits are checked in the Destination MAC Address.
Classification Results	
Specify Egress Interface	Choose the egress interface from the available list.
Specify Egress Queue	Choose the egress queue from the list of available for the specified egress interface.
Mark Differentiated Service Code Point	The selected Code Point gives the corresponding priority to packets that satisfy the rule.
Mark 802.1p Priority	Select between 0-7. - Class non-vlan packets egress to a non-vlan interface will be tagged with VID 0 and the class rule p-bits.

	- Class vlan packets egress to a non-vlan interface will have the packet p-bits re-marked by the class rule p-bits. No additional vlan tag is added. - Class non-vlan packets egress to a vlan interface will be tagged with the interface VID and the class rule p-bits. - Class vlan packets egress to a vlan interface will be additionally tagged with the packet VID, and the class rule p-bits.
Set Rate Limit	The data transmission rate limit in kbps.

6.2.3 QoS Port Shaping

QoS port shaping supports traffic shaping of the Ethernet interface.
Input the shaping rate and burst size to enforce QoS rule on each interface.
If "Shaping Rate" is set to "-1", it means no shaping and "Burst Size" will be ignored.



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

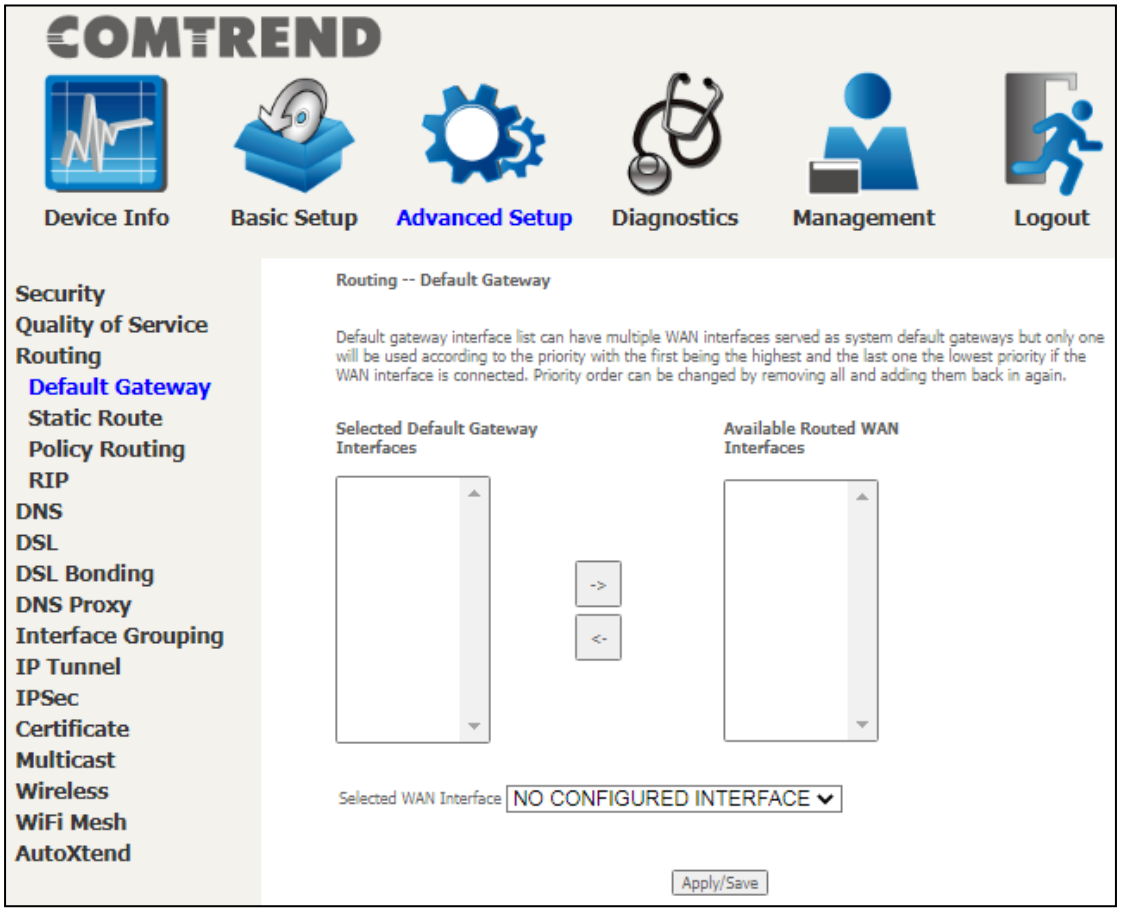
6.3 Routing

The following routing functions are accessed from this menu:
Default Gateway, Static Route, Policy Routing and **RIP**.

NOTE:	In WDS mode, the **RIP** menu option is hidden while the other menu options are shown but ineffective.

6.3.1 Default Gateway

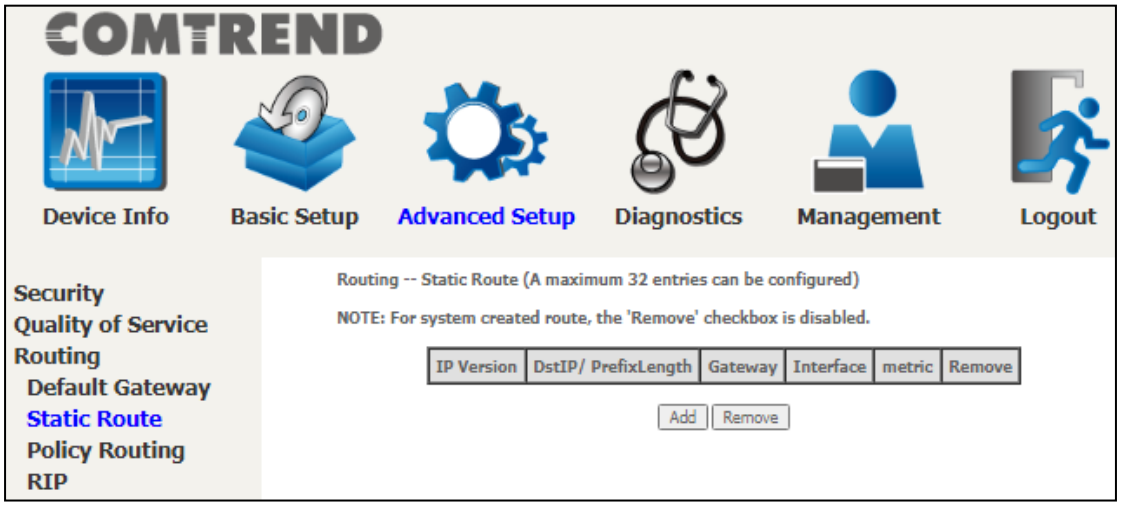
The default gateway interface list can have multiple WAN interfaces served as system default gateways but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.



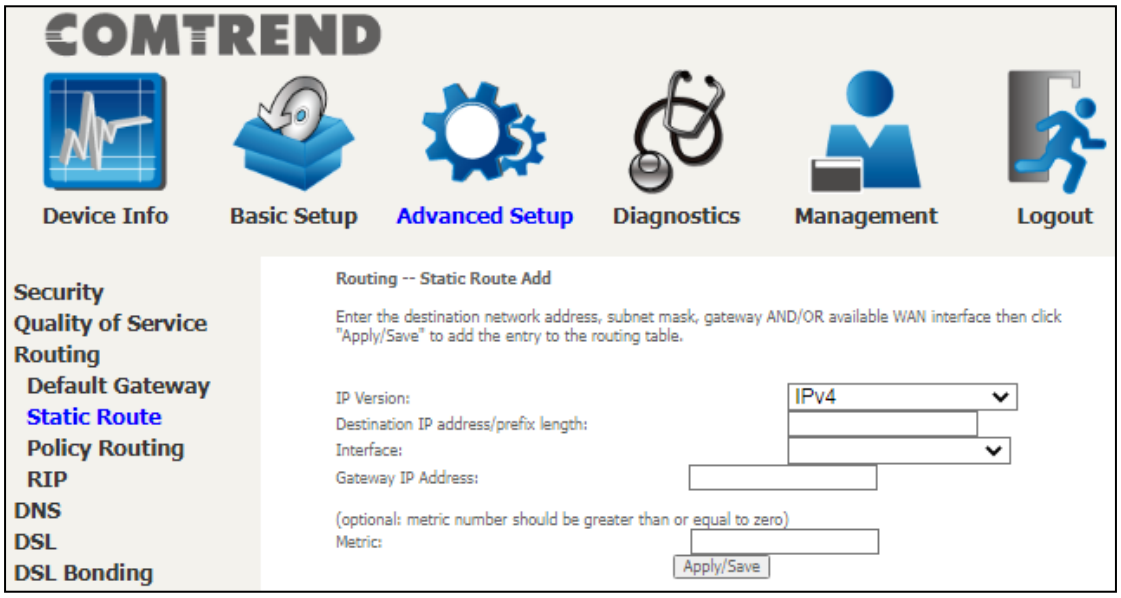
Click **Apply/Save** to apply and save the settings.

6.3.2 Static Route

This option allows for the configuration of static routes by destination IP.
Click **Add** to create a static route or click **Remove** to delete a static route.



After clicking **Add** the following will display.



- **IP Version:** Select the IP version to be IPv4 or IPv6.
- **Destination IP address/prefix length:** Enter the destination IP address.
- **Interface:** Select the proper interface for the rule.
- **Gateway IP Address:** The next-hop IP address.
- **Metric:** The metric value of routing.

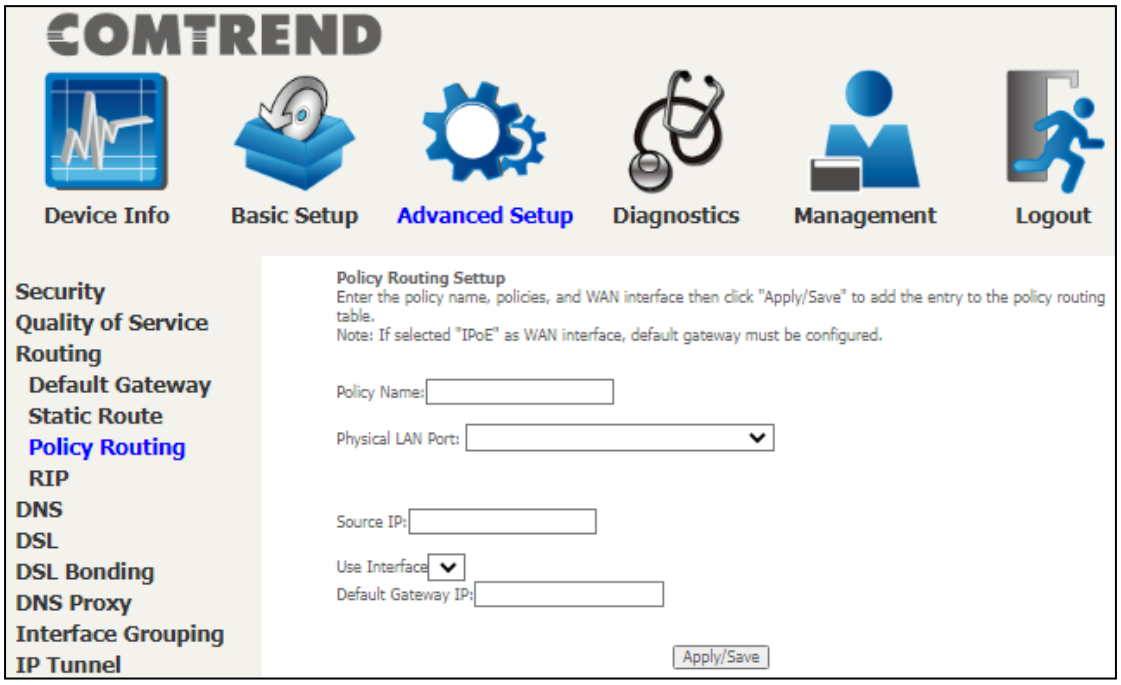
After completing the settings, click **Apply/Save** to add the entry to the routing table.

6.3.3 Policy Routing

This option allows for the configuration of static routes by policy.

Click **Add** to create a routing policy or **Remove** to delete one.

On the following screen, complete the form and click **Apply**/**Save** to create a policy.

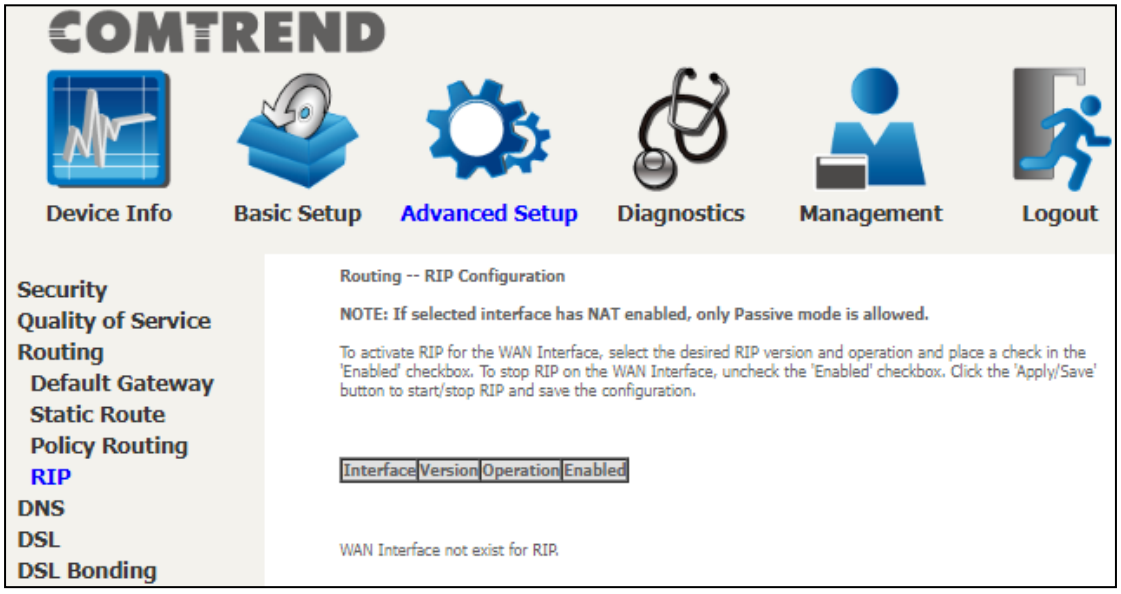


Consult the table below for detailed item descriptions.

Item	Description
Policy Name	Name of the route policy
Physical LAN Port	Specify the port to use this route policy
Source IP	IP Address to be routed
Use Interface	Interface that traffic will be directed to
Default Gateway IP	IP Address of the default gateway

6.3.4 RIP

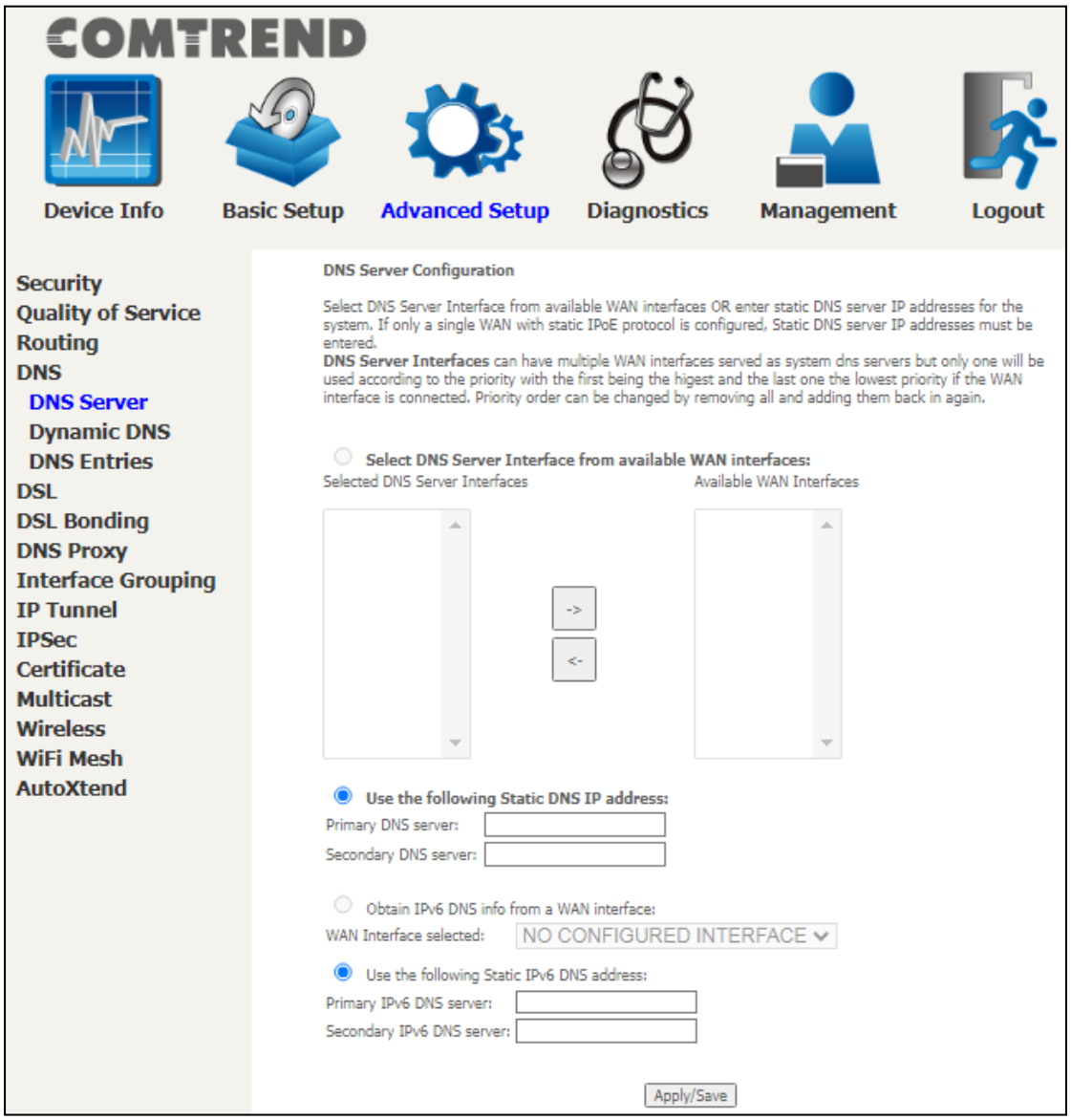
To activate RIP, configure the RIP version/operation mode and select the **Enabled** checkbox ☑ for at least one WAN interface before clicking **Apply/Save**.



6.4 DNS

6.4.1 DNS Server

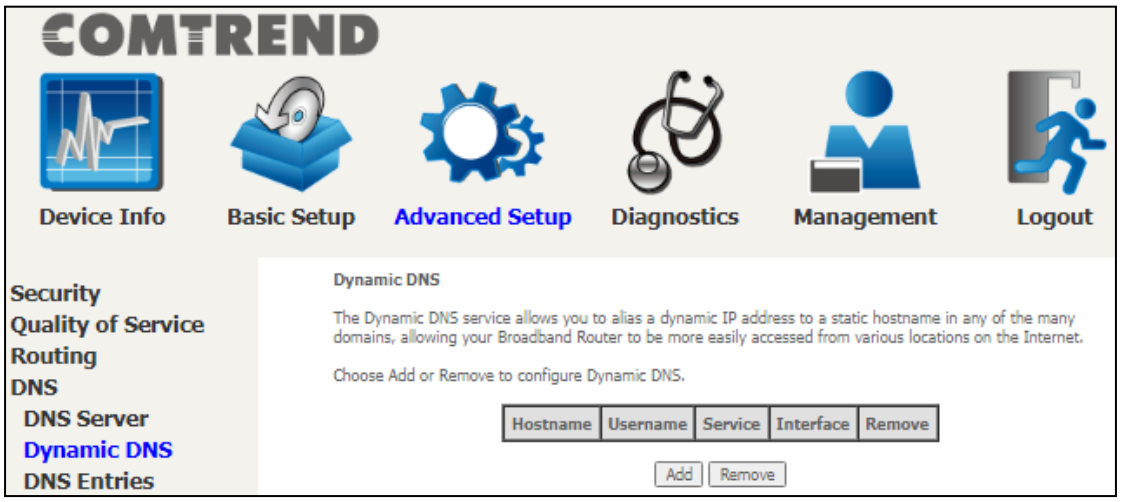
Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered. **DNS Server Interfaces** can have multiple WAN interfaces served as system DNS servers but only one will be used according to the priority with the first being the highest and the last one the lowest priority if the WAN interface is connected. Priority order can be changed by removing all and adding them back in again.



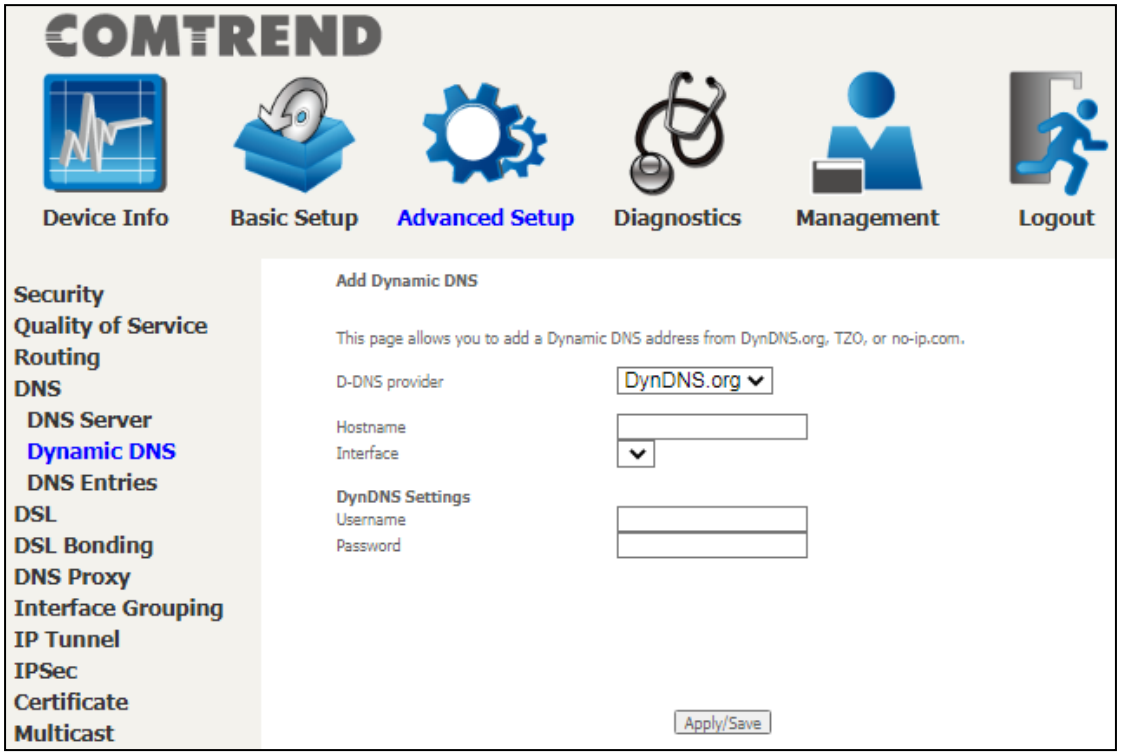
Click **Apply/Save** to save the new configuration.

6.4.2 Dynamic DNS

The Dynamic DNS service allows you to map a dynamic IP address to a static hostname in any of many domains, allowing the PRT-6302 to be more easily accessed from various locations on the Internet.



To add a dynamic DNS service, click **Add**. The following screen will display.



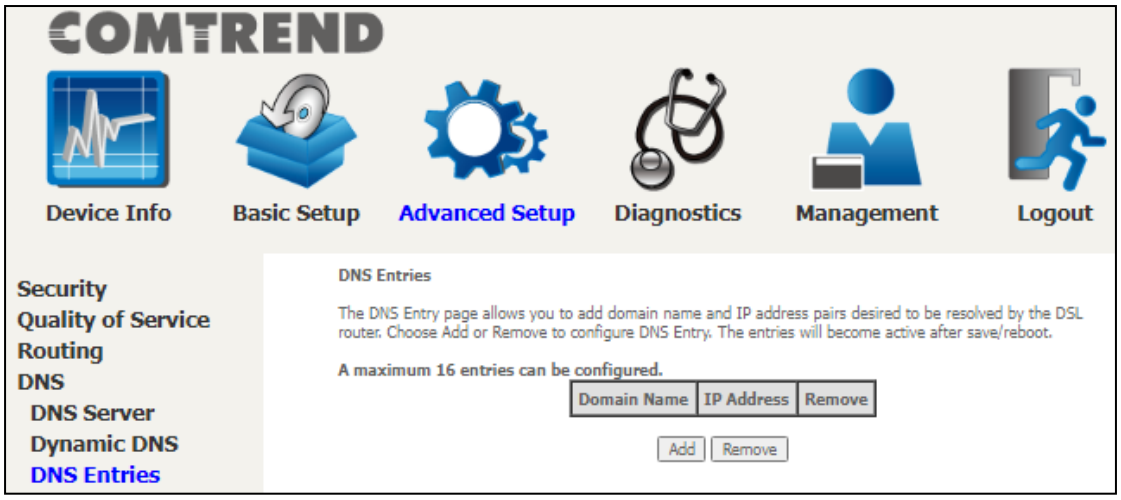
Click **Apply/Save** to save your settings.

Consult the table below for item descriptions.

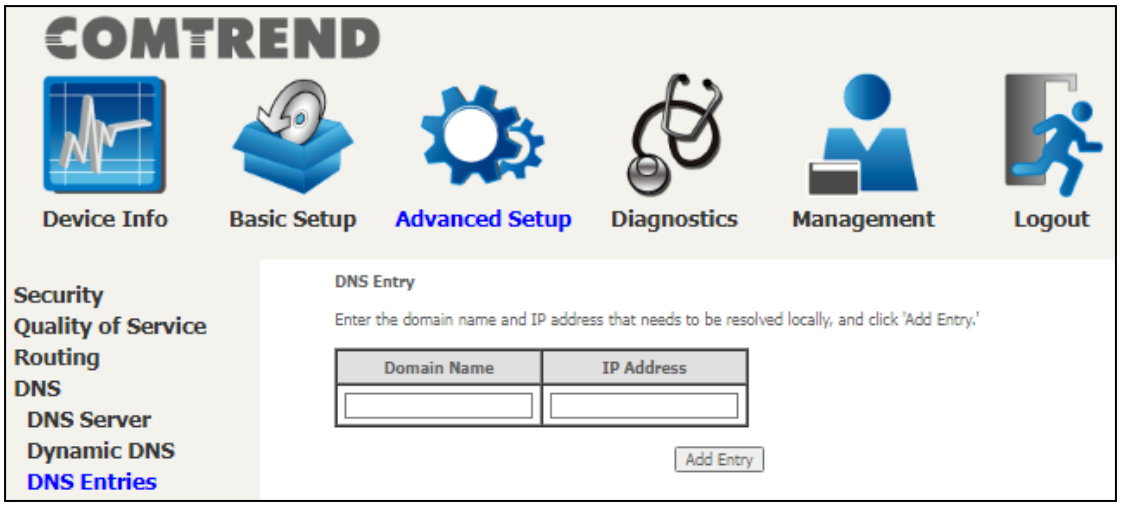
Item	Description
D-DNS provider	Select a dynamic DNS provider from the list
Hostname	Enter the name of the dynamic DNS server
Interface	Select the interface from the list
Username	Enter the username of the dynamic DNS server
Password	Enter the password of the dynamic DNS server

6.4.3 DNS Entries

The DNS Entry page allows you to add domain name and IP address pairs desired to be resolved by the DSL router.



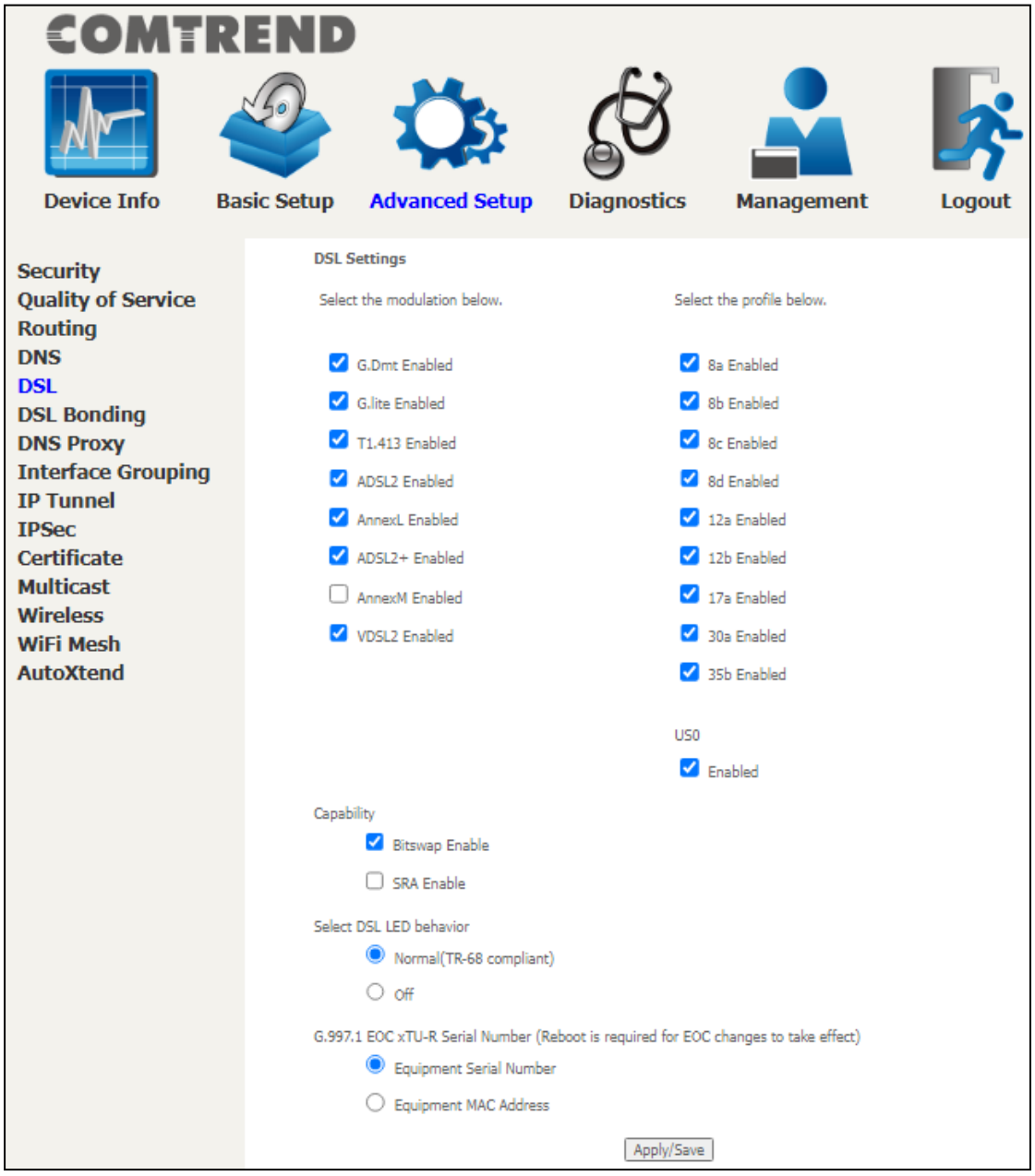
Choose Add or Remove to configure a DNS Entry. The entries will become active after save/reboot.



Enter the domain name and IP address that needs to be resolved locally, and click the **Add Entry** button.

6.5 DSL

The DSL Settings screen allows for the selection of DSL modulation modes.
For optimum performance, the modes selected should match those of your ISP.



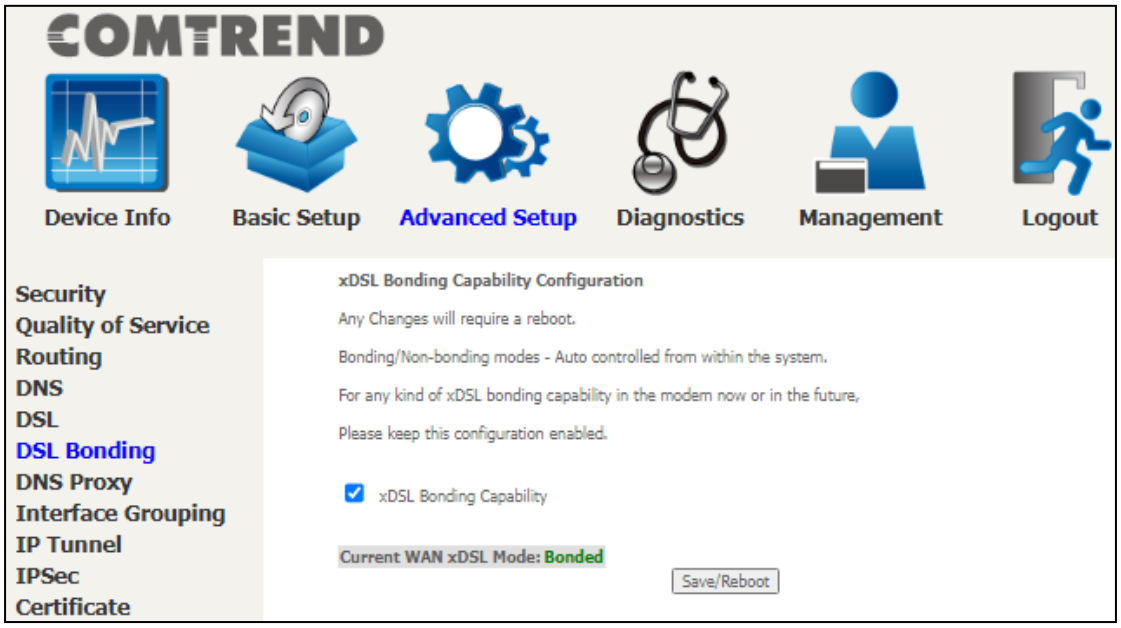
DSL Mode	Data Transmission Rate - Mbps (Megabits per second)
G.Dmt	Downstream: 12 Mbps Upstream: 1.3 Mbps
G.lite	Downstream: 4 Mbps Upstream: 0.5 Mbps
T1.413	Downstream: 8 Mbps Upstream: 1.0 Mbps
ADSL2	Downstream: 12 Mbps Upstream: 1.0 Mbps
AnnexL	Supports longer loops but with reduced transmission rates
ADSL2+	Downstream: 24 Mbps Upstream: 1.0 Mbps

DSL Mode	Data Transmission Rate - Mbps (Megabits per second)
AnnexM	Downstream: 24 Mbps Upstream: 3.5 Mbps
VDSL2	Downstream: 100 Mbps Upstream: 60 Mbps

VDSL Profile	Maximum Downstream Throughput- Mbps (Megabits per second)
8a	Downstream 50
8b	Downstream 50
8c	Downstream: 50
8d	Downstream: 50
12a	Downstream: 68
12b	Downstream: 68
17a	Downstream: 100
30a	Downstream: 100 Mbps Upstream: 100 Mbps
35b	Downstream: 300 Mbps Upstream: 100 Mbps
Options	**Description**
US0	Band between 20 and 138 kHz for long loops to upstream
Bitswap Enable	Enables adaptive handshaking functionality
SRA Enable	Enables Seamless Rate Adaptation (SRA)
Select DSL LED behavior	Normal (TR-68 compliant): Select this option for DSL LED to operate normally (See menu 2.2 LED Indicator) Off: DSL LED will always be OFF
G997.1 EOC xTU-R Serial Number	Select Equipment Serial Number or Equipment MAC Address to use router's serial number or MAC address in ADSL EOC messages

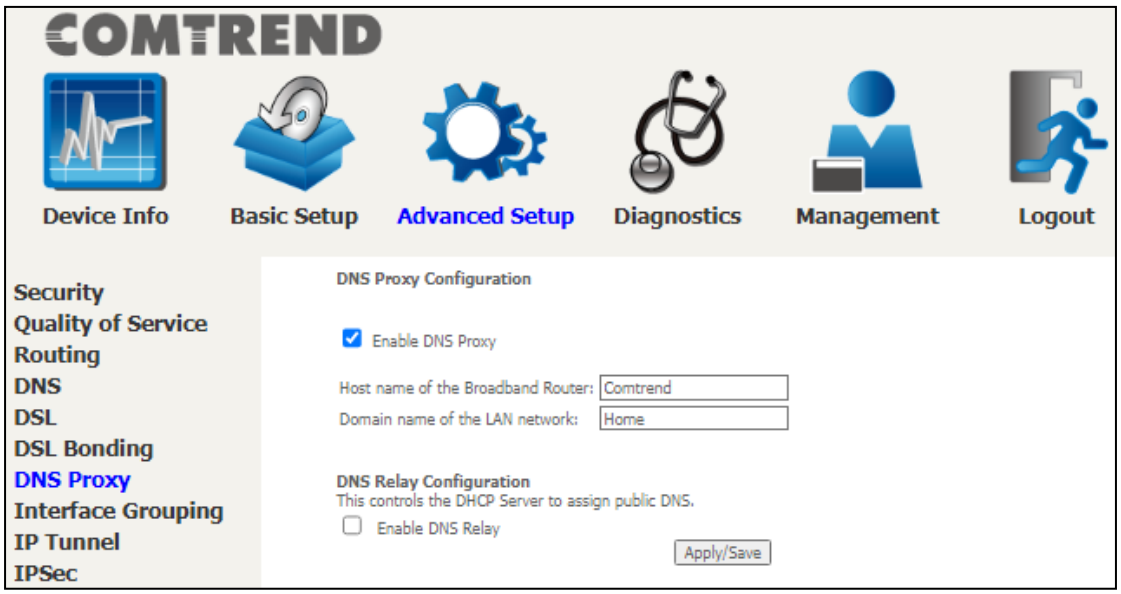
6.6 DSL Bonding

This page displays the bonding status of the connected xDSL line.



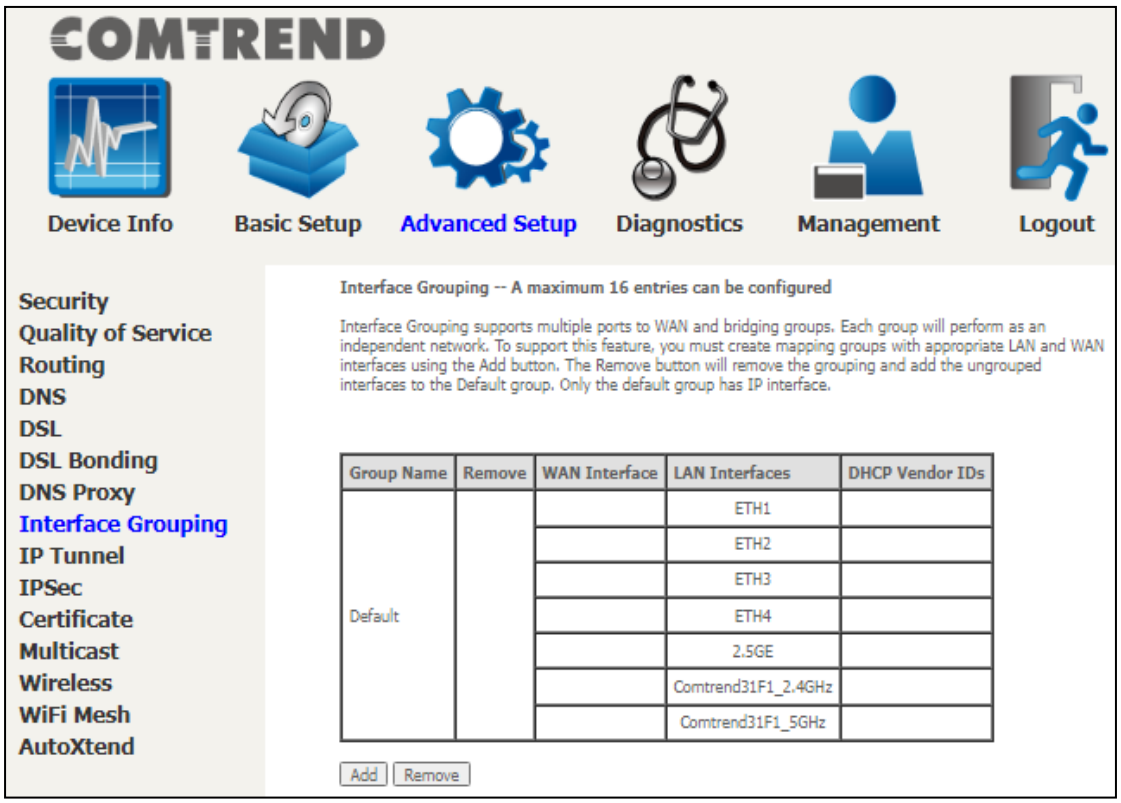
6.7 DNS Proxy

DNS proxy receives DNS queries and forwards DNS queries to the Internet. After the CPE gets answers from the DNS server, it replies to the LAN clients. Configure DNS proxy with the default setting, when the PC gets an IP via DHCP, the domain name, Home, will be added to PC's DNS Suffix Search List, and the PC can access route with "Comtrend.Home".

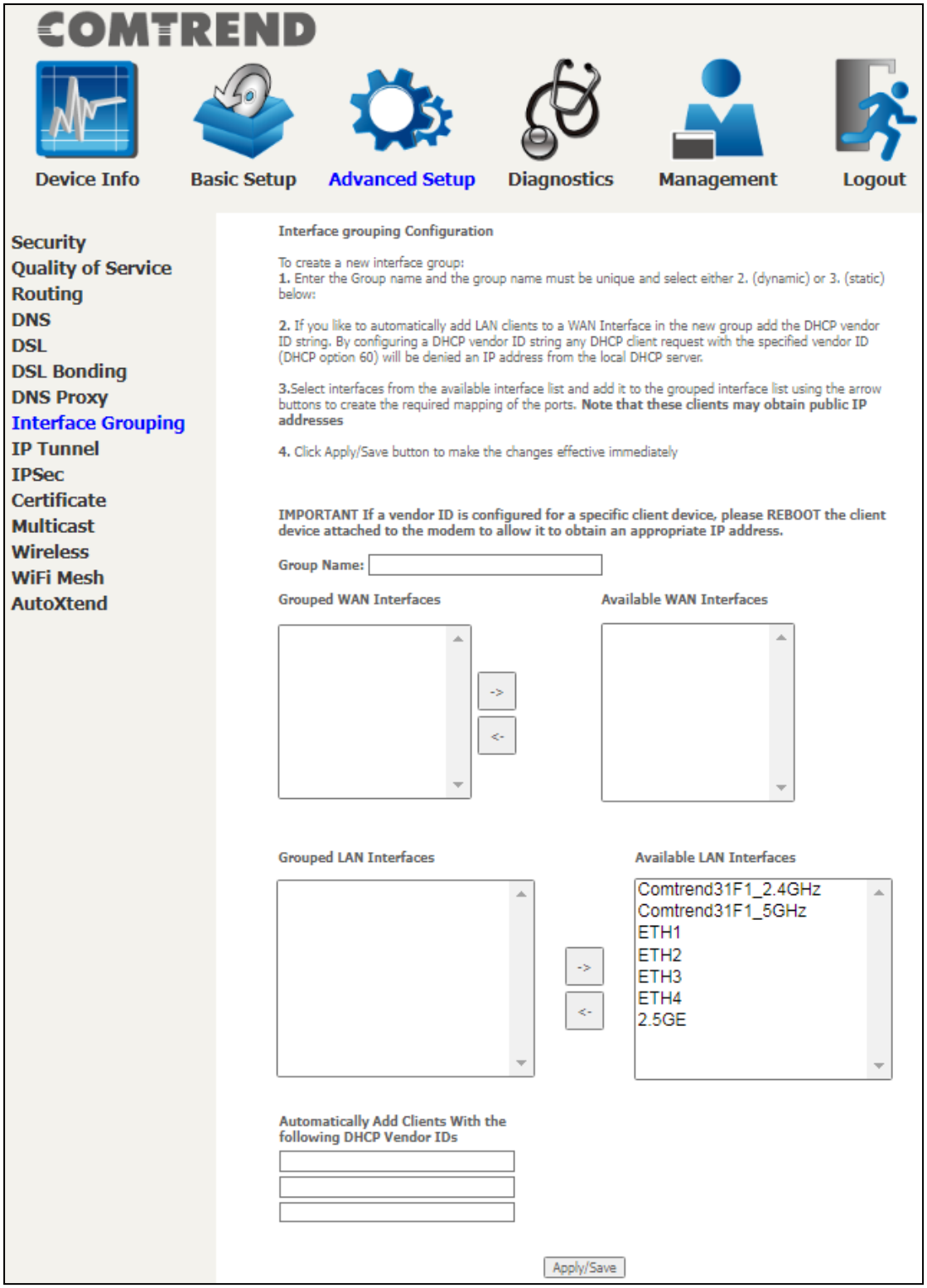


6.8 Interface Grouping

Interface Grouping supports multiple ports to PVC and bridging groups. Each group performs as an independent network. To use this feature, you must create mapping groups with appropriate LAN and WAN interfaces using the **Add** button.
The **Remove** button removes mapping groups, returning the ungrouped interfaces to the Default group. Only the default group has an IP interface.



To add an Interface Group, click the **Add** button. The following screen will appear. It lists the available and grouped interfaces. Follow the instructions shown onscreen.



Automatically Add Clients With Following DHCP Vendor IDs:

Add support to automatically map LAN interfaces to PVC's using DHCP vendor ID (option 60). The local DHCP server will decline and send the requests to a remote DHCP server by mapping the appropriate LAN interface. This will be turned on when Interface Grouping is enabled.

For example, imagine there are 4 PVCs (0/33, 0/36, 0/37, 0/38). VPI/VCI=0/33 is for PPPoE while the other PVCs are for IP set-top box (video). The LAN interfaces are ETH1, ETH2, ETH3, and ETH4.
The Interface Grouping configuration will be:

1. Default: ETH1, ETH2, ETH3, and ETH4.
2. Video: nas_0_36, nas_0_37, and nas_0_38. The DHCP vendor ID is "Video".

If the onboard DHCP server is running on "Default" and the remote DHCP server is running on PVC 0/36 (i.e. for set-top box use only). LAN side clients can get IP addresses from the CPE's DHCP server and access the Internet via PPPoE (0/33).

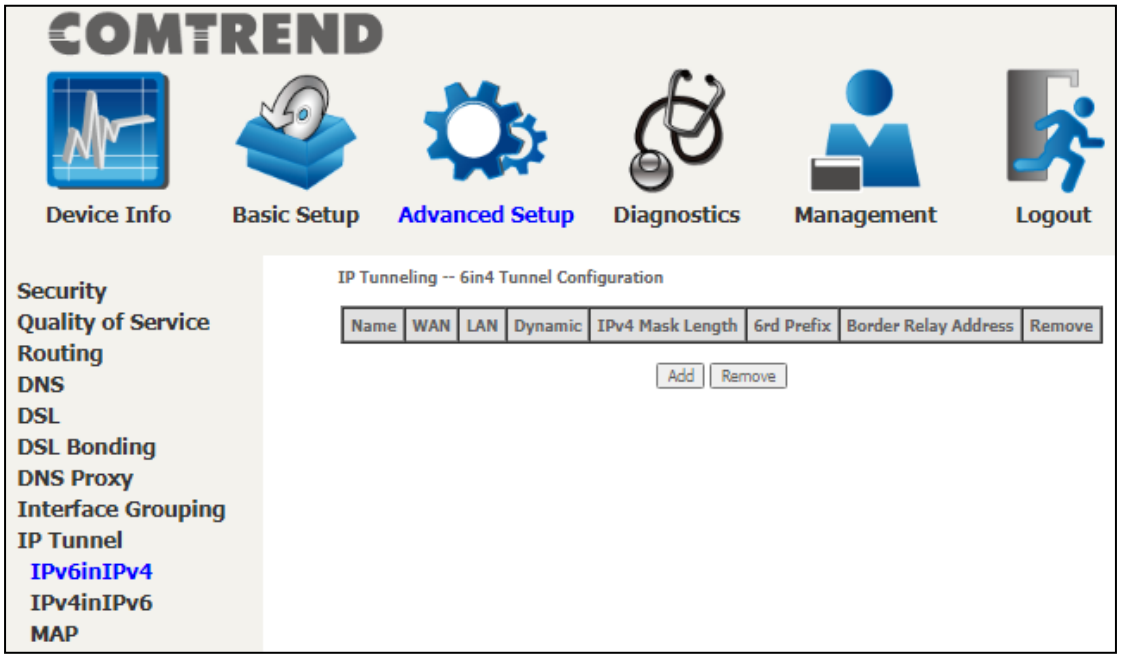
If a set-top box is connected to ETH1 and sends a DHCP request with vendor ID "Video", the local DHCP server will forward this request to the remote DHCP server. The Interface Grouping configuration will automatically change to the following:

1. Default: ETH2, ETH3, and ETH4
2. Video: nas_0_36, nas_0_37, nas_0_38, and ETH1.

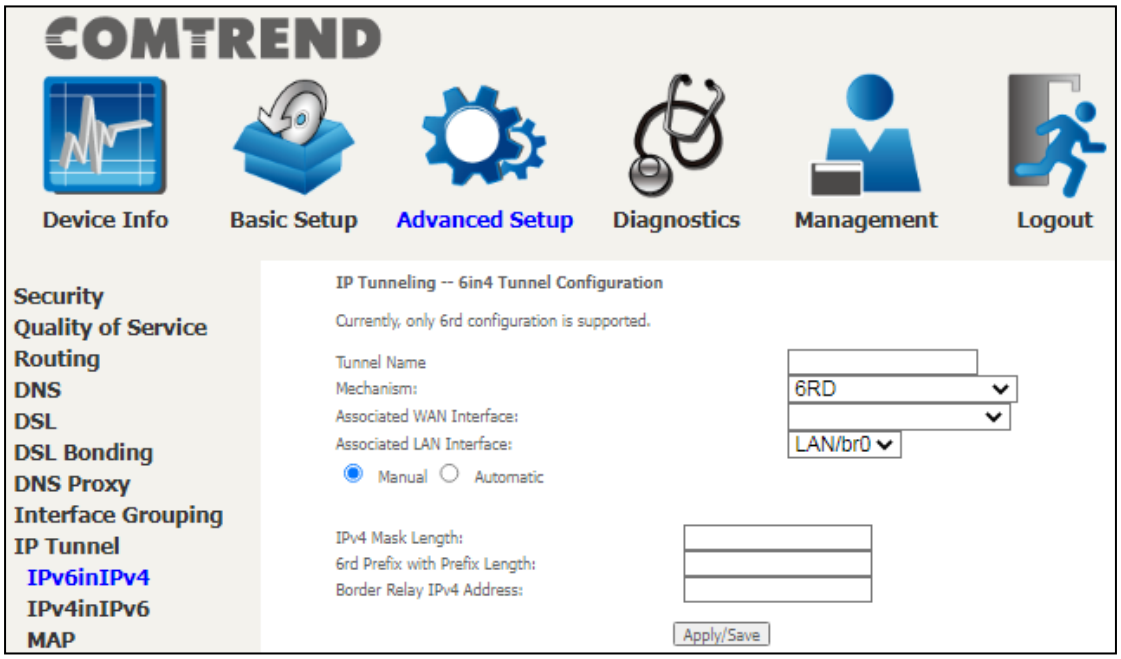
6.9 IP Tunnel

6.9.1 IPv6inIPv4

Configure 6in4 tunneling to encapsulate IPv6 traffic over explicitly-configured IPv4 links.



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



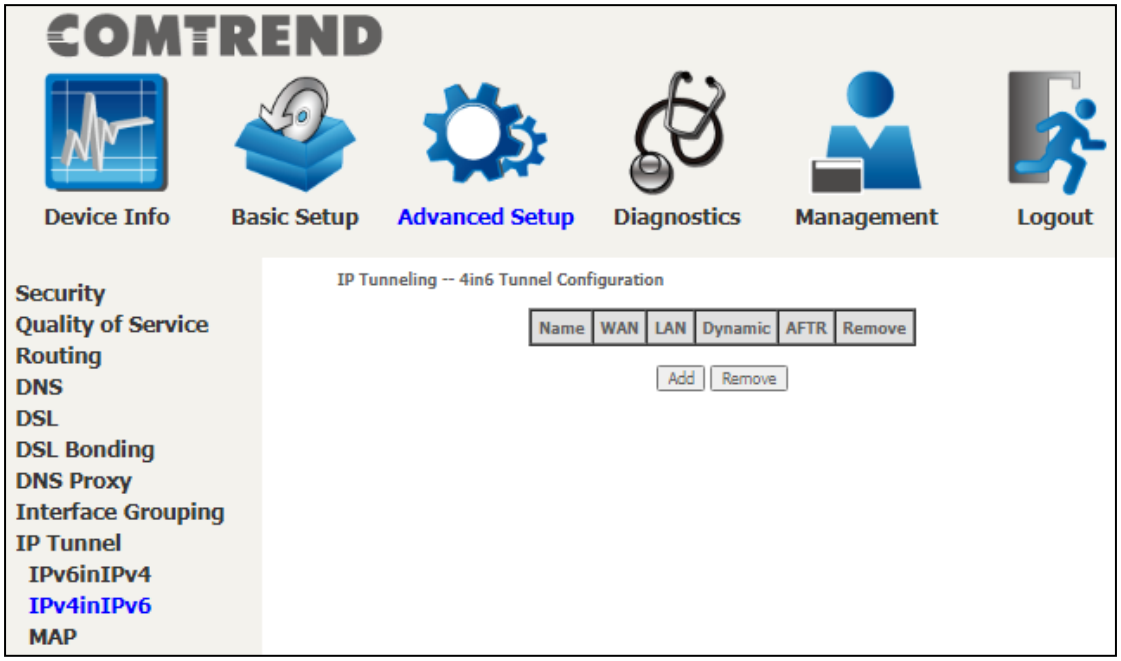
Click **Apply/Save** to apply and save the settings.

Item	Description
Tunnel Name	Input a name for the tunnel

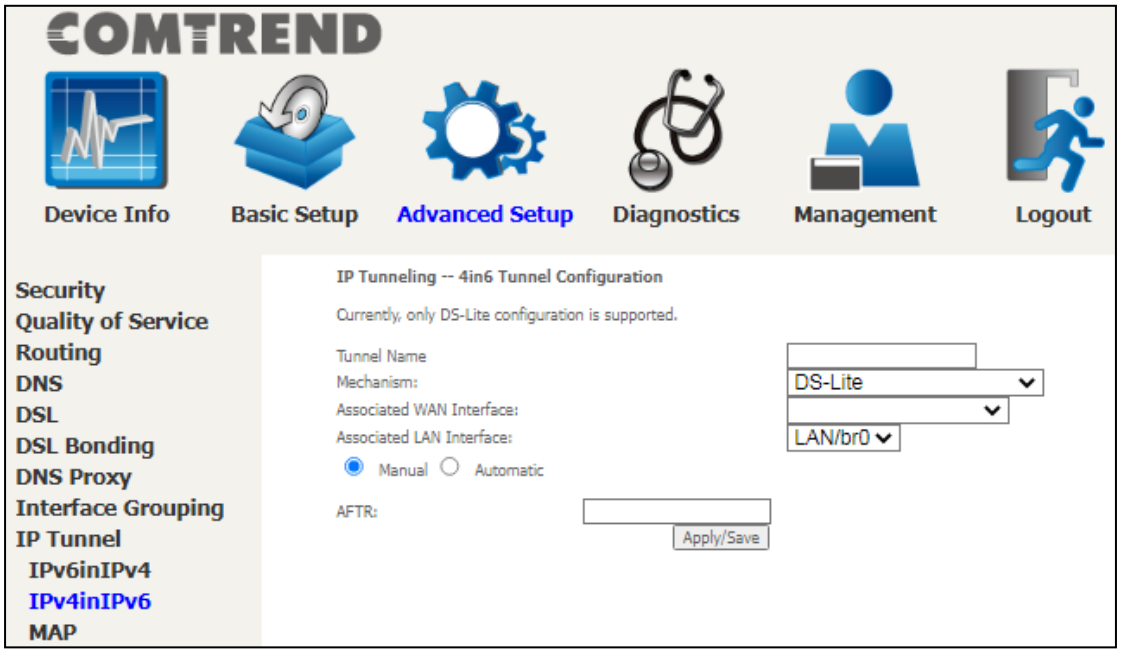
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling
IPv4 Mask Length	The subnet mask length used for the IPv4 interface
6rd Prefix with Prefix Length	Prefix and prefix length used for the IPv6 interface
Border Relay IPv4 Address	Input the IPv4 address of the other device

6.9.2 IPv4inIPv6

Configure 4in6 tunneling to encapsulate IPv4 traffic over an IPv6-only environment.



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

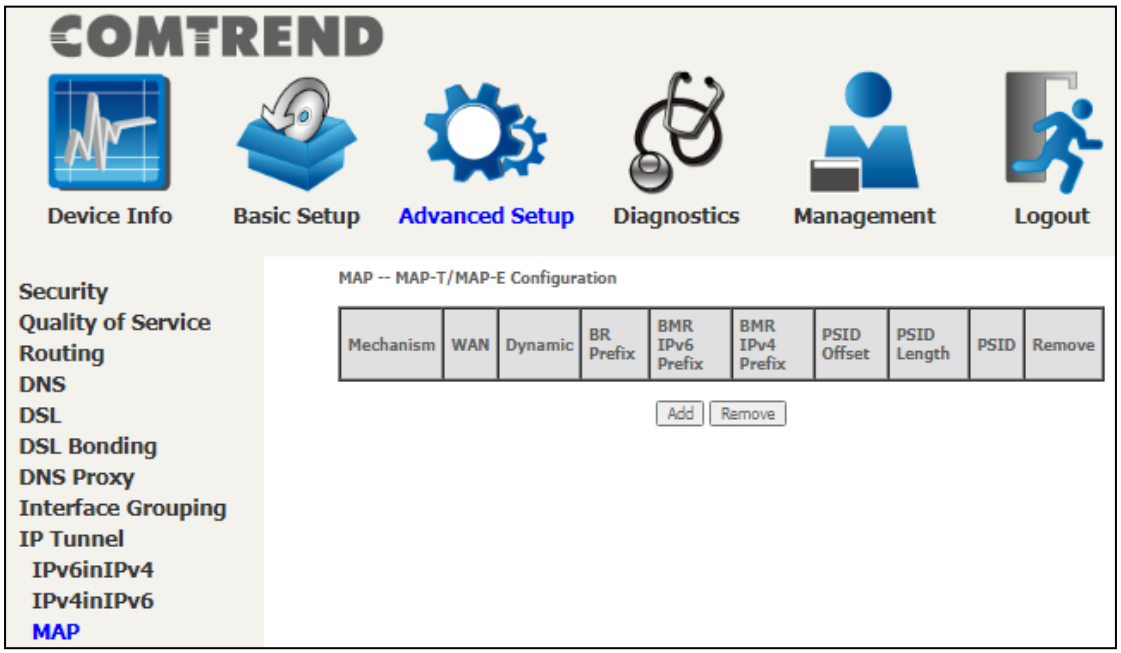


Click **Apply/Save** to apply and save the settings.

Item	Description
Tunnel Name	Input a name for the tunnel
Mechanism	Mechanism used by the tunnel deployment
Associated WAN Interface	Select the WAN interface to be used by the tunnel
Associated LAN Interface	Select the LAN interface to be included in the tunnel
Manual/Automatic	Select automatic for point-to-multipoint tunneling / manual for point-to-point tunneling
AFTR	Address of Address Family Translation Router

6.9.3 MAP

This page allows you to configure MAP-T and MAP-E entries.



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

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

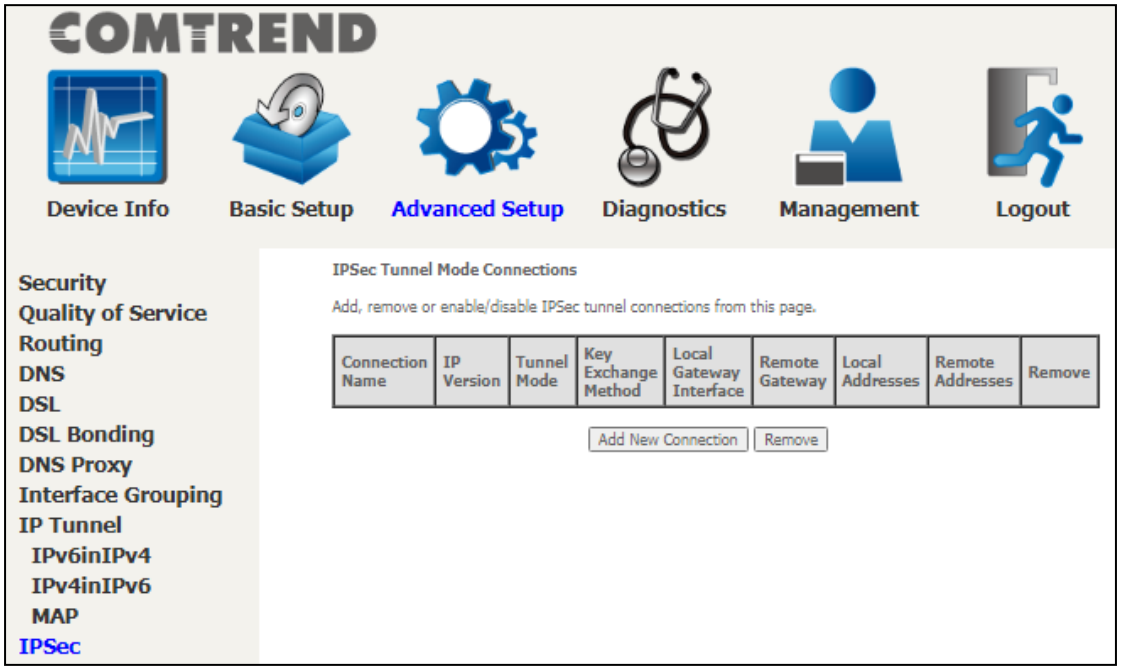
The settings shown above are described below.

Item	Description
Mechanism	Choose whether to encapsulate with MAP-E or MAP-T to be used for NAT64 translation
Associated WAN Interface	Lists the LAN interfaces available to be used for IP MAP
Associated LAN Interface	Lists the LAN interfaces available to be used for IP MAP
Manual Automatic	Configure the prefix and relative PSID settings manually The prefix settings will be configured automatically from the mapping interfaces
BR IPv6 Prefix	Configure the border relay IPv6 Prefix
BMR IPv6 Prefix	Configure the basic mapping rule IPv6 Prefix
BMR IPv4 Prefix	Configure the basic mapping rule IPv4 Prefix
PSID Offset	Port Set ID offset assigned to the IP MAP
PSID Length	Define the port set ID length
PSID Value	Define the port set ID value

6.10 IPSec

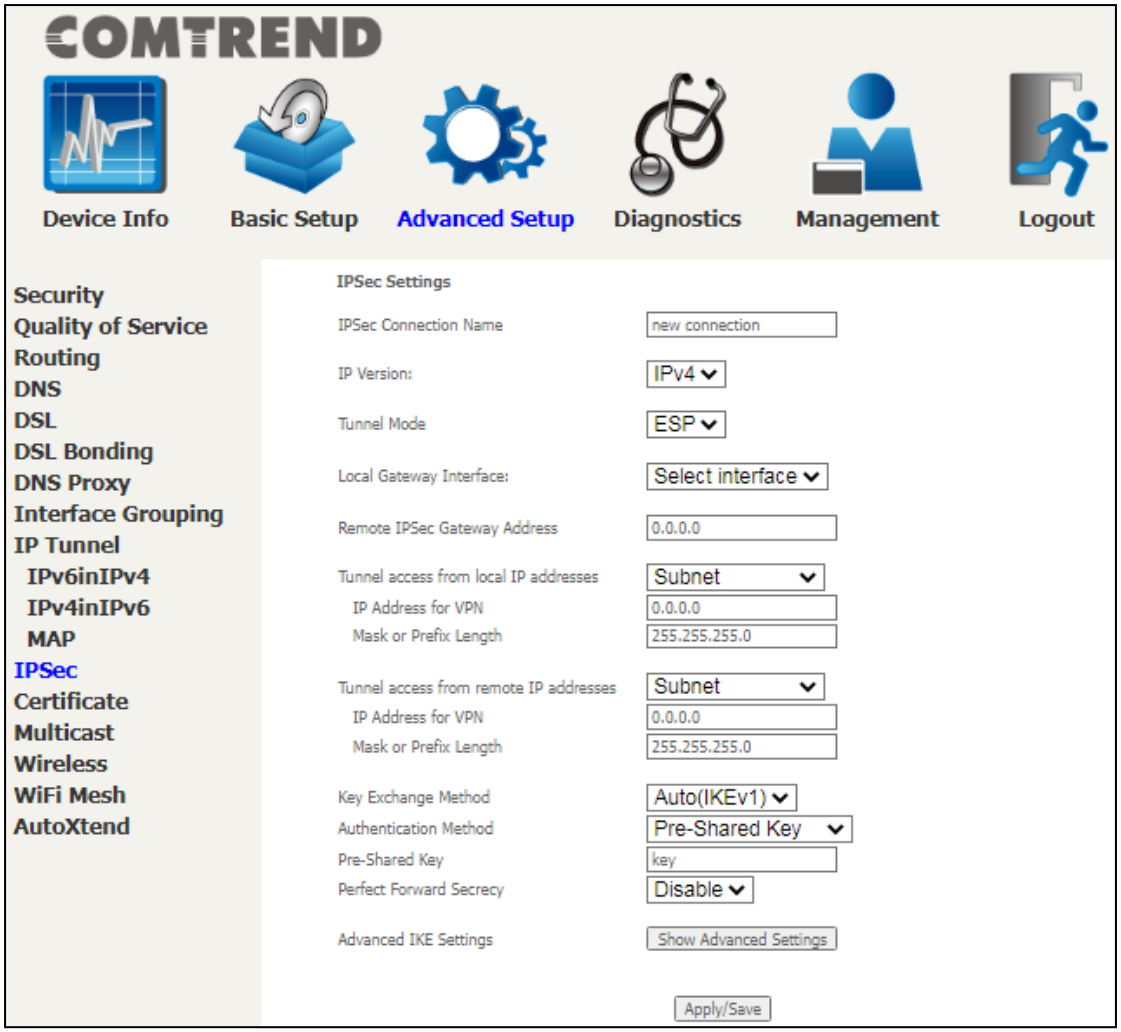
6.10.1 IPSec Tunnel Mode Connections

You can add, edit or remove IPSec tunnel mode connections from this page.



Click **Add New Connection** to add a new IPSec termination rule.

The following screen will display.

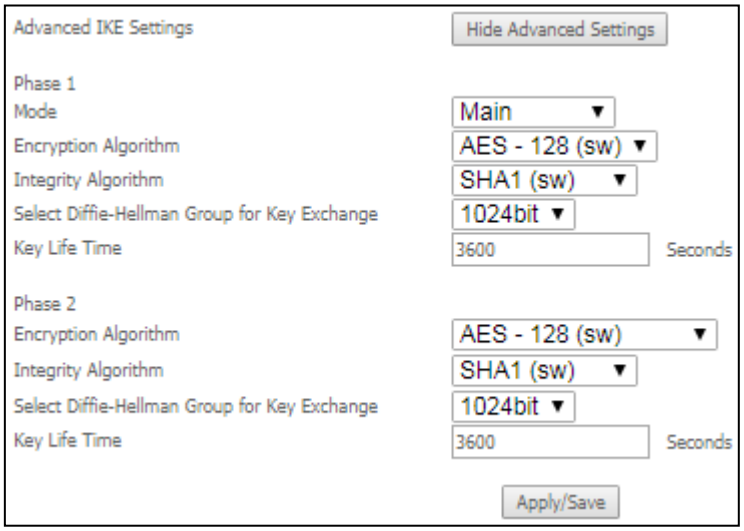


Heading	Description
IPSec Connection Name	User-defined label
IP Version	Select the corresponding IPv4 / IPv6 version for the IPSEC connection
Tunnel Mode	Select tunnel protocol, AH (Authentication Header) or ESP (Encapsulating Security Payload) for this tunnel.
Local Gateway Interface	Select from the list of wan interface to be used as gateway for the IPSEC connection
Remote IPSec Gateway Address	The location of the Remote IPSec Gateway. IP address or domain name can be used.
Tunnel access from local IP addresses	Specify the acceptable host IP on the local side. Choose **Single** or **Subnet**.

IP Address/Subnet Mask for VPN	If you chose **Single**, please enter the host IP address for VPN. If you chose **Subnet**, please enter the subnet information for VPN.
Tunnel access from remote IP addresses	Specify the acceptable host IP on the remote side. Choose **Single** or **Subnet**.
IP Address/Subnet Mask for VPN	If you chose **Single**, please enter the host IP address for VPN. If you chose **Subnet**, please enter the subnet information for VPN.
Key Exchange Method	Select from Auto(IKE) or Manual

For the Auto(IKE) key exchange method, select Pre-shared key or Certificate (X.509) authentication. For Pre-shared key authentication you must enter a key, while for Certificate (X.509) authentication you must select a certificate from the list.

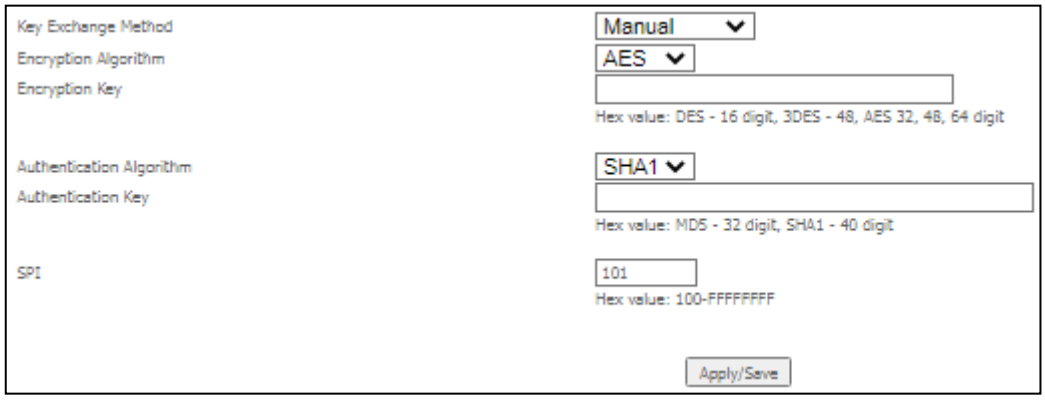
See the tables below for a summary of all available options.

Auto(IKE) Key Exchange Method	
Pre-Shared Key / Certificate (X.509)	Input Pre-shared key / Choose Certificate
Perfect Forward Secrecy	Enable or Disable
Advanced IKE Settings	Select **Show Advanced Settings** to reveal the advanced settings options shown below.
	
Advanced IKE Settings	Select **Hide Advanced Settings** to hide the advanced settings options shown above.
Phase 1 / Phase 2	Choose settings for each phase, the available options are separated with a "/" character.
Mode	Main / Aggressive

Encryption Algorithm	DES / 3DES / AES 128,192,256
Integrity Algorithm	MD5 / SHA1
Select Diffie-Hellman Group	768 – 8192 bit
Key Life Time	Enter your own or use the default (1 hour)

The Manual key exchange method options are summarized in the table below.

Manual Key Exchange Method

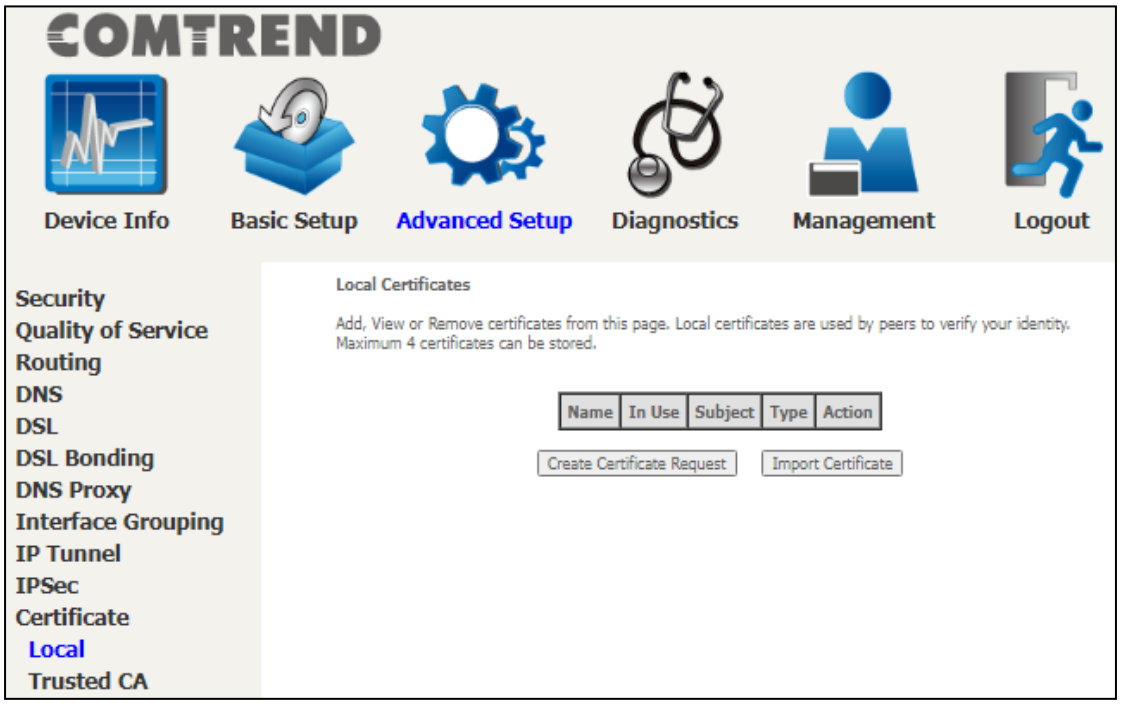


Encryption Algorithm	DES / 3DES / AES (aes-cbc)
Encryption Key	DES: 16 digit Hex, 3DES: 48 digit Hex
Authentication Algorithm	MD5 / SHA1
Authentication Key	MD5: 32 digit Hex, SHA1: 40 digit Hex
SPI (default is 101)	Enter a Hex value from 100-FFFFFFFF

6.11 Certificate

A certificate is a public key, attached with its owner's information (company name, server name, personal real name, contact e-mail, postal address, etc) and digital signatures. There will be one or more digital signatures attached to the certificate, indicating that these entities have verified that this certificate is valid.

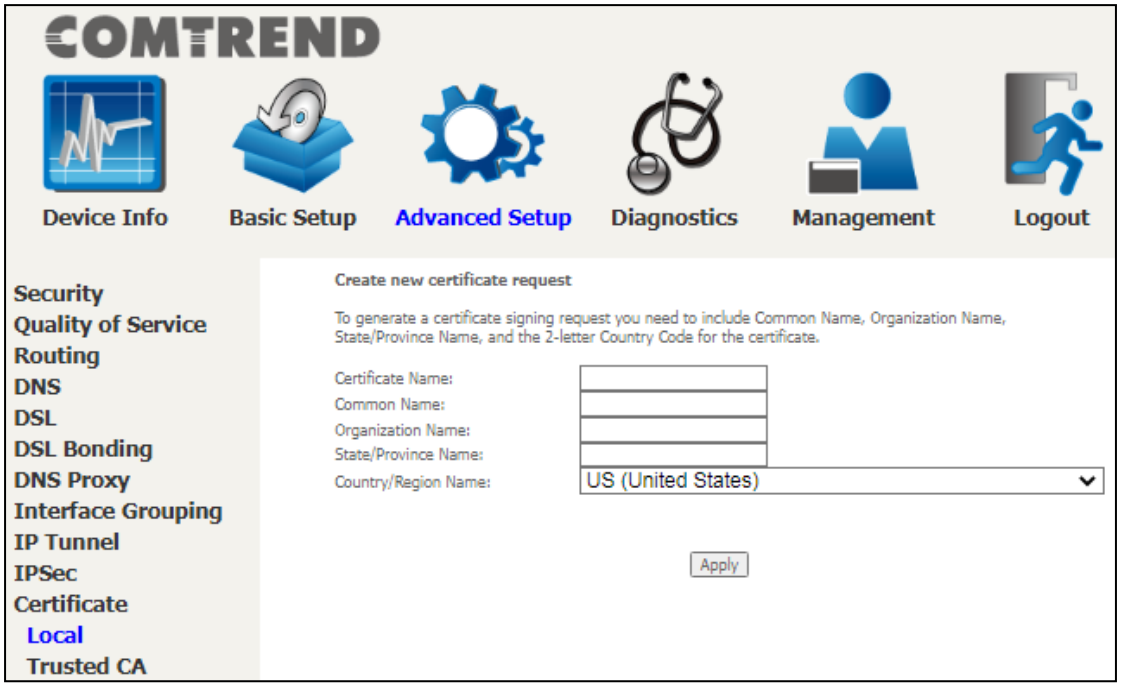
6.11.1 Local



CREATE CERTIFICATE REQUEST

Click **Create Certificate Request** to generate a certificate-signing request.

The certificate-signing request can be submitted to the vendor/ISP/ITSP to apply for a certificate. Some information must be included in the certificate-signing request. Your vendor/ISP/ITSP will ask you to provide the information they require and to provide the information in the format they regulate. Enter the required information and click **Apply** to generate a private key and a certificate-signing request. The contents of this application form do not affect the basic parameter settings of the product.

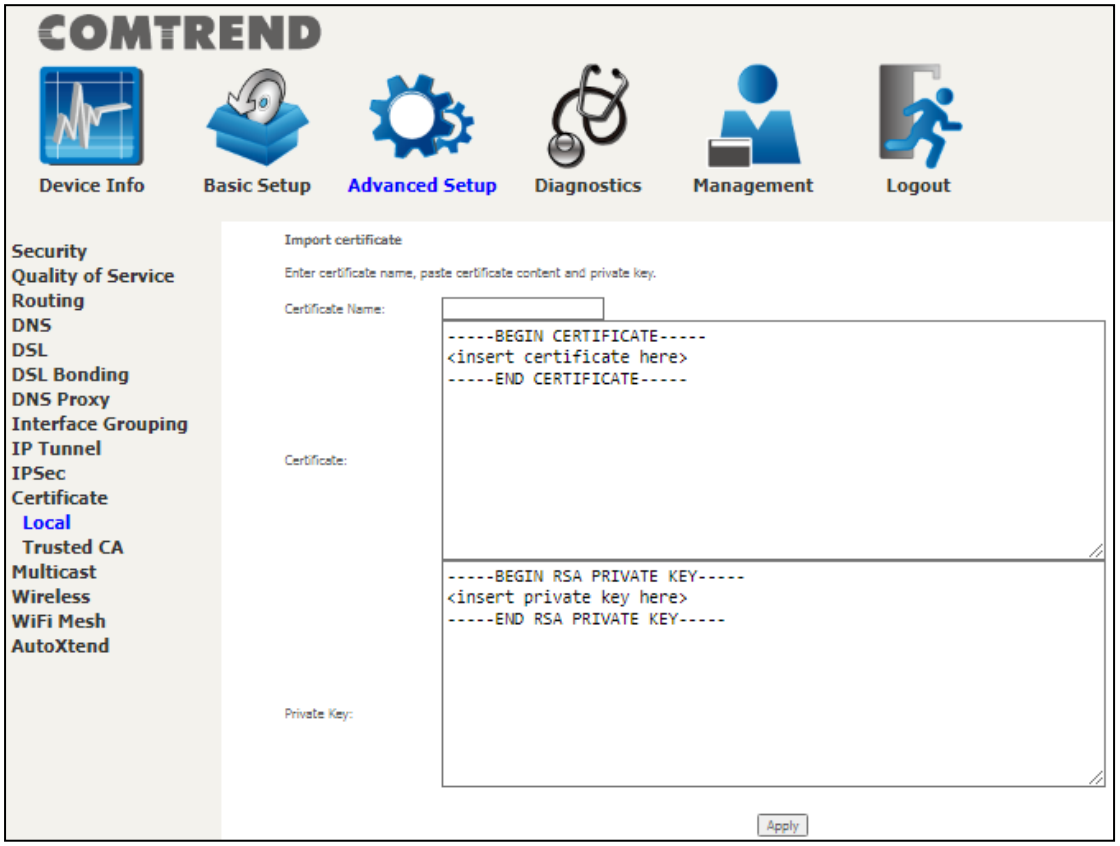


The following table is provided for your reference.

Item	Description
Certificate Name	A user-defined name for the certificate.
Common Name	Usually, the fully qualified domain name for the machine.
Organization Name	The exact legal name of your organization. Do not abbreviate.
State/Province Name	The state or province where your organization is located. It cannot be abbreviated.
Country/Region Name	The two-letter ISO abbreviation for your country.

IMPORT CERTIFICATE

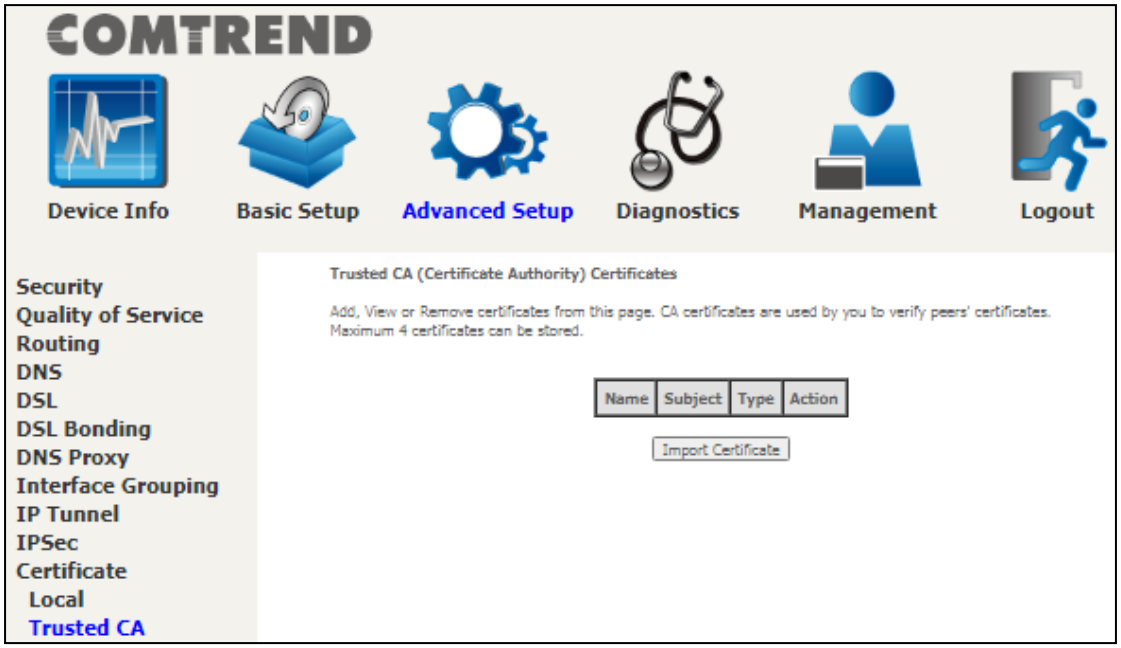
Click **Import Certificate** to paste the certificate content and the private key provided by your vendor/ISP/ITSP into the corresponding boxes shown below.



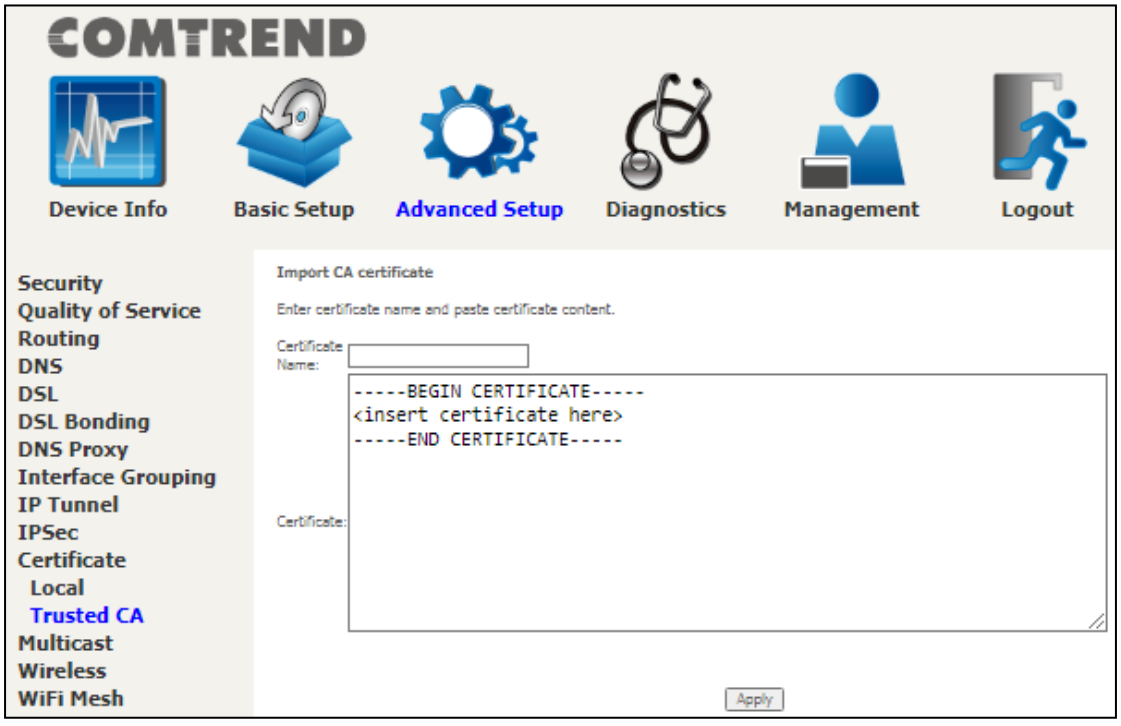
Enter a certificate name and click the **Apply** button to import the certificate and its private key.

6.11.2 Trusted CA

CA is an abbreviation for Certificate Authority, which is a part of the X.509 system. It is itself a certificate, attached with the owner information of this certificate authority; but its purpose is not encryption/decryption. Its purpose is to sign and issue certificates, in order to prove that these certificates are valid.



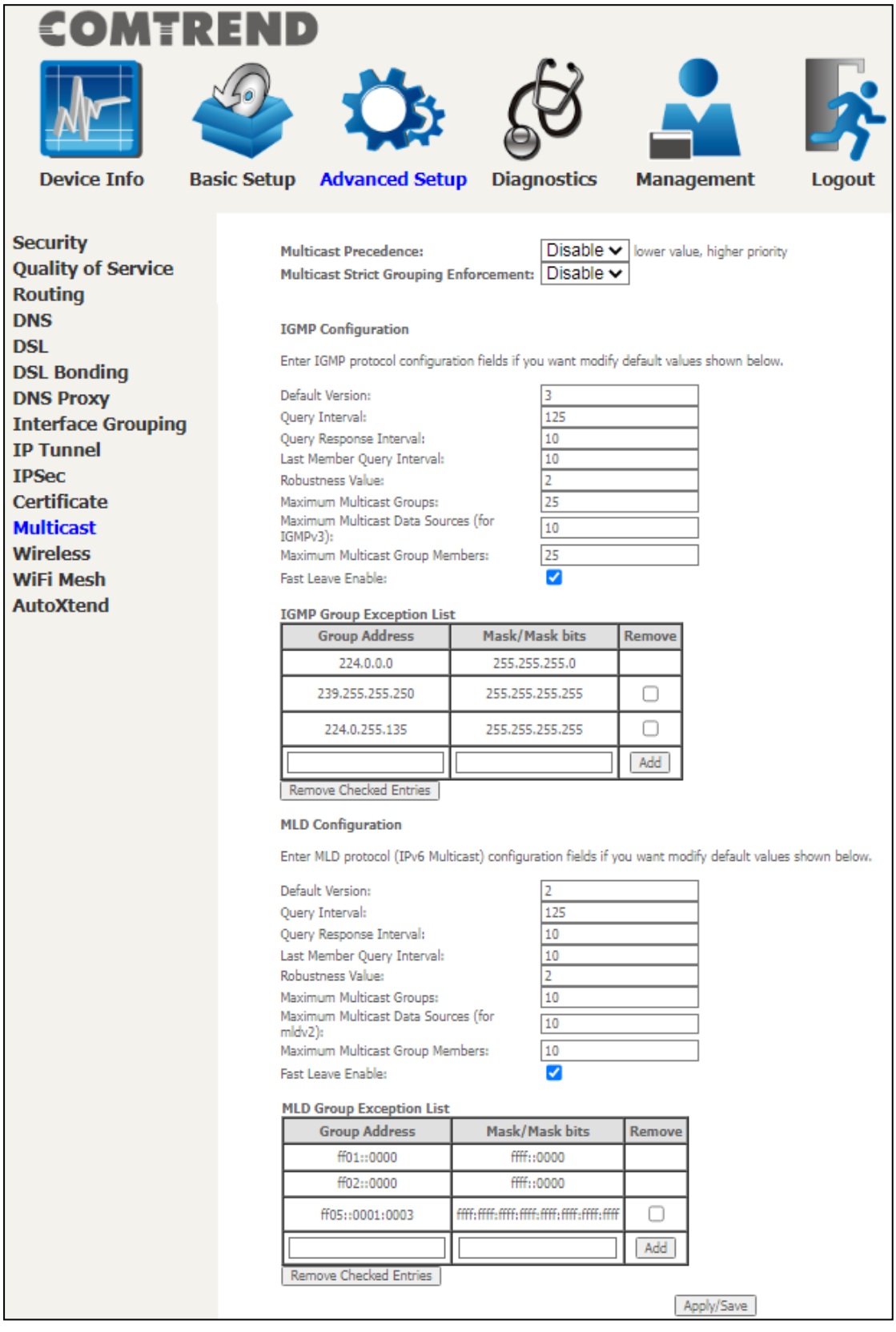
Click **Import Certificate** to paste the certificate content of your trusted CA. The CA certificate content will be provided by your vendor/ISP/ITSP and is used to authenticate the Auto-Configuration Server (ACS) that the CPE will connect to.



Enter a certificate name and click **Apply** to import the CA certificate.

6.12 Multicast

Input new IGMP or MLD protocol configuration fields if you want modify default values shown. Then click **Apply/Save**.



Multicast Precedence: Select precedence of multicast packets.

Multicast Strict Grouping Enforcement: Enable/Disable multicast strict grouping.

Item	Description
Default Version	Define IGMP using version with video server.
Query Interval	The query interval is the amount of time in seconds between IGMP General Query messages sent by the router (if the router is the querier on this subnet). The default query interval is 125 seconds.
Query Response Interval	The query response interval is the maximum amount of time in seconds that the IGMP router waits to receive a response to a General Query message. The query response interval is the Maximum Response Time field in the IGMP v2 Host Membership Query message header. The default query response interval is 10 seconds and must be less than the query interval.
Last Member Query Interval	The last member query interval is the amount of time in seconds that the IGMP router waits to receive a response to a Group-Specific Query message. The last member query interval is also the amount of time in seconds between successive Group-Specific Query messages. The default last member query interval is 10 seconds.
Robustness Value	The robustness variable is a way of indicating how susceptible the subnet is to lost packets. IGMP can recover from robustness variable minus 1 lost IGMP packets. The robustness variable should be set to a value of 2 or greater. The default robustness variable value is 2.
Maximum Multicast Groups	Setting the maximum number of Multicast groups.
Maximum Multicast Data Sources (for IGMPv3)	Define the maximum multicast video stream number.
Maximum Multicast Group Members	Setting the maximum number of groups that ports can accept.
Fast Leave Enable	When you enable IGMP fast-leave processing, the switch immediately removes a port when it detects an IGMP version 2 leave message on that port.

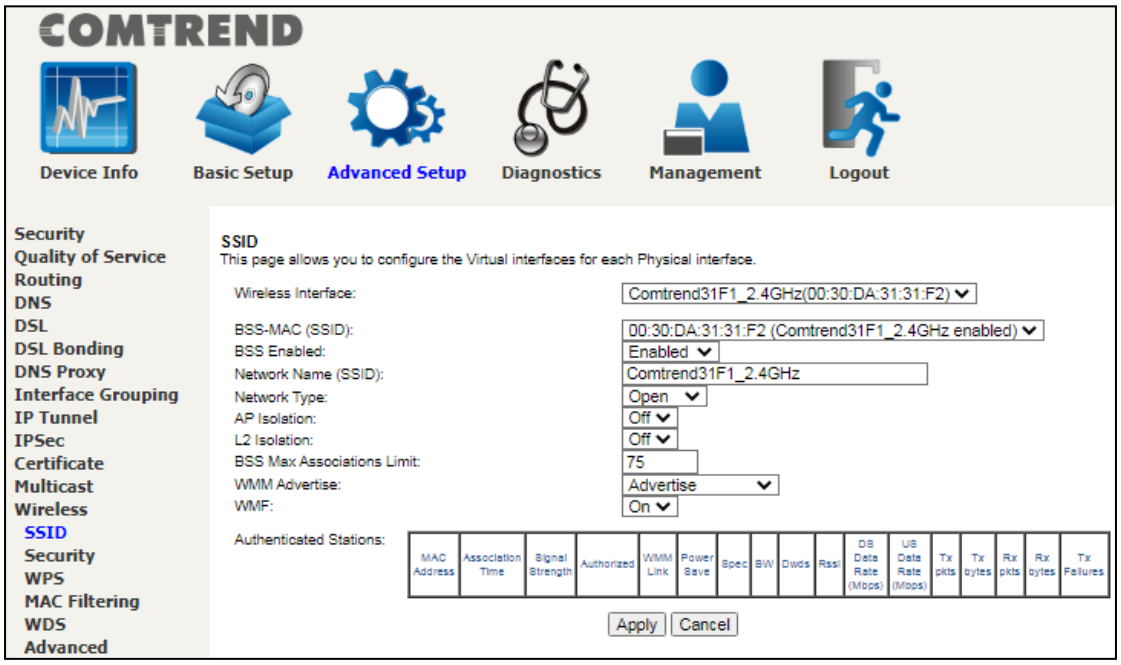
IGMP Group Exception List / MLD Group Exception List

Item	Description
Group Address	This is the delimited list of ignored multicast addresses being queried when sending a Group-Specific or Group-and-Source-Specific Query.
Mask/Mask Bits	This is the delimited list of ignored multicast mask being queried when sending a Group-Specific or Group-and-Source-Specific Query.
Remove	Allows a user to remove a specific item in the exception list.

6.13 Wireless

6.13.1 SSID

This page allows you to configure the Virtual interfaces for each Physical interface.



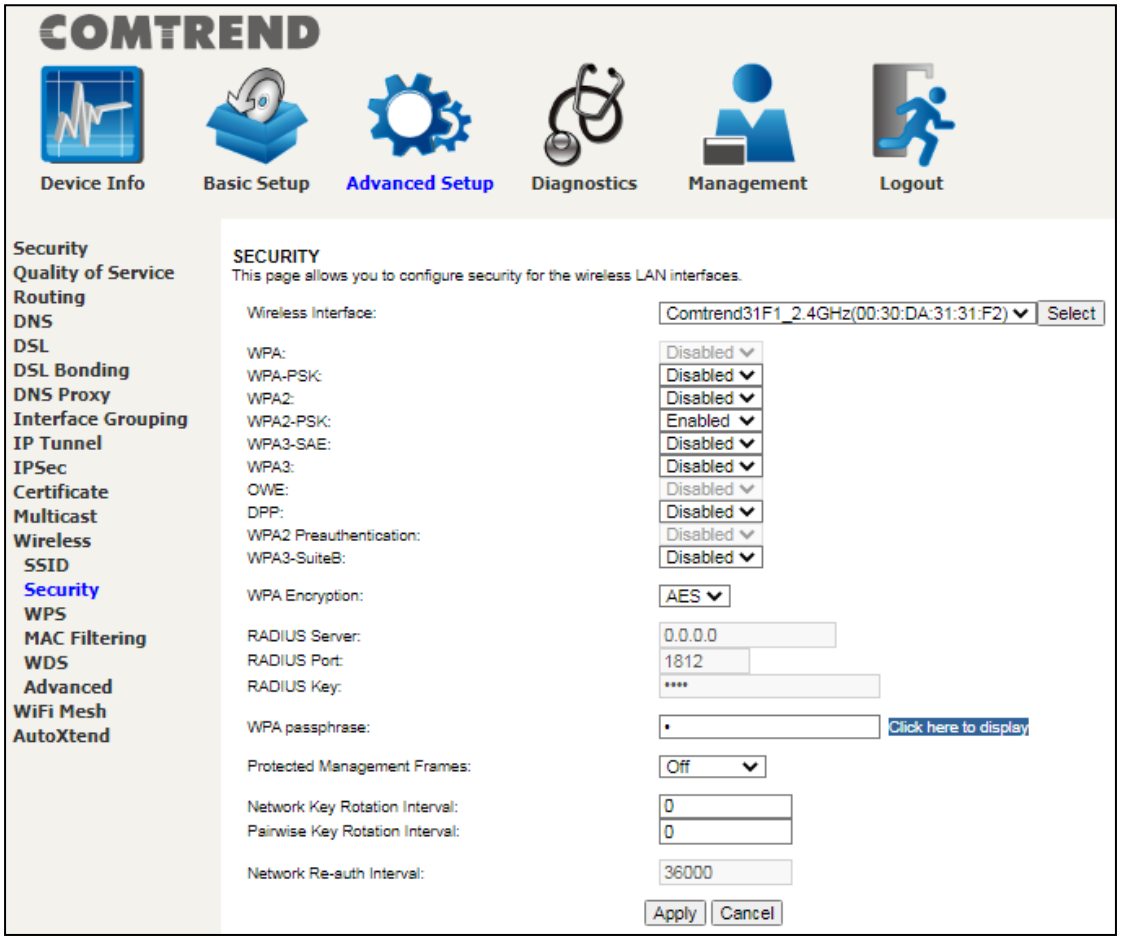
Click the **Apply** button to apply your changes. The settings shown above are described below.

Item	Description
Wireless Interface	Select which wireless interface to configure
BSS-MAC (SSID)	Select desired BSS to configure
BSS Enabled	Enable or disable this SSID
Network Name (SSID)	Sets the network name (also known as SSID) of this network
Network Type	Selecting **Closed** hides the network from active scans. Selecting **Open** reveals the network from active scans.
AP Isolation	Selecting **On** enables AP Isolation mode. When enabled, STAs associated with the AP will not be able to communicate with each other.
L2 Isolation	Wireless clients on the guest network cannot access hardwired LAN clients

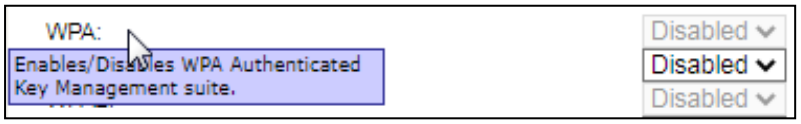
BSS Max Associations Limit	Sets the maximum associations for this BSS
WMM Advertise	When WMM is enabled for the radio, selecting **On** allows WMM to be advertised in beacons and probes for this BSS. **Off** disables advertisement of WMM in beacons and probes.
WMF	Choose **On** to enable Wireless Multicast Forwarding on this BSS. **Off** disables this feature.
MAC Address	Lists the MAC address of all the stations.
Association Time	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.
Signal Strength	Wi-Fi connection signal strength icon
Authorized	Lists those devices with authorized access
WMM Link	Lists those devices that utilize WMM
Power Save	Lists those devices that utilize the Power Save Feature
Spec	Wi-Fi Spec
BW	Bandwidth
Dwds	Lists the devices that utilize Dynamic WDS
Rssi	Received Signal Strength Indicator
DS Data Rate (Mbps)	Receive Rate
US Data Rate (Mbps)	Transmit Rate
Tx pkts	Shows total Tx packets
Tx bytes	Shows total Tx bytes
Rx pkts	Shows total Rx packets
Rx bytes	Shows total Rx bytes
Tx Failures	Shows total Tx packets failed

6.13.2 Security

This page allows you to configure security for the wireless LAN interfaces.



Click the **Apply** button to apply your changes. For information on each parameter, move the cursor over the parameter that you are interested in (as shown here).



The descriptions are also shown below.

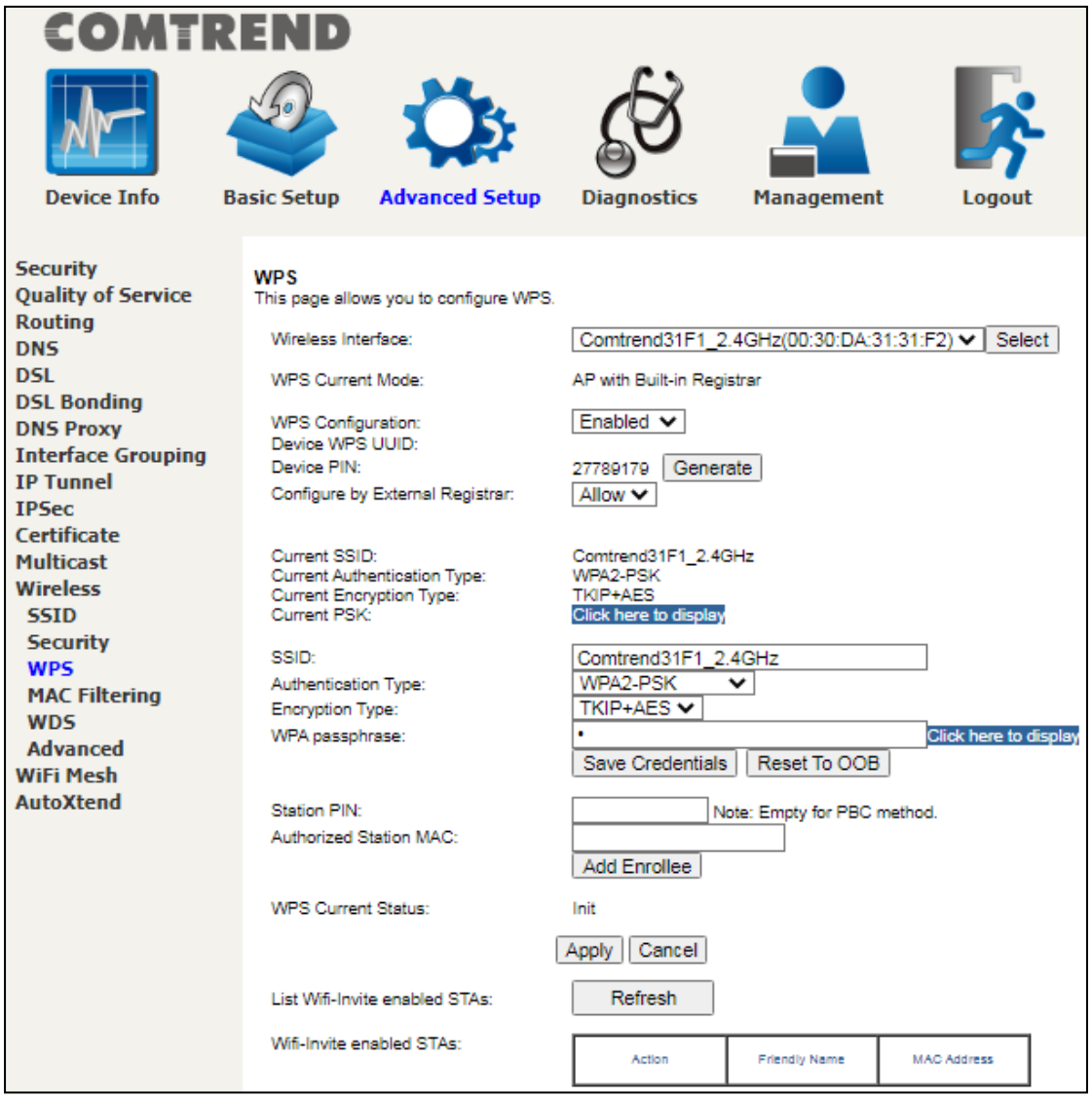
Item	Description
Wireless Interface	Select which wireless interface to configure
WPA	Enable/disable WPA authenticated key management suite

WPA-PSK	Enable/disable WPA-PSK authenticated key management suite
WPA2	Enable/disable WPA2 authenticated key management suite
WPA2-PSK	Enable/disable WPA2-PSK authenticated key management suite
WPA3-SAE	Enable/disable WPA3-SAE authenticated key management suite
WPA3	Enable/disable WPA3 authenticated key management suite
OWE	Enable/disable OWE authenticated key management suite
DPP	Enable/disable DPP authenticated key management suite
WPA2 Preauthentication	Enable/disable WPA2 Preauthenticated key management suite
WPA3-SuiteB	Enable/disable WPA3-SuiteB key management suite
WPA Encryption	Select the WPA encryption algorithm
RADIUS Server	Set the IP of the RADIUS (Remote Authentication Dial In User Service) to use for authentication and dynamic key derivation
RADIUS Port	Set the UDP port number of the RADIUS server. The port number is usually 1812 or 1645 and depends upon the server.
RADIUS Key	Set the shared secret for the RADIUS connection
WPA passphrase	Set the WPA passphrase
Protected Management Frames	Wi-Fi CERTIFIED WPA2 with Protected Management Frames provides a WPA2-level of protection for unicast and multicast management action frames.
Network Key Rotation Interval	Set the Network Key Rotation interval in seconds. Leave blank or set to zero to disable the rotation.

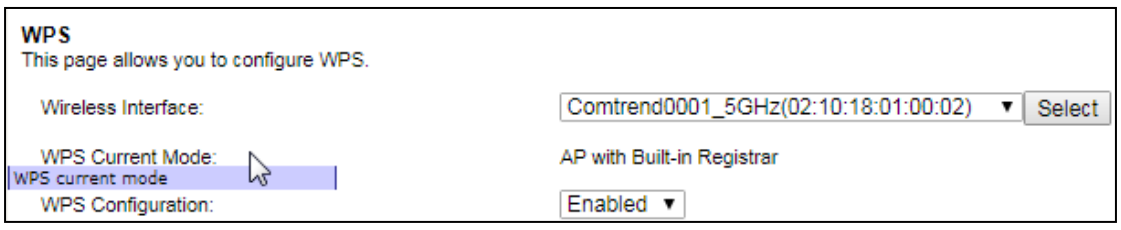
Pairwise Key Rotation Interval	Set the Pairwise Key Rotation interval in seconds. Leave blank or set to zero to disable the rotation.
Network Re-auth Interval	Set the Network Key Re-authentication interval in seconds. Leave blank or set to zero to disable periodic network re-authentication.

6.13.3 WPS

This page allows you to configure WPS.



Click the **Apply** button to apply your changes. For information on each parameter, move the cursor over the parameter that you are interested in (as shown here).



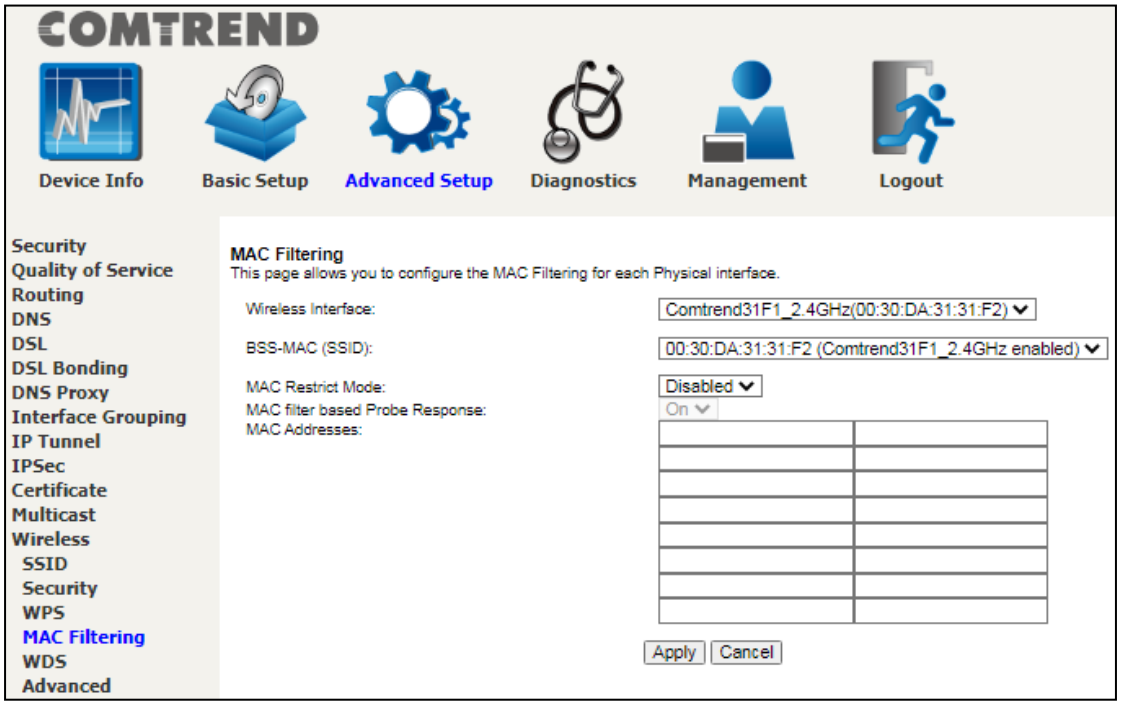
The descriptions are also shown below.

Item	Description
Wireless Interface	Select which wireless interface to configure
WPS Current Mode	Displays WPS current mode
WPS Configuration	Enable/Disable Wi-Fi simple config mode
Device WPS UUID	Displays the WPS UUID number of this device
Device PIN	Displays the PIN number for this device. Click the **Generate** button to change a unique Device PIN number.
Configure by External Registrar	Set Allow/Deny wireless external registrar to get/configure AP security through AP PIN
Current SSID	Displays the current SSID
Current Authentication Type	Displays the current authentication type
Current Encryption Type	Displays the current encryption type
Current PSK	Displays the current PSK by clicking Click here to display
SSID	Set the network name (also known as the SSID) of this network
Authentication Type	Select the authentication type from the drop-down menu
Encryption Type	Select the encryption type from the drop-down menu
WPA passphrase	Set the WPA passphrase. Click the **Save Credentials** button to save the Wi-Fi access password. Click the **Reset To OOB** (Out of Box configure) button to restore SSID/ Authentication Type / Encryption Type / WPA passphrase default setting.
Station PIN	Input the station PIN to verify expected station. Note: Empty for PBC method.

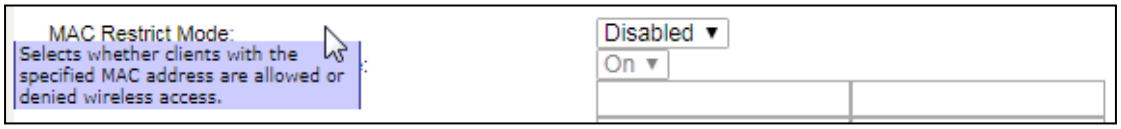
Authorized Station MAC	Input the authorized station MAC address. Click the **Add Enrollee** button to start a WPS process. This WPS process is only for the client whose MAC is typed in this field.
WPS Current Status	Displays the WPS current status
List Wifi-Invite enabled STAs	Click the Refresh button to find WiFi-Invite enabled STAs
Wifi-Invite enabled STAs	Displays the list of WiFi-Invite enabled STAs

6.13.4 MAC Filtering

This page allows you to configure the MAC Filtering for each Physical interface.



Click the **Apply** button to apply your changes. For information on each parameter, move the cursor over the parameter that you are interested in (as shown here).

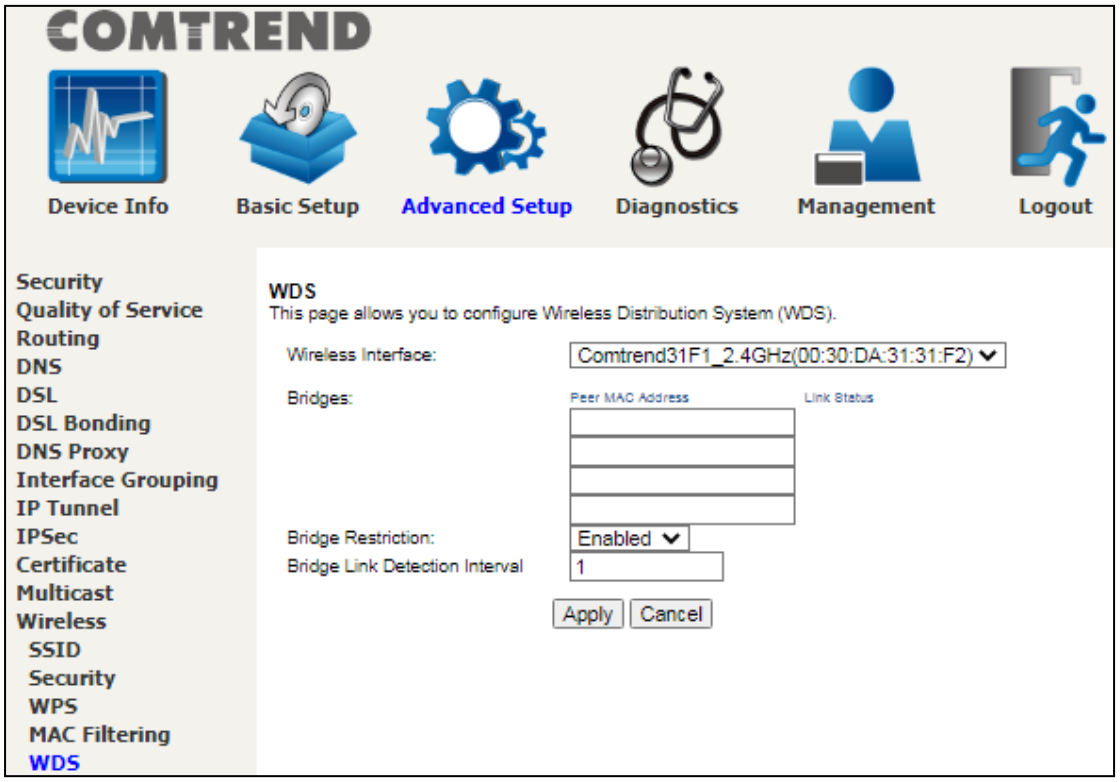


The descriptions are also shown below.

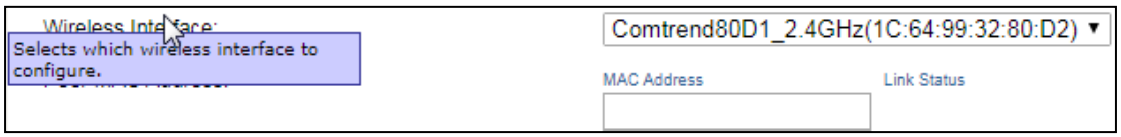
Item	Description
Wireless Interface	Select which wireless interface to configure
BSS-MAC (SSID)	Select desired BSS to configure
MAC Restrict Mode	Select whether clients with the specified MAC address are allowed or denied wireless access
MAC filter based Probe Response	Enable/Disable MAC filter based probe response mode
MAC Addresses	Allow/Deny wireless access to clients with the specified MAC addresses. The MAC address format is xx:xx:xx:xx:xx:xx.

6.13.5 WDS

The wireless distribution system supports extended networking of wireless access points and can be configured as described below.



Click the **Apply** button to apply your changes. For information on each parameter, move the cursor over the parameter that you are interested in (as shown here).



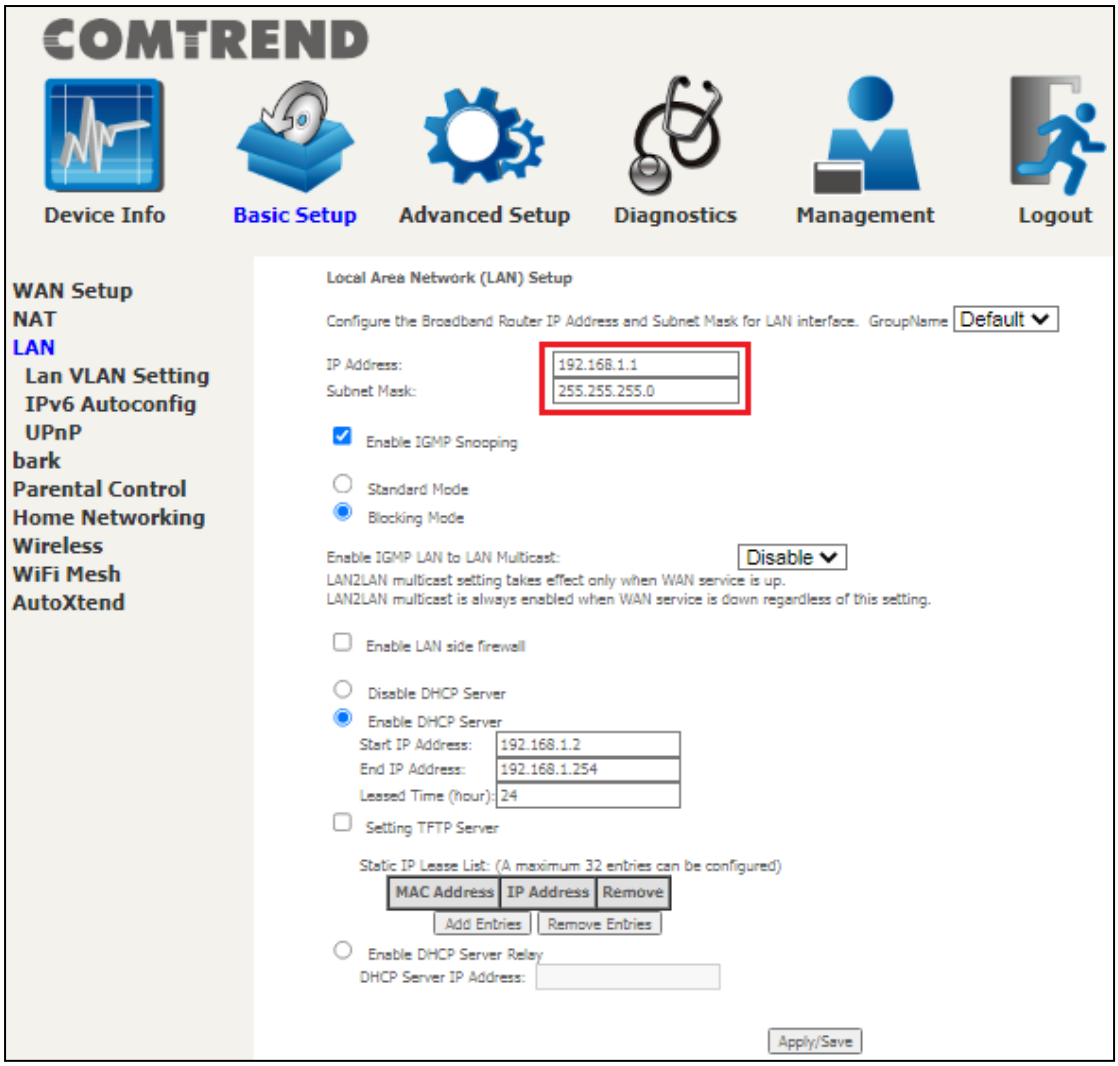
The descriptions are also shown below.

Item	Description
Wireless Interface	Select which wireless interface to configure
Peer MAC address	Enter the peer wireless MAC addresses of any member that should be part of the Wireless Distribution System (WDS)
Restriction	Select Disabled to disable the WDS restriction. Any WDS (including the ones listed in Remote Bridges) will be granted access. Select Enabled to enable WDS restriction. Only those bridges listed in Remote Bridges will be granted access.

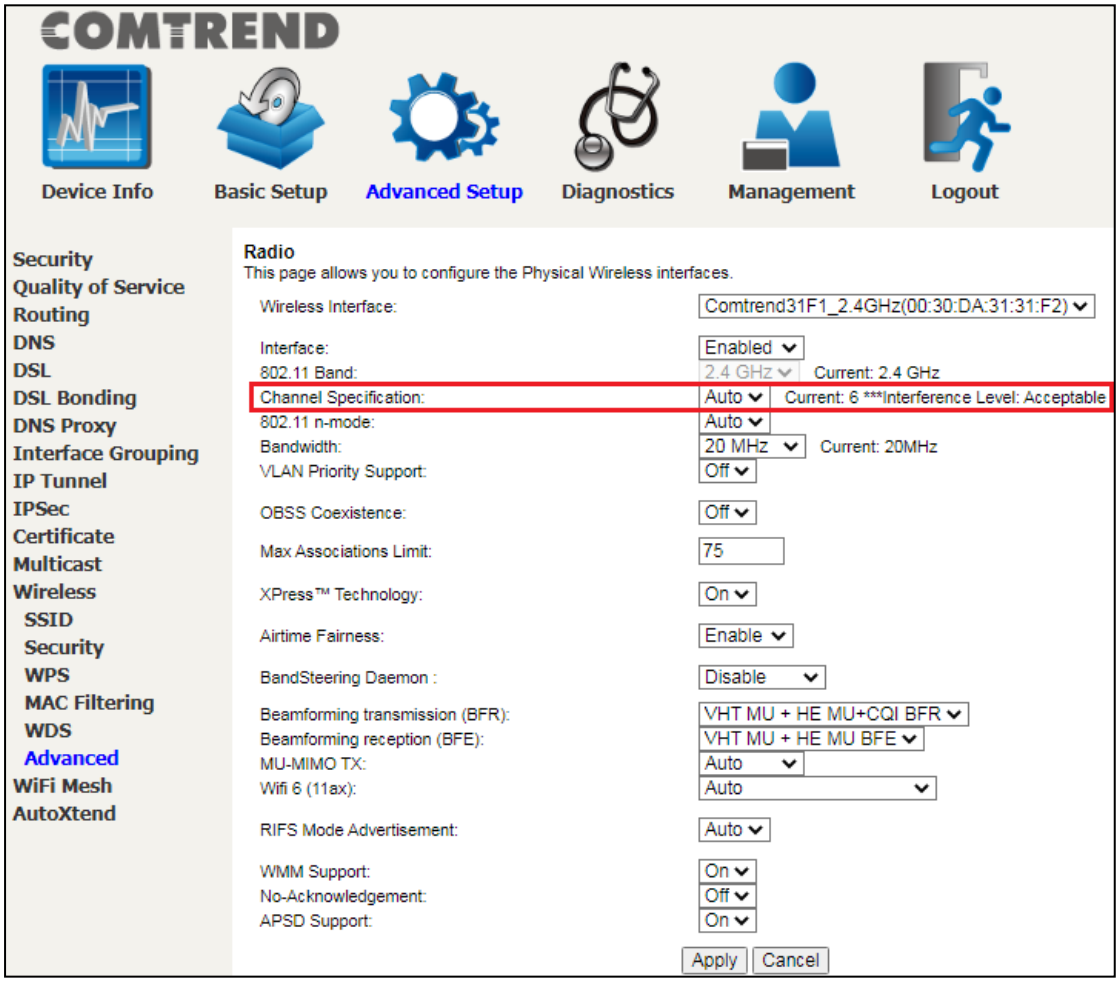
Link Direction Interval	Set the WDS link detection interval in seconds. Leave blank or set to zero to disable the detection.

Note: With reference to the above setup, please ensure that the conditions below are met, and both devices are rebooted afterwards:

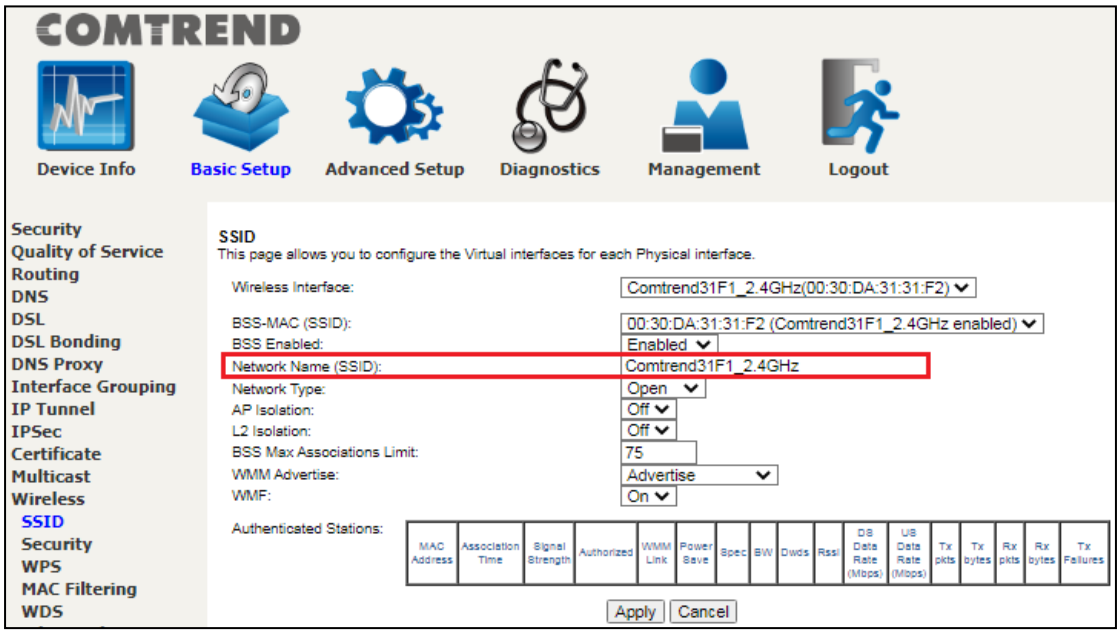
1. Ensure that the first Comtrend device (home router) does not use the same IP address as the second Comtrend wireless device (wireless bridge). See section 5.3 LANfor details on how to change the IP address.



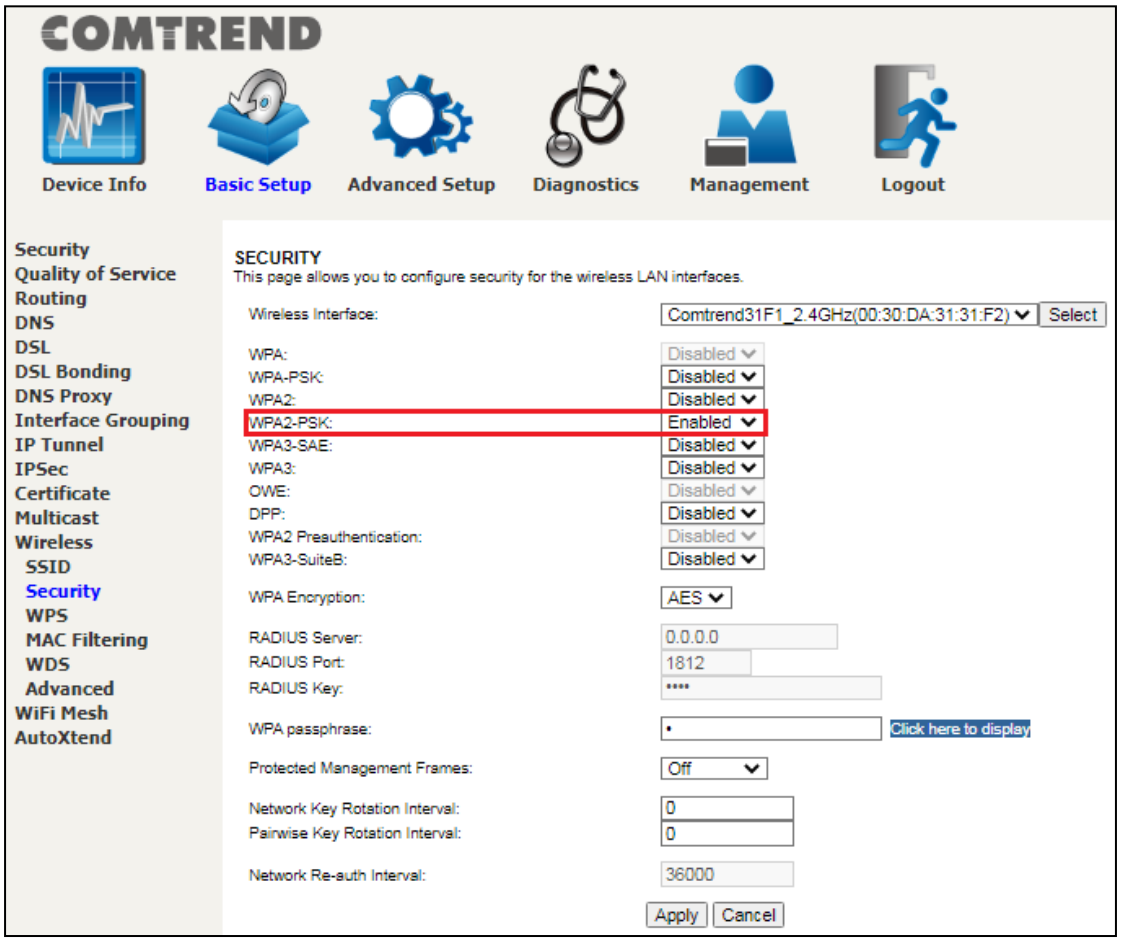
2. Both devices need to have the same fixed channel. See section 6.13.6 Advanced for details.



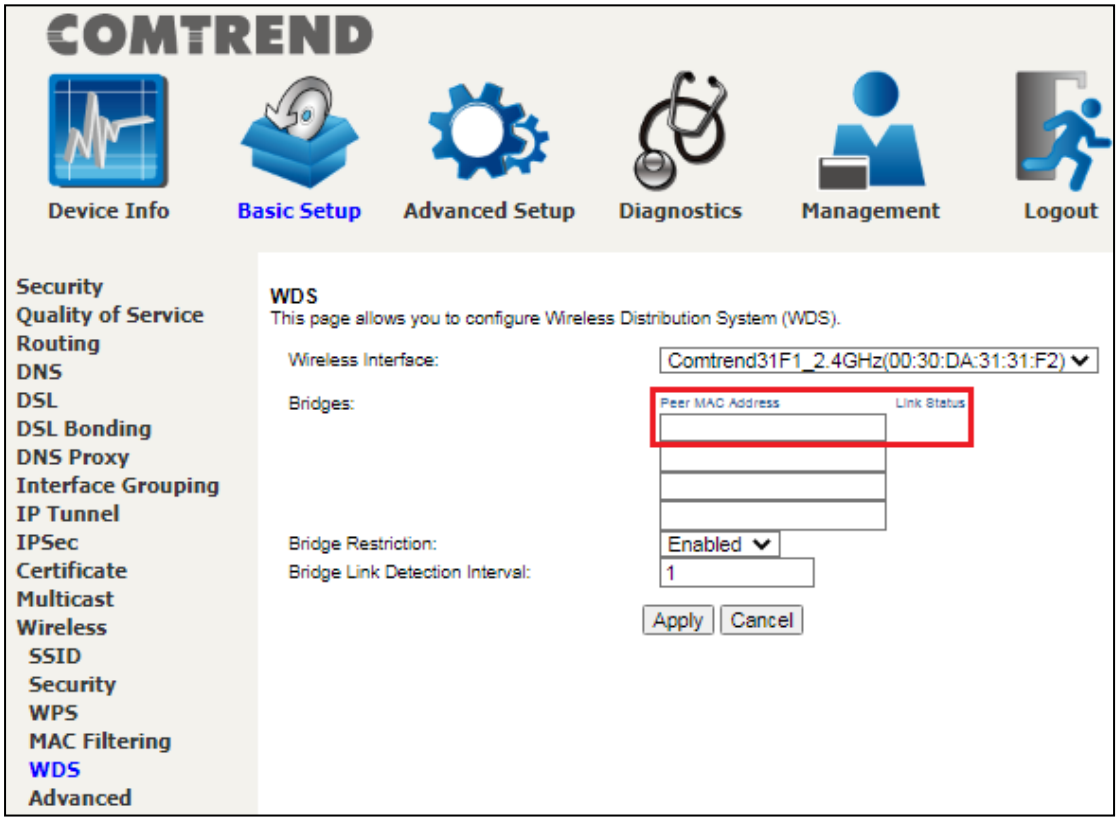
3. Both devices need to have a (different) fixed access SSID (Network Name). See section 6.13.1 SSID for details.



4. Both devices need to have WPA2-PSK enabled. See section 6.13.2 Security for details.



5. Both devices (A & B) need to have each other's MAC address. See section 6.13.5 WDS for details.

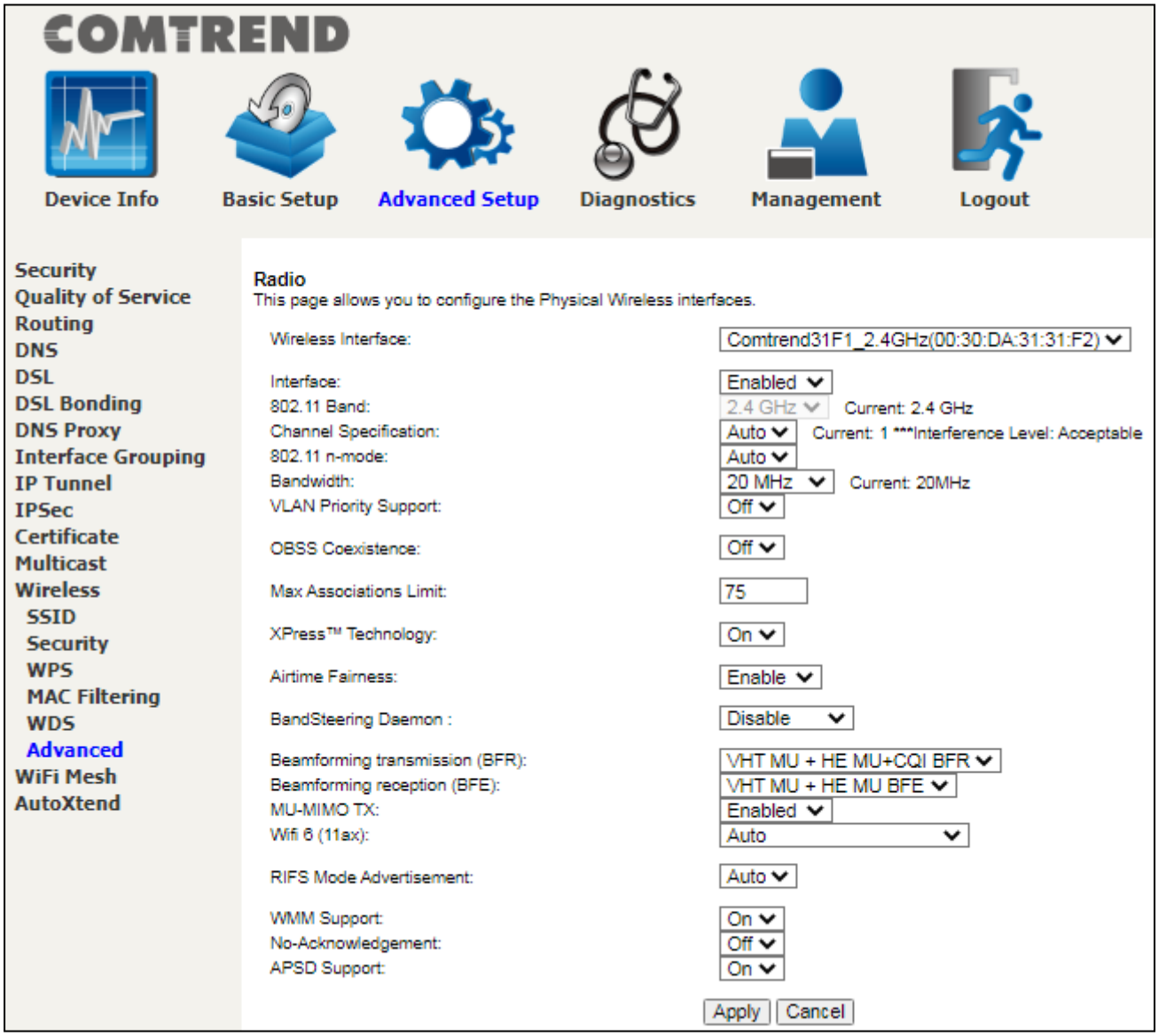


6. Now make sure to reboot both devices. See section 8.9 Reboot for details.

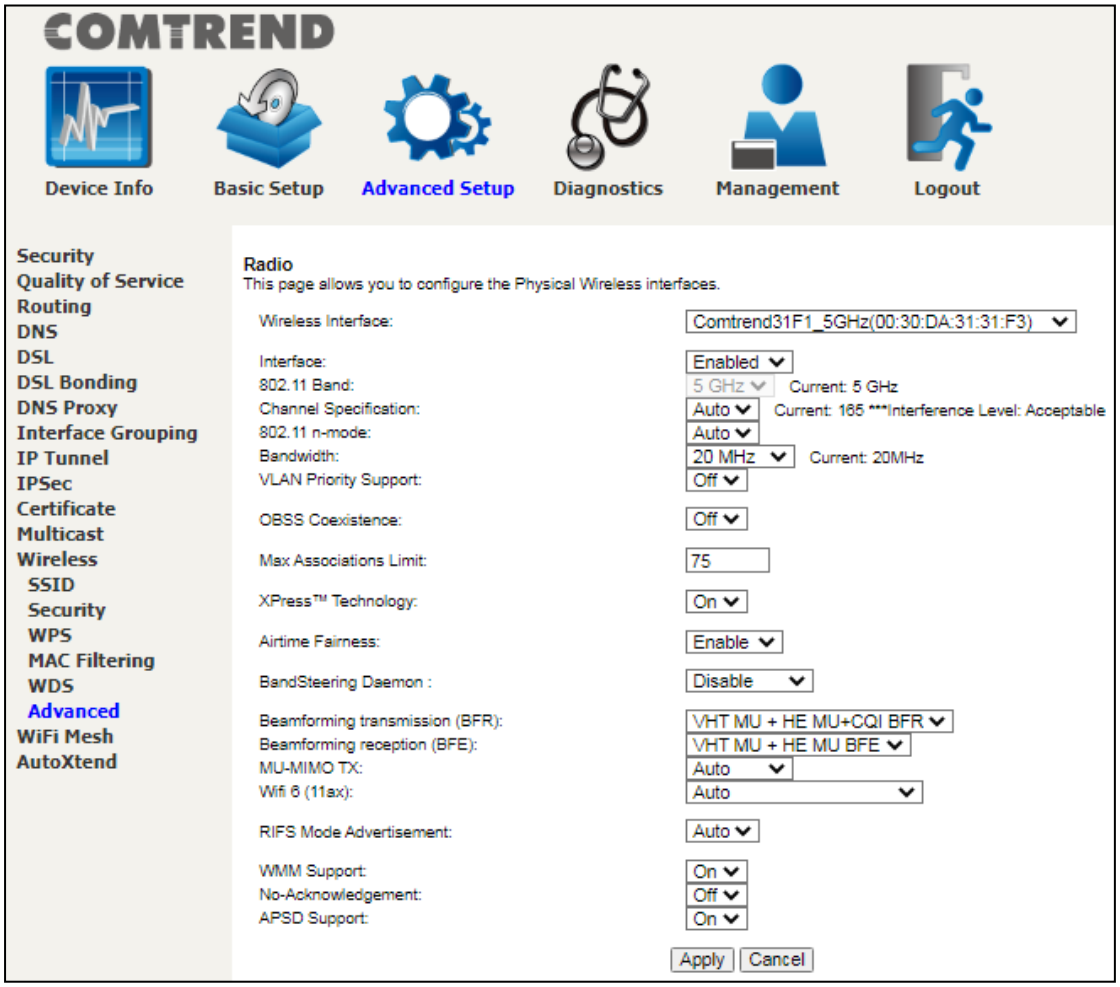
6.13.6 Advanced

This page allows you to configure the Physical Wireless interfaces.

2.4GHz

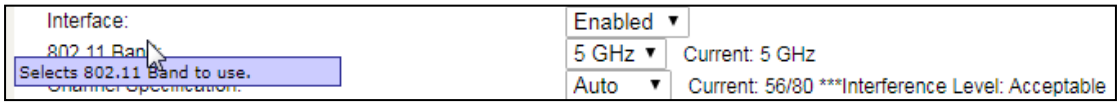


5GHz



Click the **Apply** button to apply your changes.

For information on each parameter, move the cursor over the parameter that you are interested in (as shown here).



The descriptions are also shown below.

Item	Description
Wireless Interface	Select which wireless interface to configure
Interface	Enable/Disable the wireless interface
802.11 Band	Select the 802.11 band to use
Channel Specification	Select a channel specification
802.11 n-mode	Enable/Disable 802.11N support

Bandwidth	Select channel bandwidth
VLAN Priority Support	Advertise packet priority using VLAN tag
OBSS Coexistence	Enable/Disable overlapping BSS coexistence aka 20/40 coex
Max Associations Limit	Set the number of associations the driver should accept
Xpress Technology	Enable/Disable Xpress mode
Airtime Fairness	Enable/Disable airtime fairness between multiple links
BandSteering Deamon	This is a function that automatically steers anyone connecting to a wireless network to the best available frequency band (e.g. from 5G to 2.4G or vice versa) providing an optimized performance for the client. Please note that this feature is not supported in this software version. Default is Disable Select Standalone to enable BandSteering
Beamforming transmission (BFR)	This is a versatile technique for signal transmission from a number of antennas to one or multiple users. In wireless networks it increases signal power for the intended user and reduces interference to non-intended users. VHT MU BFR: Wi-Fi 5 Multi User Beamforming transmission HE MU BFR: Wi-Fi 6 Multi User Beamforming transmission VHT MU + HE MU BFR: Wi-Fi 5 & Wi-Fi 6 Multi User Beamforming transmission Disabled - Disables beamforming transmission
Beamforming reception (BFE)	This is a versatile technique for signal reception from a number of antennas to one or multiple users. In wireless networks it increases signal power for the intended user and reduces interference to non-intended users. VHT MU BFE: Wi-Fi 5 Multi User Beamforming reception HE MU BFE: Wi-Fi 6 Multi User Beamforming reception VHT MU + HE MU BFE: Wi-Fi 5 & Wi-Fi 6 Multi User Beamforming reception Disabled - Disables beamforming reception

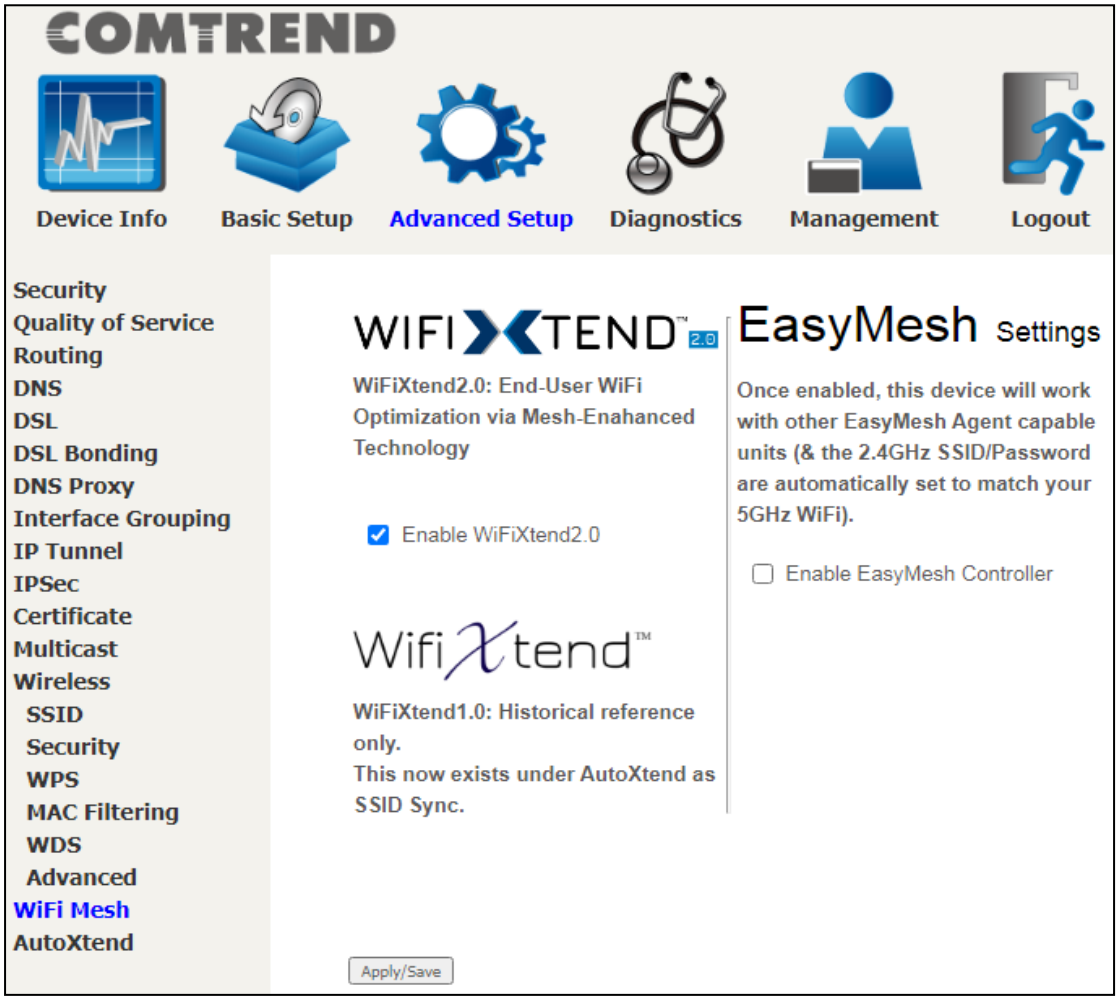
MU-MIMO TX	(MU) Multi-user MIMO transmission is a set of multiple-input and multiple-output technologies for multipath wireless communication, in which multiple users or terminals, each radioing over one or more antennas, communicate with one another. Client devices that support Wi-Fi 6 are highly recommended to enable this feature. Disabled: Disables MU-MIMO transmission Note: Disabling MU-MIMO TX, will also disable HE (Wi-Fi 6) MU-MIMO Enabled: Enables MU-MIMO transmission Auto: In this mode of operation, the Access Point will detect the wireless stations currently present in the network to determine the operation mode
Wifi 6 (11ax)	Control Wifi 6 features
RIFS Mode Advertisement	Select the RIFS (Reduced Inter-Frame Spacing) mode to advertise in beacons and probe responses
WMM Support	Enable/Disable WMM support
No-Acknowledgement	Enable/Disable EMM No-acknowledgement
APSD Support	Enable/Disable Automatic Power Save Technology

6.14 WiFi Mesh

WiFiXtend
A Comtrend proprietary WiFi Mesh solution that makes the slave devices automatically synchronize, and makes slave devices choose the best uplink path in a covered network environment.

EasyMesh
The Wi-Fi EasyMesh defines the control protocols between APs, mechanisms to route traffic within the network, and the data objects necessary to enable easy onboarding, provisioning, control, and automated management of APs in a Wi-Fi EasyMesh network.

Wi-Fi EasyMesh networks use a controller to manage the network, with agent APs connected to it.



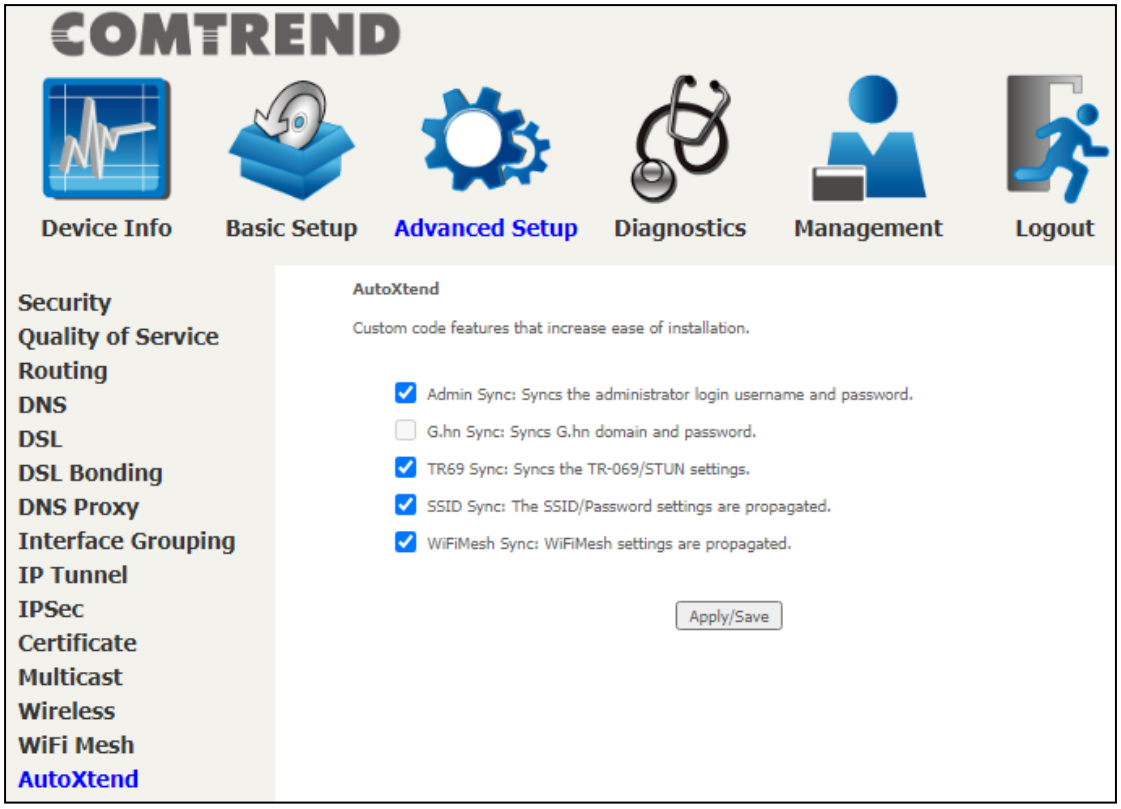
Once you have decided to use **WifiXtend** or **EasyMesh** follow the instructions below.

Check the checkbox and click the **Apply/Save** button to enable **WifiXtend.**

To enable **EasyMesh**, check the checkbox and click the **Apply/Save** button. Once enabled, this device will work with other EasyMesh Agent capable units (& the 2.4GHz SSID/Password are automatically set to match your 5GHz WiFi).

6.15 AutoXtend

AutoXtend is a function to construct and optimize a mesh-network. To select information to synchronize with all mesh-network nodes, please check the desired item and click the **Apply/Save** button.



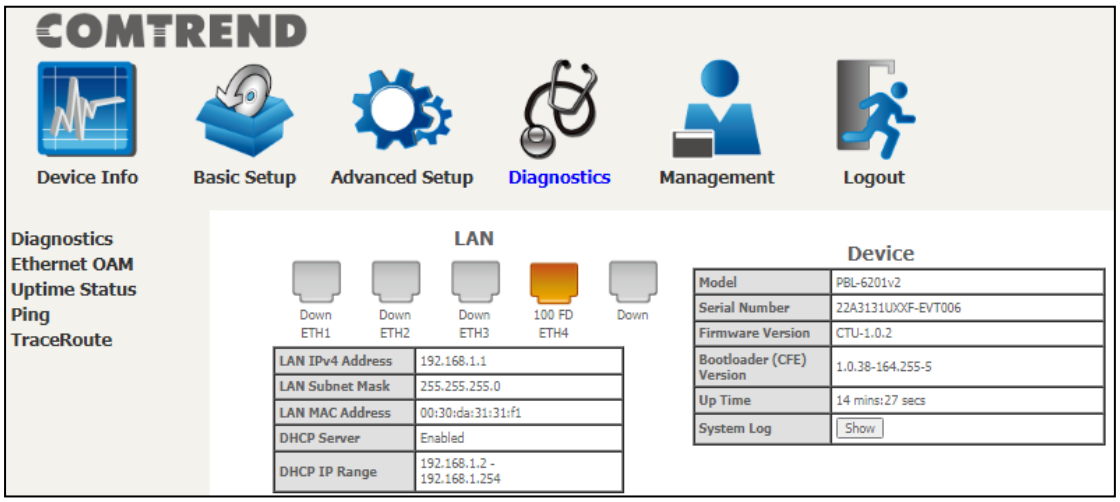
To enable the AutoXtend features, check the required checkboxes and click the **Apply/Save** button.

Chapter 7 Diagnostics

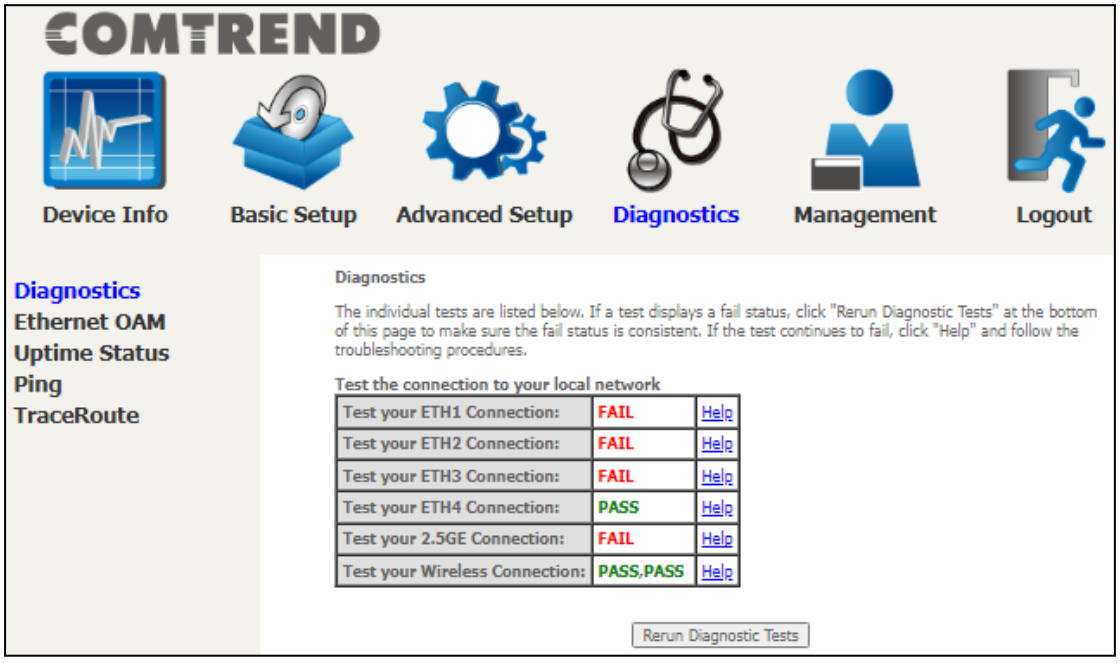
You can reach this page by clicking on the following icon located at the top of the screen.

7.1 Diagnostics – Individual Tests

The first Diagnostics screen is a dashboard that shows overall connection status.

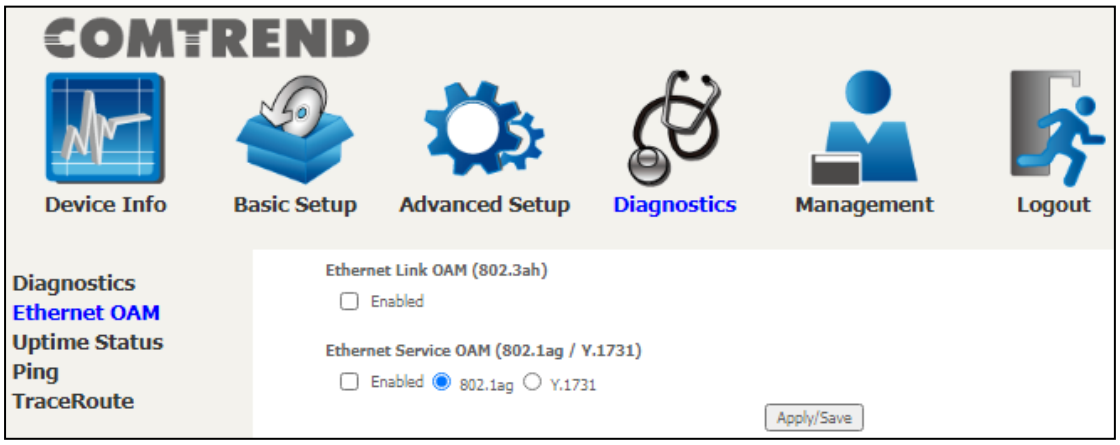


Click the Diagnostics Menu item on the left side of the screen to display the individual connections.

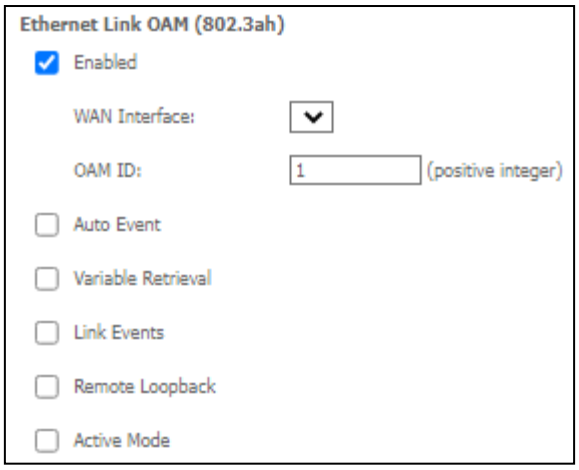


7.2 Ethernet OAM

The Ethernet OAM (Operations, Administration, Management) page provides settings to enable/disable 802.3ah, 802.1ag/Y1.731 OAM protocols.

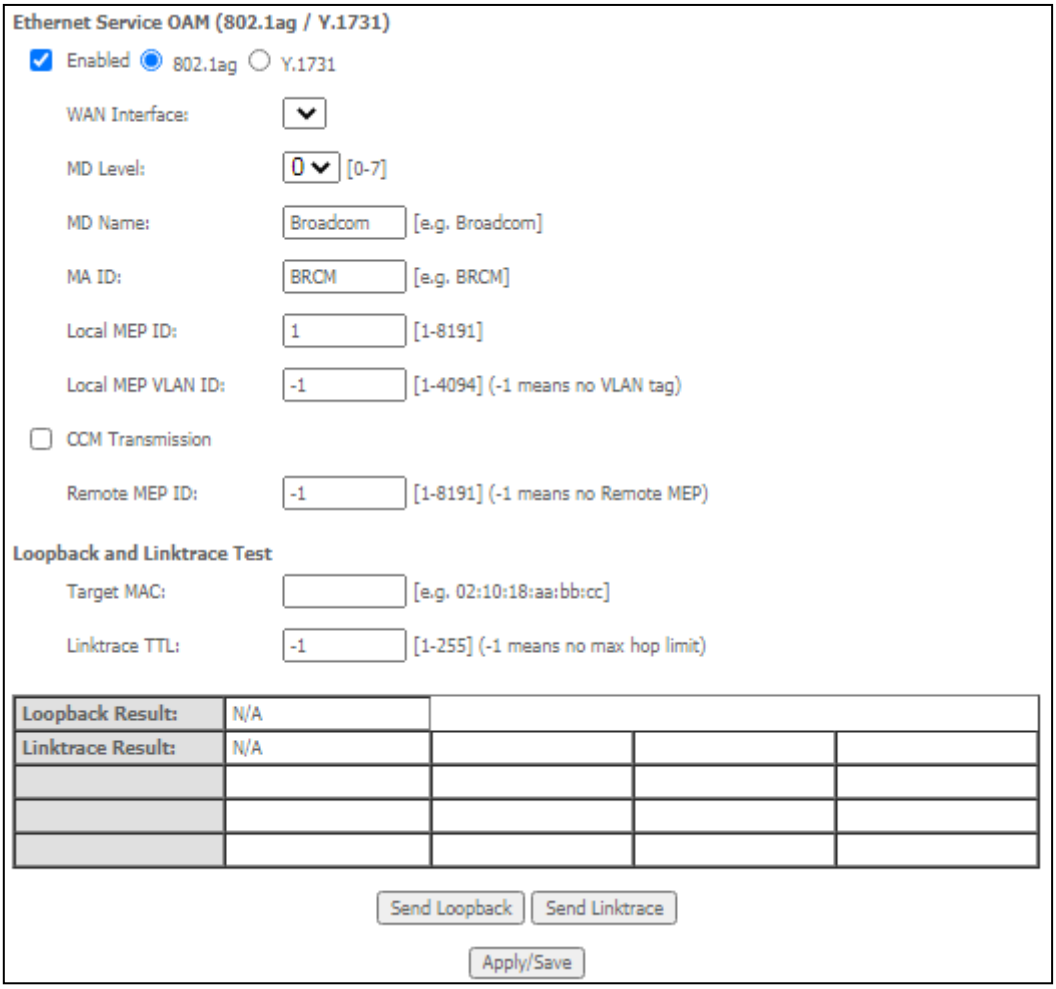


To enable Ethernet Link OAM (802.3 ah), click Enabled to display the full configuration list. At least one option must be enabled for 802.1ah.



Item	Description
WAN Interface	Select layer 2 WAN interface for outgoing OAM packets
OAM ID	OAM Identification number
Auto Event	Supports OAM auto event
Variable Retrieval	Supports OAM variable retrieval
Link Events	Supports OAM link events
Remote Loopback	Supports OAM remove loopback
Active mode	Supports OAM active mode

To enable Ethernet Service OAM (802.1ag/Y1731), click Enabled to display the full configuration list.



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

Item	Description
WAN Interface	Select from the list of WAN Interfaces to send OAM packets
MD Level	Maintenance Domain Level
MD Name	Maintenance Domain name
MA ID	Maintenance Association Identifier
Local MEP ID	Local Maintenance association End Point Identifier
Local MEP VLAN ID	VLAN IP used for Local Maintenance End point

Click CCM Transmission to enable CPE sending Continuity Check Message (CCM) continuously.

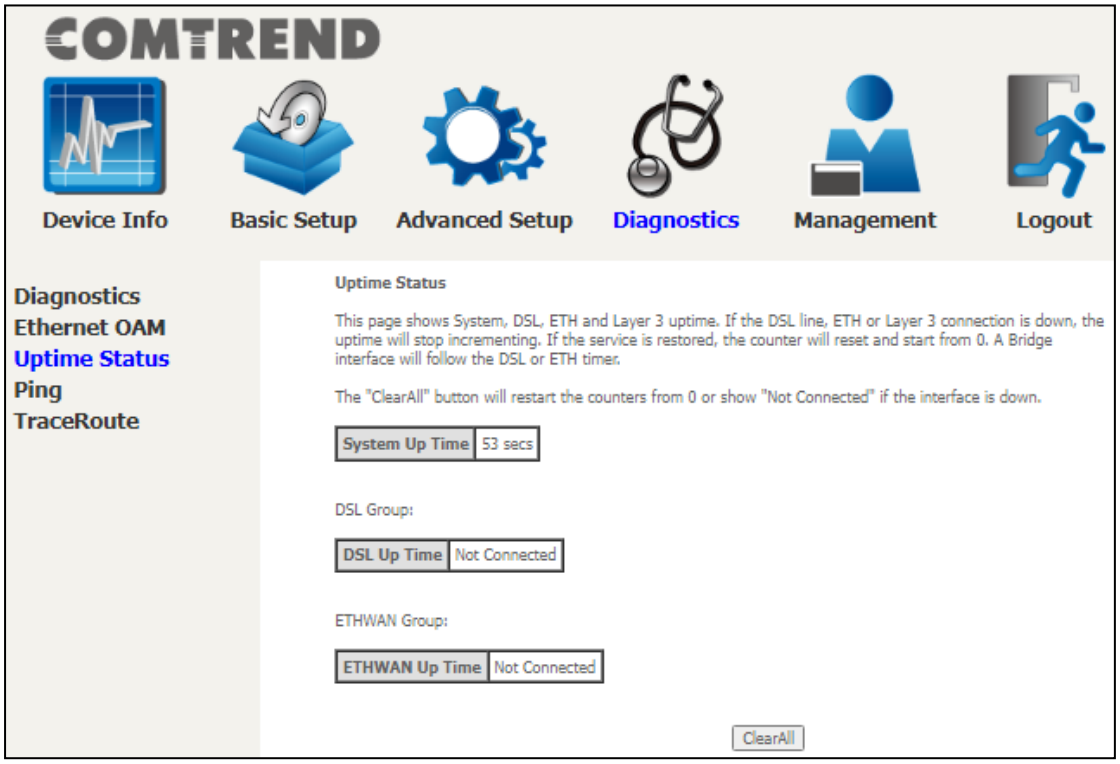
Remote MEP ID	Maintenance association End Point Identifier for the remote receiver

To perform Loopback/Linktrace OAM test, enter the Target MAC of the destination and click "Send Loopback" or "Send Linktrace" button.

Target MAC	MAC Address of the destination to send OAM loopback/linktrace packet
Linktrace TTL	Time to Live value for the loopback/linktrace packet

7.3 Uptime Status

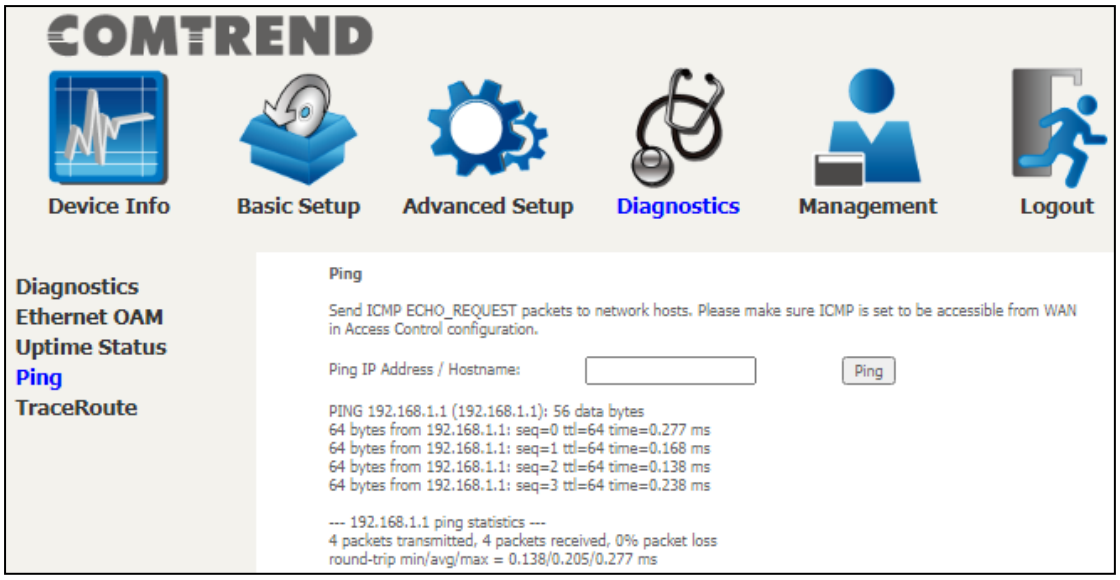
This page shows System, ETH and Layer 3 uptime. If the ETH or Layer 3 connection is down, the uptime will stop incrementing. If the service is restored, the counter will reset and start from 0. A Bridge interface will follow the ETH timer.



The "ClearAll" button will restart the counters from 0 or show "Not Connected" if the interface is down.

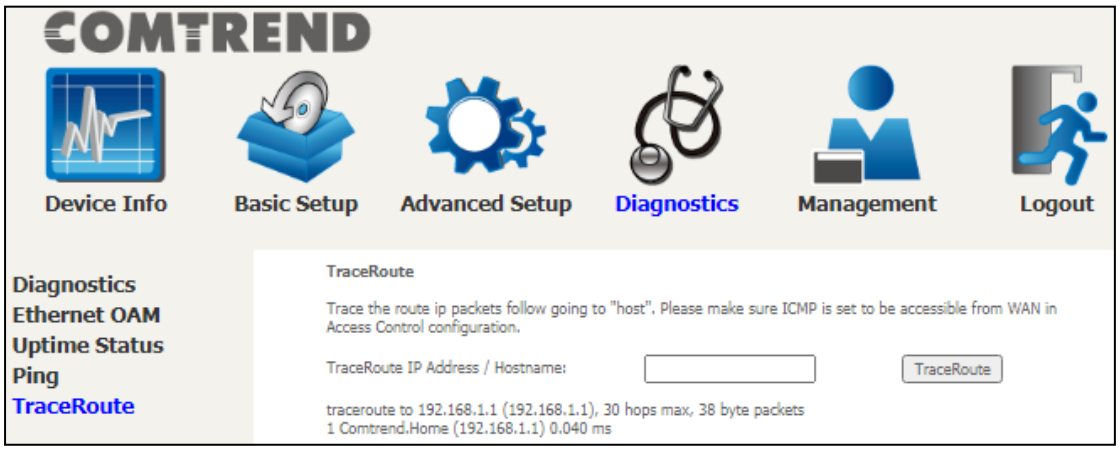
7.4 Ping

Input the IP address/hostname and click the **Ping** button to execute ping diagnostic test to send the ICMP request to the specified host.



7.5 Trace Route

Input the IP address/hostname and click the **TraceRoute** button to execute the trace route diagnostic test to send the ICMP packets to the specified host.



Chapter 8 Management

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

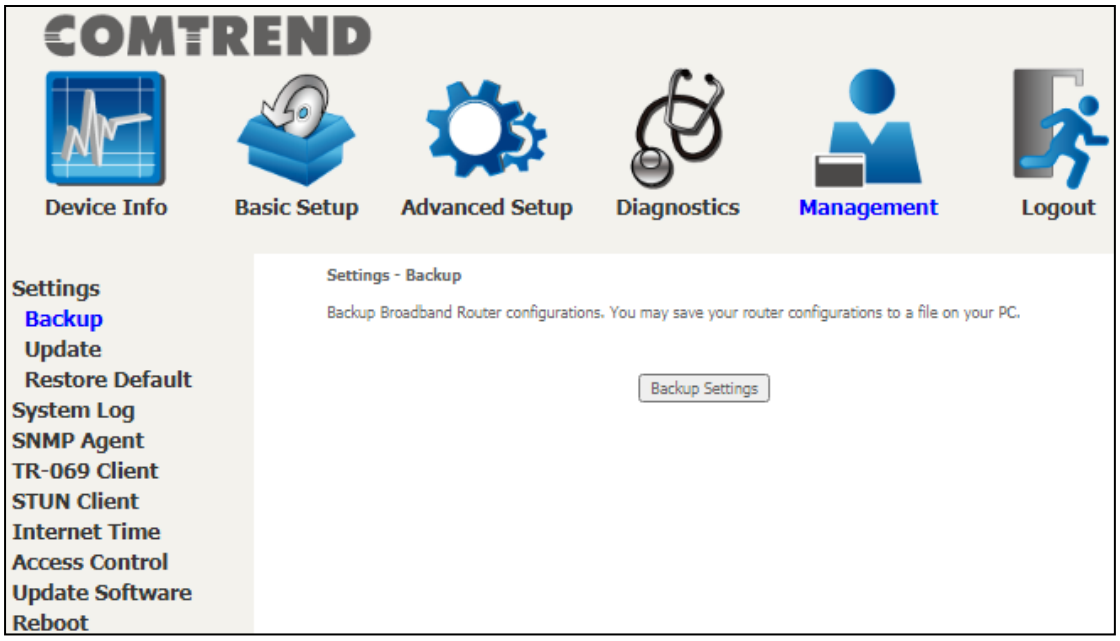
The Management menu has the following maintenance functions and processes:

8.1 Settings

This includes Backup Settings, Update Settings, and Restore Defaultscreens.

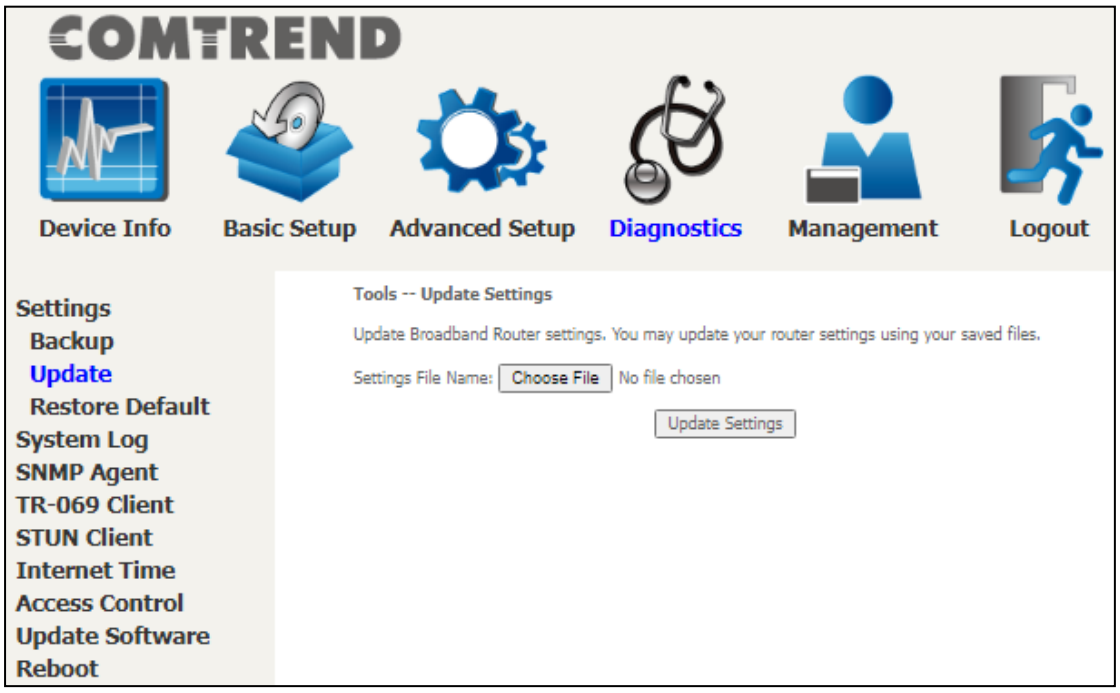
8.1.1 Backup Settings

This option recovers configuration files previously saved using **Backup Settings**. Click the Choose File button to locate the backup file. Then click the **Update Settings** button to update your device settings.



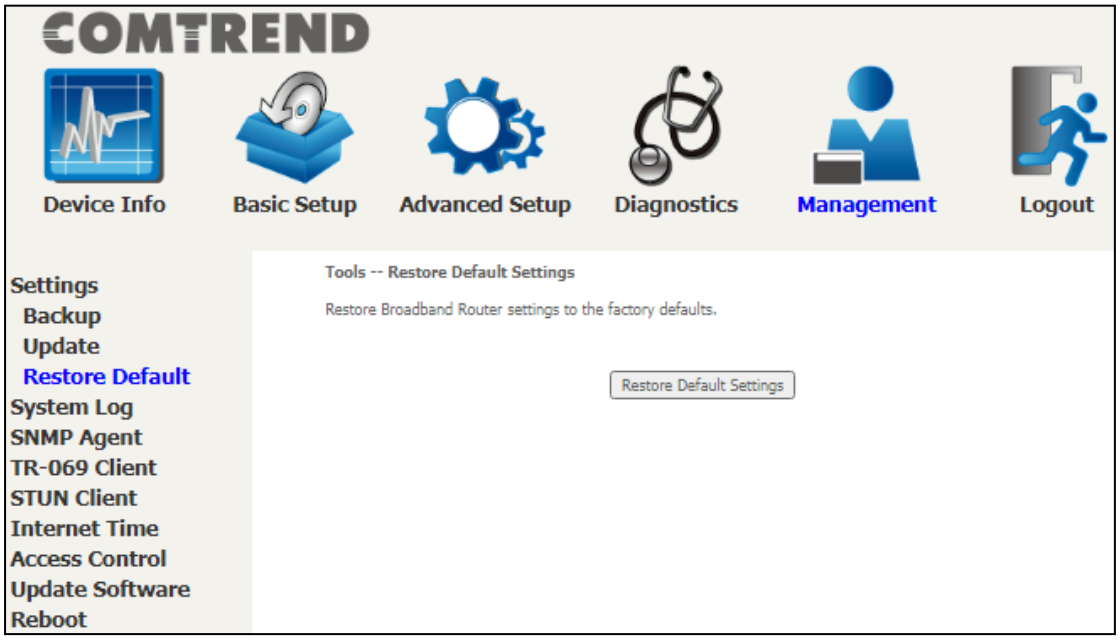
8.1.2 Update Settings

This option recovers configuration files previously saved using **Backup Settings**. Click the **Choose File** button to search for the file, then click **Update Settings** to recover settings.

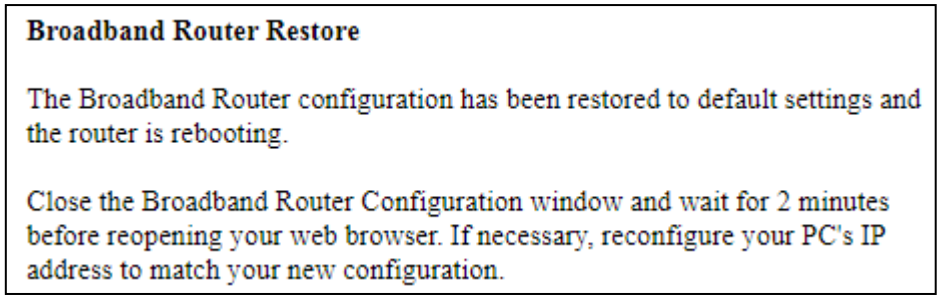


8.1.3 Restore Default

Click **Restore Default Settings** to restore factory default settings.



After **Restore Default Settings** is clicked, the following screen appears.



Close the browser and wait for 2 minutes before reopening it. It may also be necessary, to reconfigure your PC IP configuration to match any new settings.

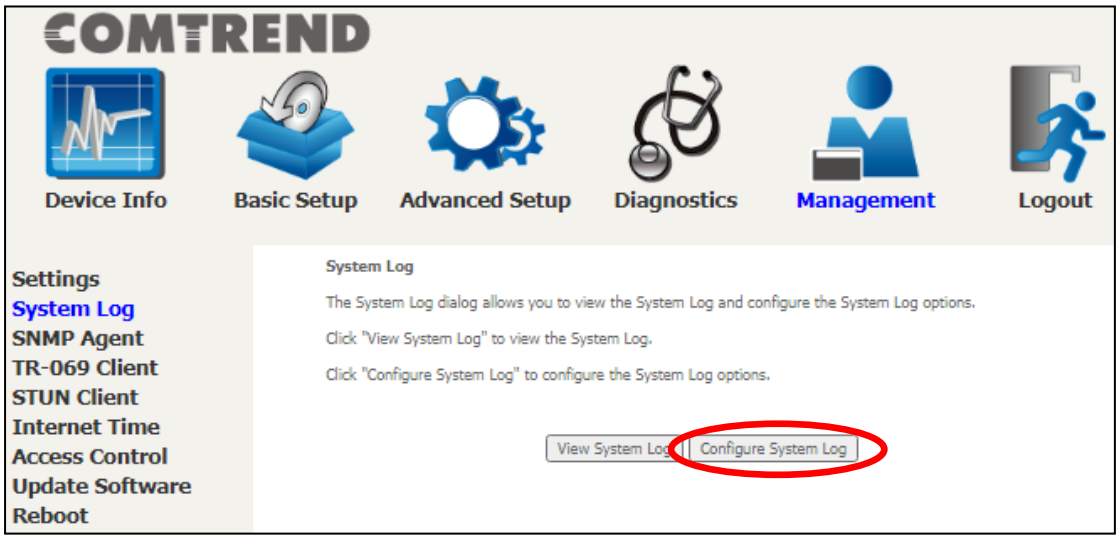
NOTE:	This entry has the same effect as the **Reset** button. The PBL-6201v2 board hardware and the boot loader support the reset to default. If the **Reset** button is continuously pressed for more than 10 seconds, the current configuration data will be erased. If the **Reset** button is continuously pressed for more than 60 seconds, the boot loader will erase all configuration data saved in flash memory and enter bootloader mode.

8.2 System Log

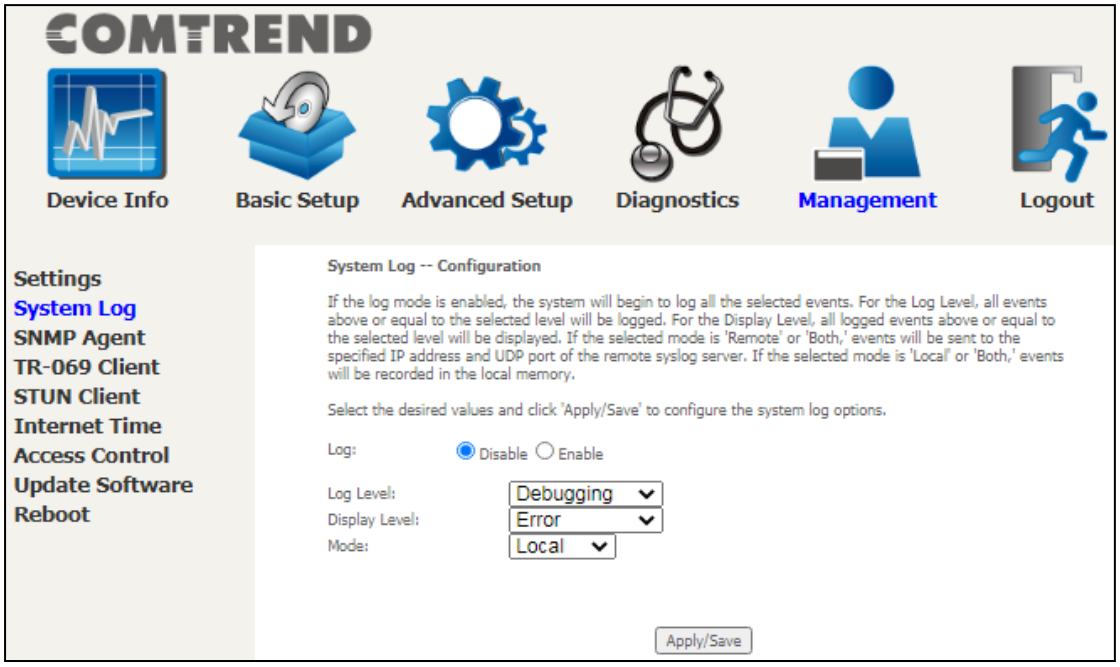
This function allows a system log to be kept and viewed upon request.

Follow the steps below to configure, enable, and view the system log.

STEP 1: Click **Configure System Log**, as shown below (circled in **Red**).



STEP 2: Select desired options and click **Apply/Save**.

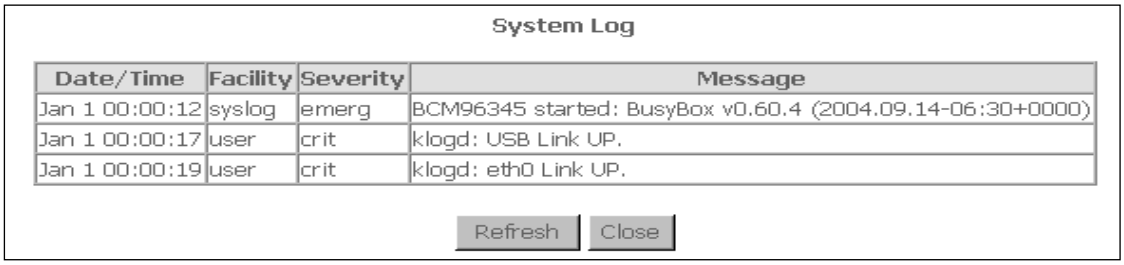


Consult the table below for detailed descriptions of each system log option.

Item	Description
Log	Indicates whether the system is currently recording events. The user can enable or disable event logging. By default, it is disabled. To enable it, select the **Enable** radio button and then click **Apply/Save**.

Log Level	Allows you to configure the event level and filter out unwanted events below this level. The events ranging from the highest critical level "Emergency" down to this configured level will be recorded to the log buffer on the PBL-6201v2 SDRAM. When the log buffer is full, the newer event will wrap up to the top of the log buffer and overwrite the old event. By default, the log level is "Debugging", which is the lowest critical level. The log levels are defined as follows: • Emergency = system is unusable • Alert = action must be taken immediately • Critical = critical conditions • Error = Error conditions • Warning = normal but significant condition • Notice= normal but insignificant condition • Informational= provides information for reference • Debugging = debug-level messages Emergency is the most serious event level, whereas Debugging is the least important. For instance, if the log level is set to Debugging, all the events from the lowest Debugging level to the most critical level Emergency level will be recorded. If the log level is set to Error, only Error and the level above will be logged.
Display Level	Allows the user to select the logged events and displays on the **View System Log** window for events of this level and above to the highest Emergency level.
Mode	Allows you to specify whether events should be stored in the local memory, or be sent to a remote system log server, or both simultaneously. If remote mode is selected, view system log will not be able to display events saved in the remote system log server. When either Remote mode or Both mode is configured, the WEB UI will prompt the user to enter the Server IP address and Server UDP port.

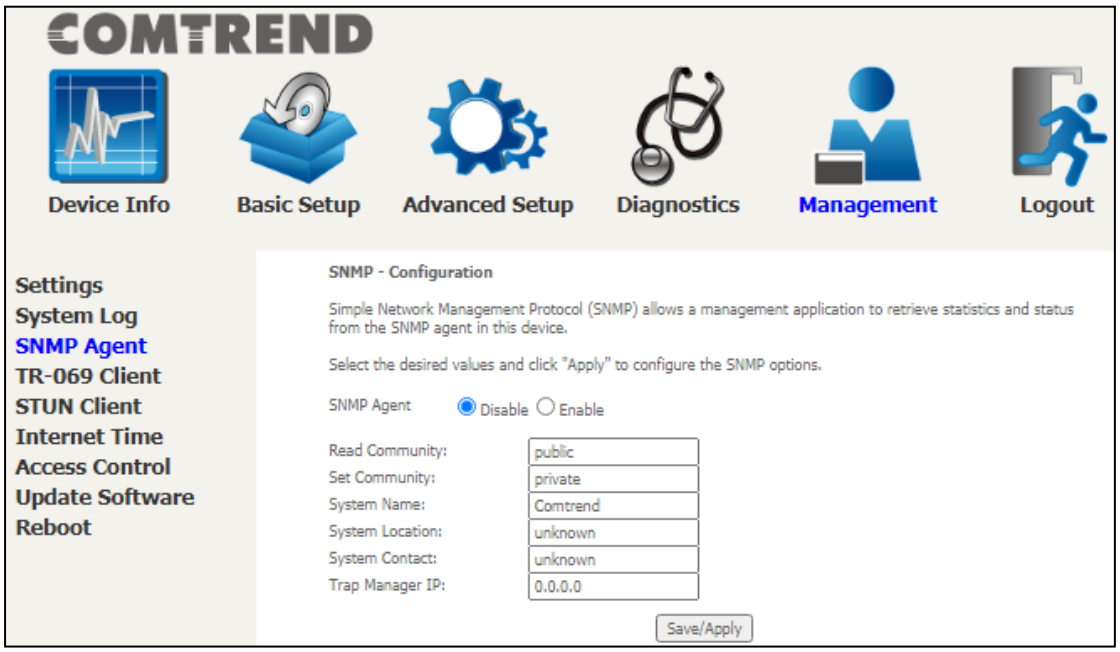
STEP 3: Click **View System Log**. The results are displayed as follows.



Click the **Refresh** button to update the system log and click the **Close** button to remove the current log from the screen.

8.3 SNMP Agent

Simple Network Management Protocol (SNMP) allows a management application to retrieve statistics and status from the SNMP agent in this device. Select the **Enable** radio button, configure options, and click **Save/Apply** to activate SNMP.

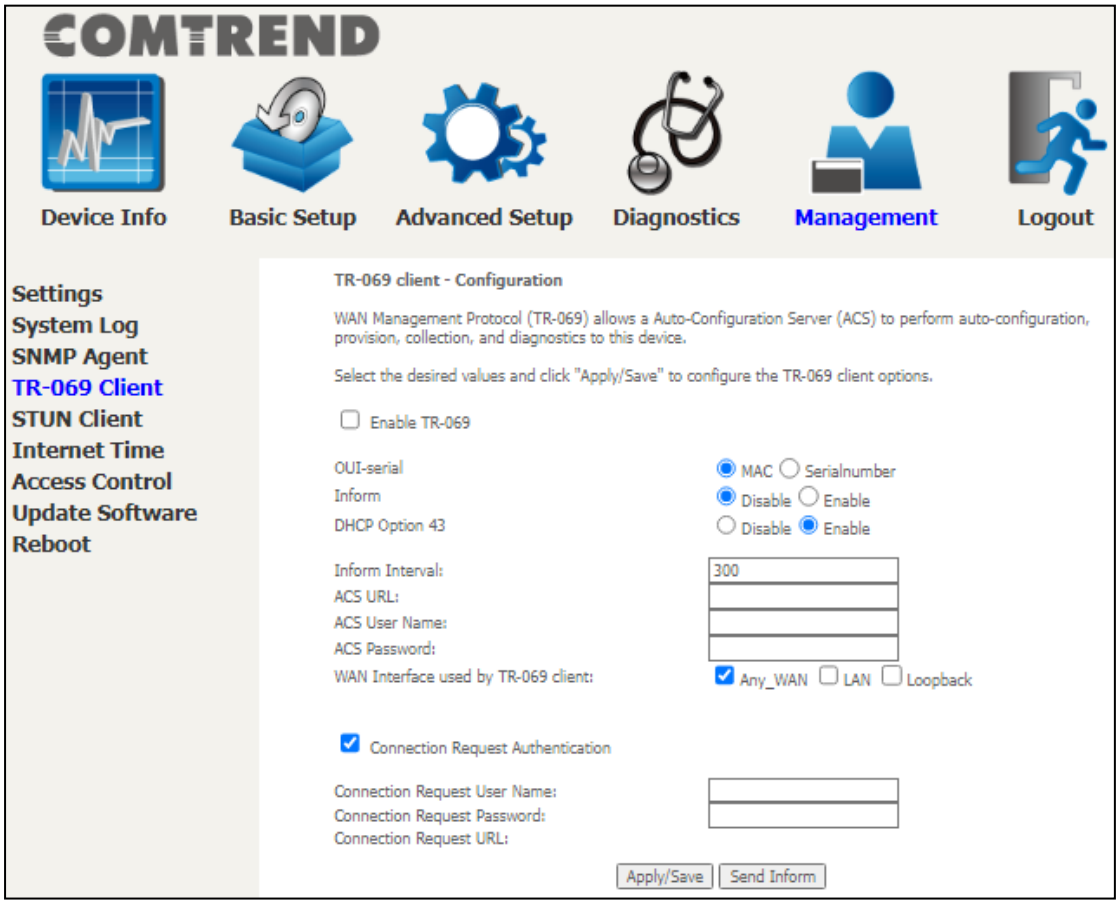


The settings shown above are described below.

Item	Description
SNMP Agent	Enable or Disable the SNMP Agent
Read Community	Default is "public"
Set Community	Default is "private"
System Name	Default is "Comtrend"
System Location	Describes the location of the system (user defined)
System Contact	Describes who should be contacted about the host the agent is running on (user defined)
Trap Manager IP	Trap request supports to monitor and alarm via port 162 from Agent

8.4 TR-069 Client

WAN Management Protocol (TR-069) allows an Auto-Configuration Server (ACS) to perform auto-configuration, provision, collection, and diagnostics to this device. Select desired values and click **Apply/Save** to configure TR-069 client options.



The table below is provided for ease of reference.

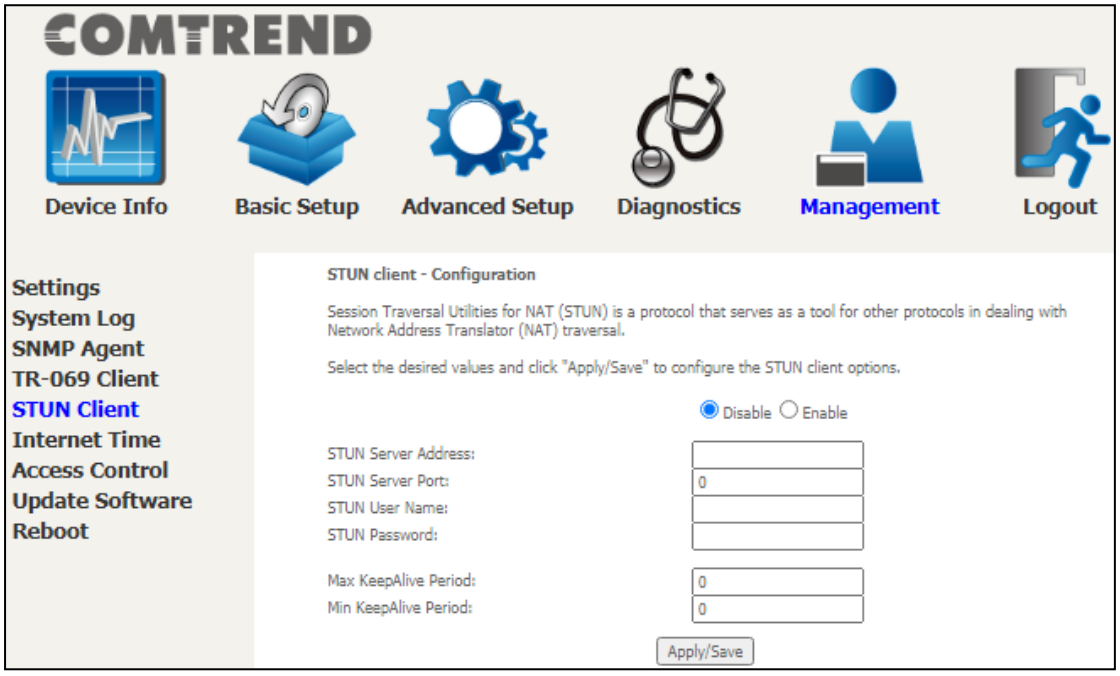
Item	Description
Enable TR-069	Tick the checkbox ☑ to enable.
OUI-serial	The serial number used to identify the CPE when making a connection to the ACS using the CPE WAN Management Protocol. Select MAC to use the router's MAC address as serial number to authenticate with the ACS or select serial number to use the router's serial number.
Inform	Disable/Enable TR-069 client on the CPE.
DHCP Option 43	Enable/Disable using DHCP option 43 received from WAN server to configure ACS URL.

Inform Interval	The duration in seconds of the interval for which the CPE MUST attempt to connect with the ACS and call the Inform method.
ACS URL	URL for the CPE to connect to the ACS using the CPE WAN Management Protocol. This parameter MUST be in the form of a valid HTTP or HTTPS URL. An HTTPS URL indicates that the ACS supports SSL. The "host" portion of this URL is used by the CPE for validating the certificate from the ACS when using certificate-based authentication.
ACS User Name	Username used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This username is used only for HTTP-based authentication of the CPE.
ACS Password	Password used to authenticate the CPE when making a connection to the ACS using the CPE WAN Management Protocol. This password is used only for HTTP-based authentication of the CPE.
WAN Interface used by TR-069 client	Choose Any_WAN, LAN, Loopback or a configured connection.
Connection Request	
Authentication	Tick the checkbox ☑ to enable.
User Name	Username used to authenticate an ACS making a Connection Request to the CPE.
Password	Password used to authenticate an ACS making a Connection Request to the CPE.
URL	IP address and port the ACS uses to connect to the router.

The **Send Inform** button forces the CPE to establish an immediate connection to the ACS.

8.5 STUN Client

Session Traversal Utilities for NAT (STUN) is a protocol that serves as a tool for other protocols in dealing with Network Address Translator (NAT) traversal.



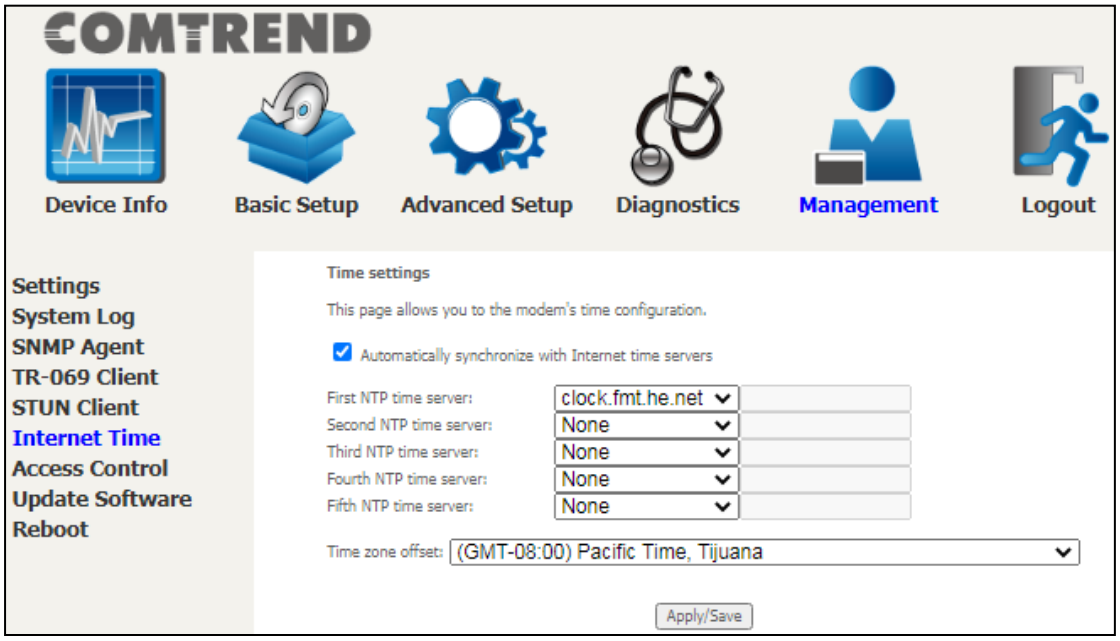
Select the desired values and click the **Apply/Save** button to configure the STUN client options.

The settings shown above are described below.

Item	Description
Disable/Enable	Disable/Enable STUN client.
STUN Server Address	IP address of the STUN server.
STUN Server Port	Service port of the STUN server.
STUN User Name	Account to link to the STUN server.
STUN Password	Password of said account to link to the STUN server.
Max KeepAlive Period	Maximum period to wait for a packet to be received from the STUN server to keep the link alive.
Min KeepAlive Period	Minimum period to send a packet to the STUN server to keep the link alive.

8.6 Internet Time

This option automatically synchronizes the router time with Internet timeservers. To enable time synchronization, tick the corresponding checkbox ☑, choose your preferred time server(s), select the correct time zone offset, and click **Apply/Save**.



NOTE: Internet Time must be activated to use. See 5.5 Parental Control. The internet time feature will not operate when the router is in bridged mode, since the router would not be able to connect to the NTP timeserver.

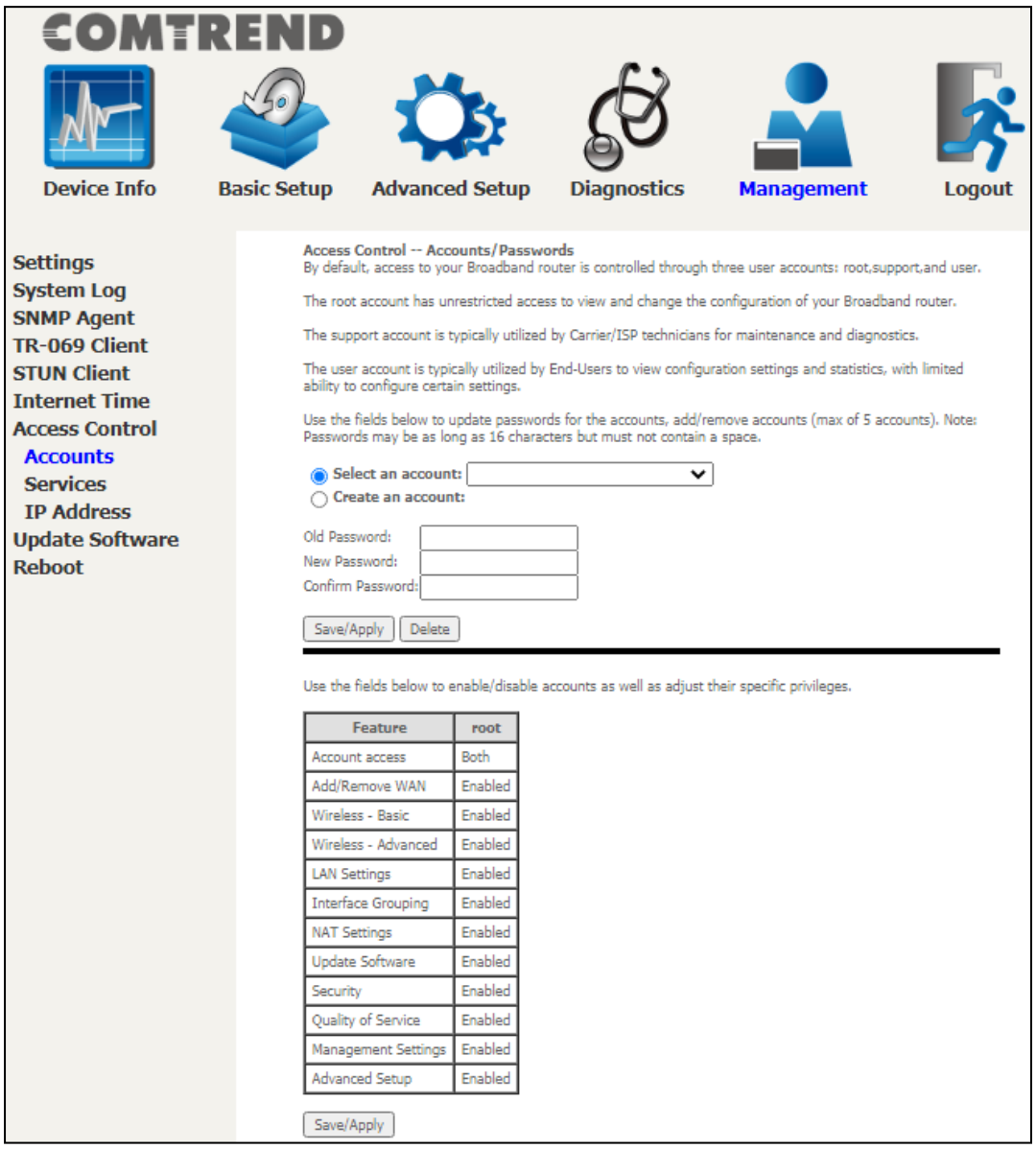
8.7 Access Control

8.7.1 Accounts

This screen is used to configure the user account access passwords for the device. Access to the PBL-6201v2 is controlled through the following user accounts:

- The root account has unrestricted access to view and change the configuration of your Broadband router.

Use the fields to update passwords for the accounts, add/remove accounts (max of 5 accounts) as well as adjust their specific privileges.

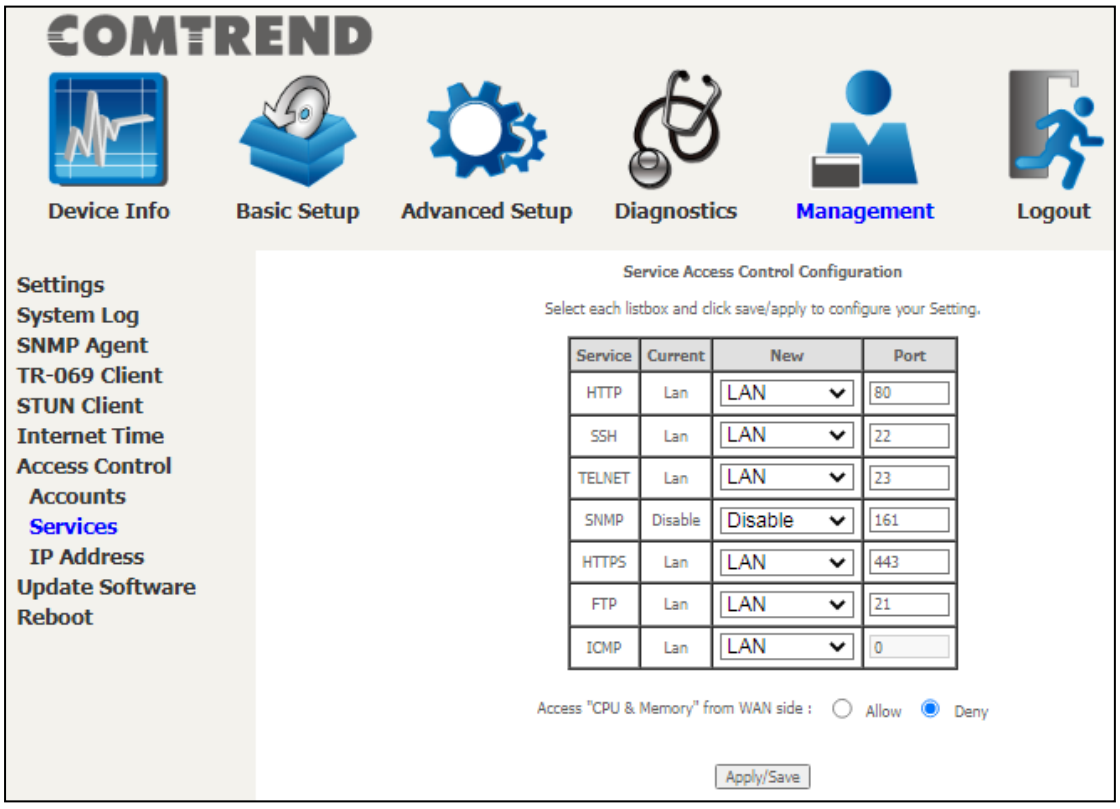


Note: Passwords may be as long as 16 characters but must not contain a space. Click **Save/Apply** to continue.

8.7.2 Services

The Services option limits or opens the access services over the LAN or WAN. These access services available are: HTTP, SSH, TELNET, SNMP, HTTPS, FTP, TFTP and ICMP. Enable a service by selecting its dropdown listbox. Click **Apply/Save** to activate.

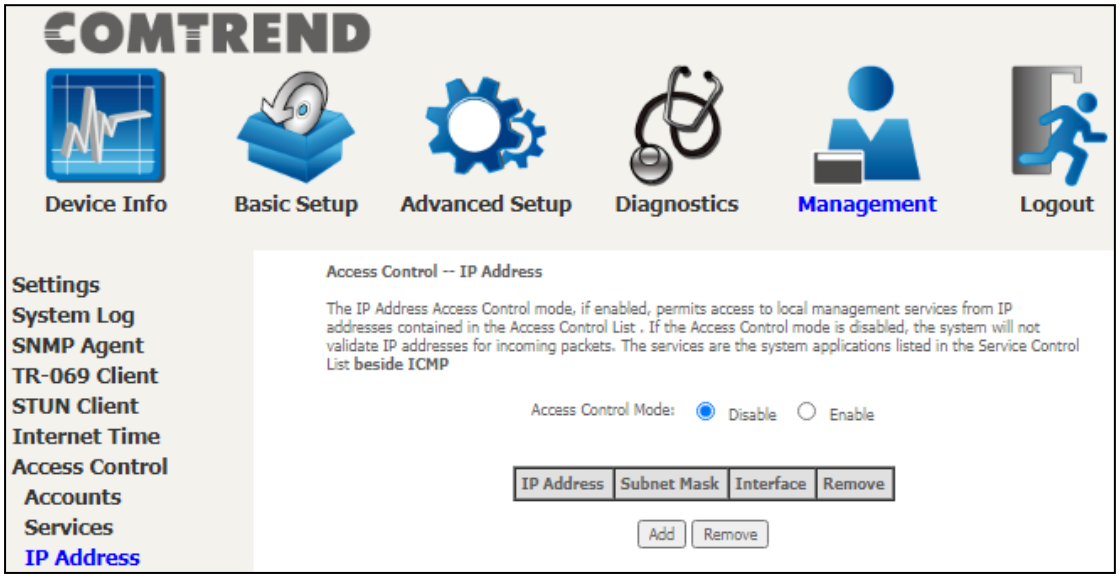
Access "CPU & Memory" from WAN side:This allows the WAN side to access the Device Info CPU & Memory page.



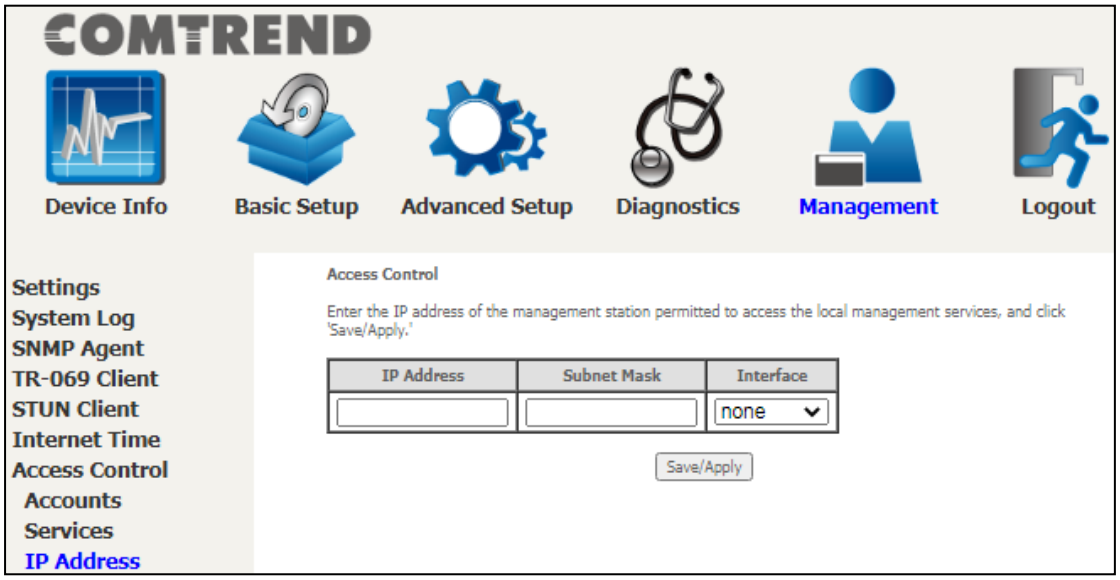
Please note that any Comtrend firmware upgrade will not modify any WiFi parameters (including the WiFi power setting). Comtrend's products follow the market's standard requirements.

8.7.3 IP Address

The IP Address Access Control mode, if enabled, permits access to local management services from IP addresses contained in the Access Control List. If the Access Control mode is disabled, the system will not validate IP addresses for incoming packets. The services are the system applications listed in the Service Control List **beside ICMP**.



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



Configure the address and subnet of the management station permitted to access the local management services, and click **Save/Apply**.

IP Address – IP address of the management station.

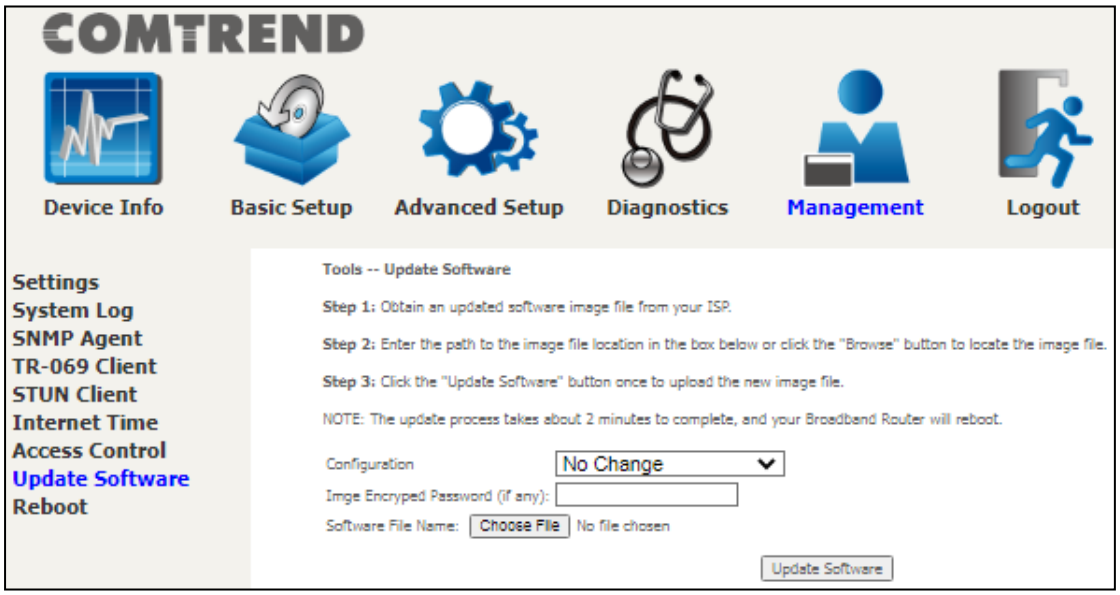
Subnet Mask – Subnet address for the management station.

Interface – Access permission for the specified address, allowing the address to access the local management service from none/lan/wan/lan&wan interfaces.

8.8 Update Software

This option allows for firmware upgrades from a locally stored file.

Please note that any Comtrend firmware upgrade will not modify any WiFi parameters (including the Wi-Fi power setting). Comtrend's products follow the market's standard requirements.



STEP 1: Obtain an updated software image file from your ISP.

STEP 2: Enter the path to the image file location in the box below or click the **Choose File** button to locate the image file.

Configuration options:

No change – upgrade software directly.

Erase current config – If the router has save_default configuration, this option will erase the current configuration and restore to save_default configuration after software upgrade.

Erase All – Router will be restored to factory default configuration after software upgrade.

Image Encrypted Password: Input the encryption password of the firmware image if the binary file was secured by the password. This option is applicable to users with a high security requirement.

STEP 3: Click the **Update Software** button once to upload and install the file.

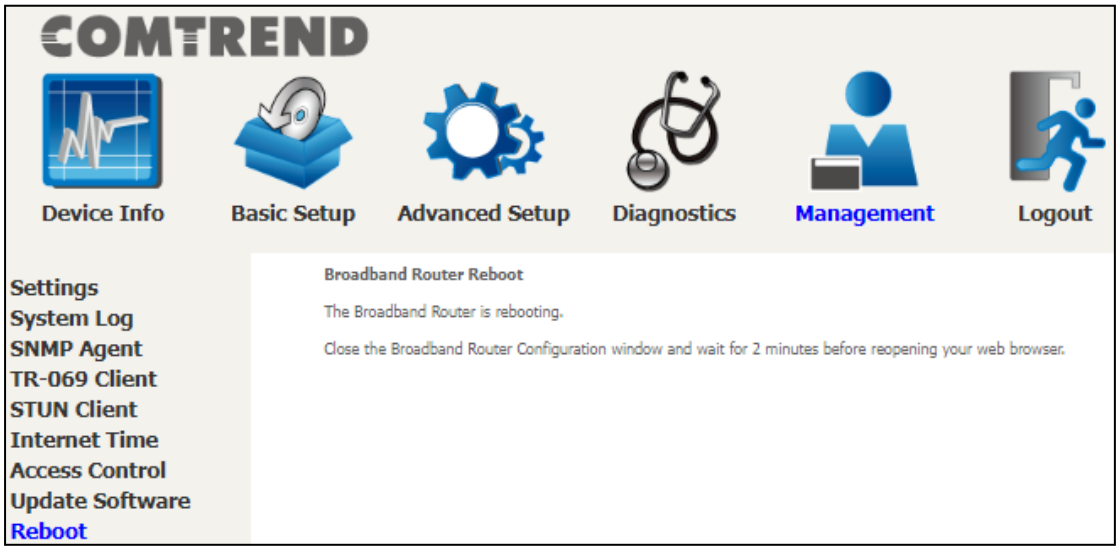
NOTE1: The update process will take about 2 minutes to complete. The device will reboot and the browser window will refresh to the default screen upon successful installation. It is recommended that you compare the **Software Version** on the Device Information screen with the firmware version installed, to confirm the installation was successful.

NOTE2: The Power LED indicates the status of firmware update progress. Please **DO NOT** power off the device when Power LED is flashing or the device will be damaged.

8.9 Reboot

To save the current configuration and reboot the router, click **Reboot**.

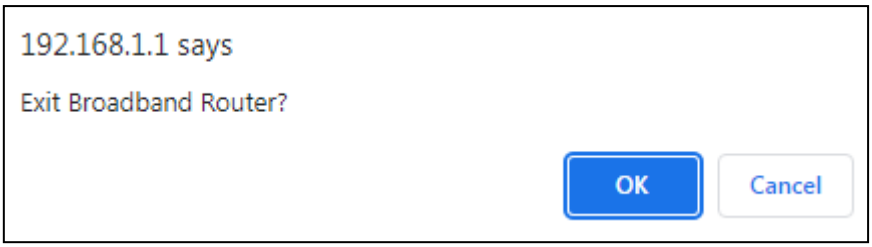
NOTE: You may need to close the browser window and wait for 2 minutes before reopening it. It may also be necessary, to reset your PC IP configuration.



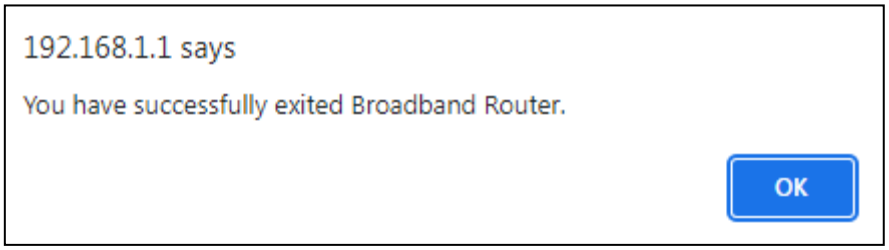
Chapter 9 Logout

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

When the following window pops up, click the **OK** button to exit the router.



Upon successful exit, the following message will be displayed.



Appendix A - Firewall

STATEFUL PACKET INSPECTION
Refers to an architecture, where the firewall keeps track of packets on each connection traversing all its interfaces and makes sure they are valid. This is in contrast to static packet filtering which only examines a packet based on the information in the packet header.

DENIAL OF SERVICE ATTACK
Is an incident in which a user or organization is deprived of the services of a resource they would normally expect to have. Various DoS attacks the device can withstand are ARP Attack, Ping Attack, Ping of Death, Land, SYN Attack, Smurf Attack, and Tear Drop.

TCP/IP/PORT/INTERFACE FILTER
These rules help in the filtering of traffic at the Network layer (i.e. Layer 3). When a Routing interface is created, **Enable Firewall** must be checked. Navigate to Advanced Setup → Security → IP Filtering.

OUTGOING IP FILTER
Helps in setting rules to DROP packets from the LAN interface. By default, if the Firewall is Enabled, all IP traffic from the LAN is allowed. By setting up one or more filters, specific packet types coming from the LAN can be dropped.

Example 1:	Filter Name	: Out_Filter1
	Protocol	: TCP
	Source IP address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 80
	Dest. IP Address	: NA
	Dest. Subnet Mask	: NA
	Dest. Port	: NA

This filter will Drop all TCP packets coming from the LAN with IP Address/Subnet Mask of 192.168.1.45/24 having a source port of 80 irrespective of the destination. All other packets will be Accepted.

Example 2:	Filter Name	: Out_Filter2
	Protocol	: UDP
	Source IP Address	: 192.168.1.45
	Source Subnet Mask	: 255.255.255.0
	Source Port	: 5060:6060
	Dest. IP Address	: 172.16.13.4
	Dest. Subnet Mask	: 255.255.255.0
	Dest. Port	: 6060:7070

This filter will drop all UDP packets coming from the LAN with IP Address / Subnet Mask of 192.168.1.45/24 and a source port range of 5060 to 6060, destined to 172.16.13.4/24 and a destination port range of 6060 to 7070.

INCOMING IP FILTER
Helps in setting rules to Allow or Deny packets from the WAN interface. By default, all incoming IP traffic from the WAN is Blocked, if the Firewall is Enabled. By setting up one or more filters, specific packet types coming from the WAN can be Accepted.

Example 1:

Filter Name	: In_Filter1
Protocol	: TCP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 80
Dest. IP Address	: NA
Dest. Subnet Mask	: NA
Dest. Port	: NA
Selected WAN interface	: br0

This filter will ACCEPT all TCP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 with a source port of 80, irrespective of the destination. All other incoming packets on this interface are DROPPED.

Example 2:

Filter Name	: In_Filter2
Protocol	: UDP
Policy	: Allow
Source IP Address	: 210.168.219.45
Source Subnet Mask	: 255.255.0.0
Source Port	: 5060:6060
Dest. IP Address	: 192.168.1.45
Dest. Sub. Mask	: 255.255.255.0
Dest. Port	: 6060:7070
Selected WAN interface	: br0

This rule will ACCEPT all UDP packets coming from WAN interface "br0" with IP Address/Subnet Mask 210.168.219.45/16 and a source port in the range of 5060 to 6060, destined to 192.168.1.45/24 and a destination port in the range of 6060 to 7070. All other incoming packets on this interface are DROPPED.

MAC LAYER FILTER

These rules help in the filtering of Layer 2 traffic. MAC Filtering is only effective in bridge mode. After a bridge mode connection is created, navigate to Advanced Setup → Security → MAC Filtering in the WUI.

Example 1:

Global Policy	: Forwarded
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: NA
Src. Interface	: eth1
Dest. Interface	: eth2

Addition of this rule drops all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78:90 irrespective of its Source MAC Address. All other frames on this interface are forwarded.

Example 2:

Global Policy	: Blocked
Protocol Type	: PPPoE
Dest. MAC Address	: 00:12:34:56:78:90
Source MAC Address	: 00:34:12:78:90:56
Src. Interface	: eth1
Dest. Interface	: eth2

Addition of this rule forwards all PPPoE frames going from eth1 to eth2 with a Destination MAC Address of 00:12:34:56:78 and Source MAC Address of 00:34:12:78:90:56. All other frames on this interface are dropped.

DAYTIME PARENTAL CONTROL
This feature restricts access of a selected LAN device to an outside Network through the PBL-6201v2, as per chosen days of the week and the chosen times.

Example:

User Name	: FilterJohn
Browser's MAC Address	: 00:25:46:78:63:21
Days of the Week	: Mon, Wed, Fri
Start Blocking Time	: 14:00
End Blocking Time	: 18:00

With this rule, a LAN device with MAC Address of 00:25:46:78:63:21 will have no access to the WAN on Mondays, Wednesdays, and Fridays, from 2pm to 6pm. On all other days and times, this device will have access to the outside Network.

Appendix B - Pin Assignments

Giga ETHERNET Ports (RJ45)

Pin	Name	Description
1	BI_DA+	Bi-directional pair A +
2	BI_DA-	Bi-directional pair A -
3	BI_DB+	Bi-directional pair B +
4	BI_DC+	Bi-directional pair C +
5	BI_DC-	Bi-directional pair C -
6	BI_DB-	Bi-directional pair B -
7	BI_DD+	Bi-directional pair D +
8	BI_DD-	Bi-directional pair D -

Appendix C – Specifications

Hardware

· RJ-14 X1 for VDSL2 (35b)/ADSL2+ (Annex A) Bonding and Single line
· RJ-45 X 4 for GELAN
· RJ-45 X 1 for 2.5GEWAN
· USB 3.0 X 1
· Reset button X 1
· 2.4G WiFi on/off, WPS button X 1
· 5G WiFi on/off, WPS button X 1
· Internal Antenna X 4
· Power switch X 1

ADSL

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

VDSL

· G.993.2 (VDSL2) 35b, 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)

2.5Gigabit Ethernet

· IEEE 802.3bz
· 2.5G BASE-T, auto-sense
· Support MDI/MDX

Gigabit Ethernet

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

Management

· TR-069/TR-104/TR-111/TR-181, SNMP, Telnet, Web- Based Management, Configuration Backup and Restoration
· Software Upgrade via HTTP, TFTP Server, or FTP Server

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)

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 802.11ax, 2.4GHz, 4T4R
  Backward compatible with 802.11n/g/b
  2412～2462 MHz
- IEEE 802.11ax,5GHz, 4T4R,
- Backward compatible with 802.11ac/n/a
- U-NII-1 (5150～5250 MHz)
- U-NII-2a (5250～5350 MHz) optional
- U-NII-2c/2e (5470～5725 MHz) optional
- 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/ 3A

Environment

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

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

· Storage Temperature: -25°C ~65°C (-13°F ~149°F)

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

Kit Weight

(1* PBL-6201v2, 1*RJ45 cable, 1*power adapter) = 0.95 kg

NOTE:	Specifications are subject to change without notice.

Appendix D - 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*

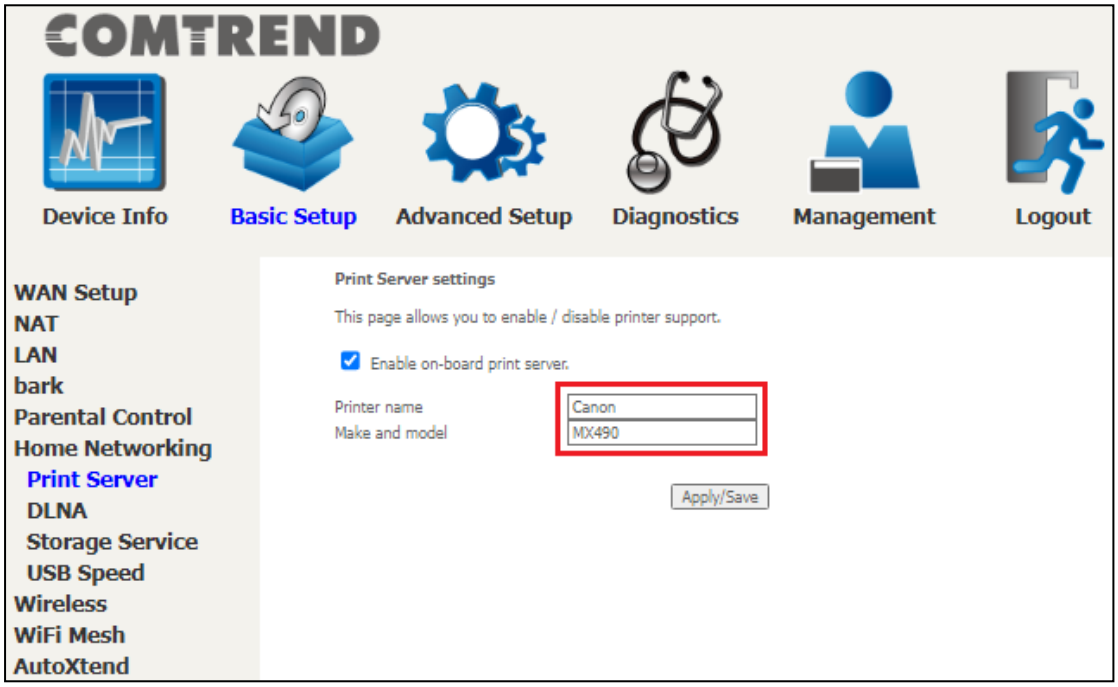
NOTE: The *WAN IP address* can be found on the Device Info → WAN screen

Appendix E - Printer Server

These steps explain the procedure for enabling the Printer Server.

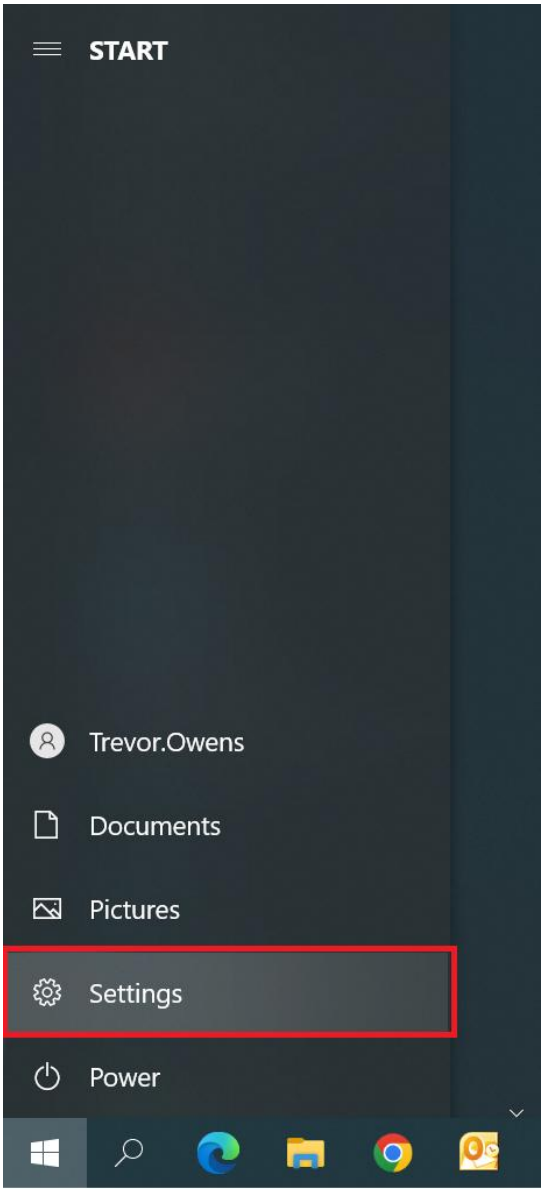
NOTE:	This function only applies to models with an USB host port.

STEP 1: Enable Print Server from Web User Interface. Select the Enable on-board print server checkbox ☑ and input Printer name & Make and model. Click the **Apply/Save** button.

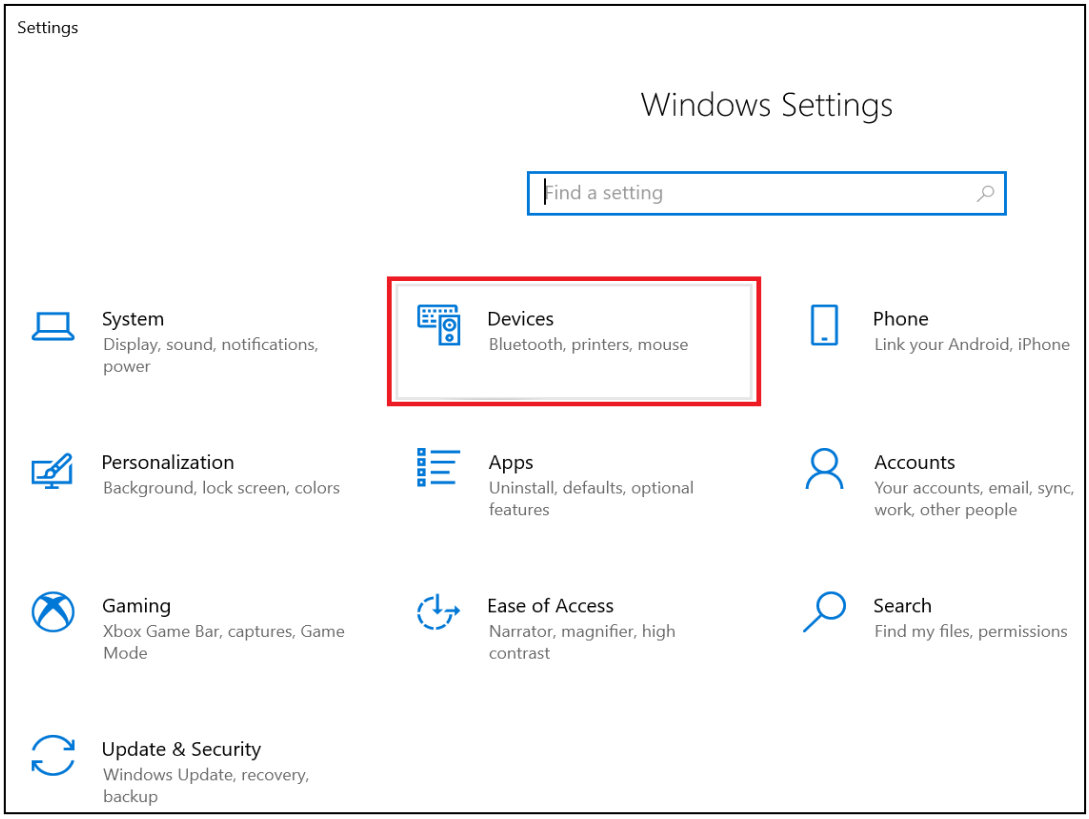


NOTE:	The **Printer name** can be any text string up to 40 characters. The **Make and model** can be any text string up to 128 characters.

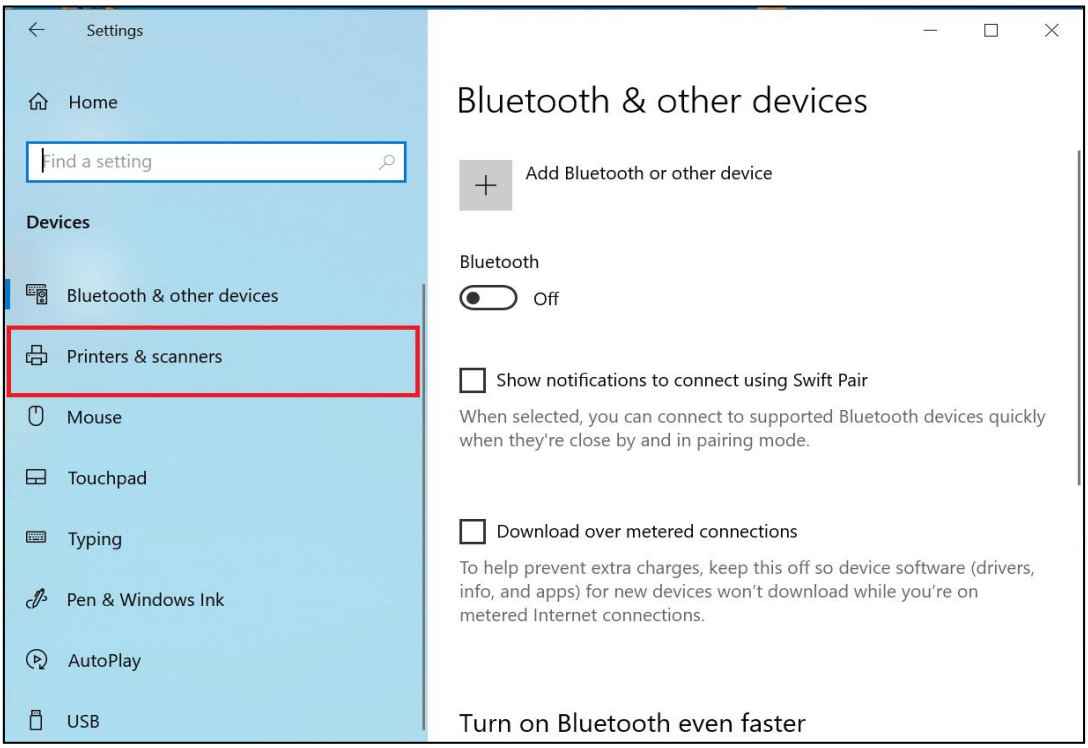
STEP 2: Click the Windows start button. → Then select **Settings**.



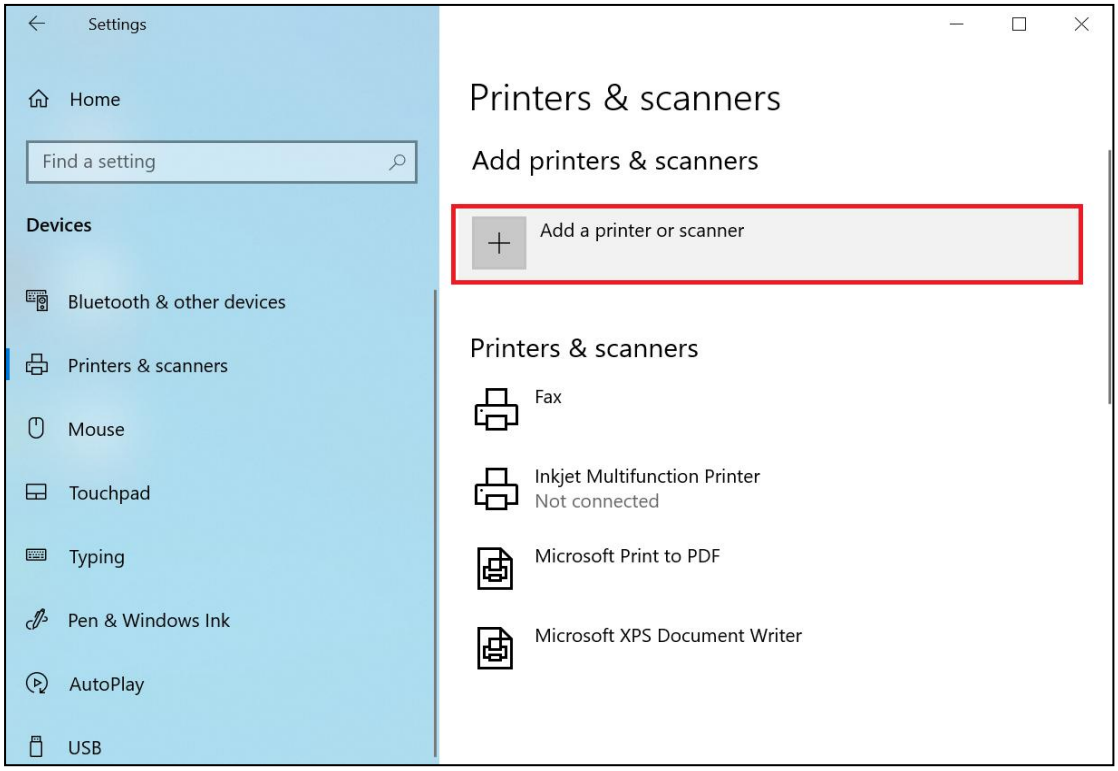
STEP 3: Select **Devices**.



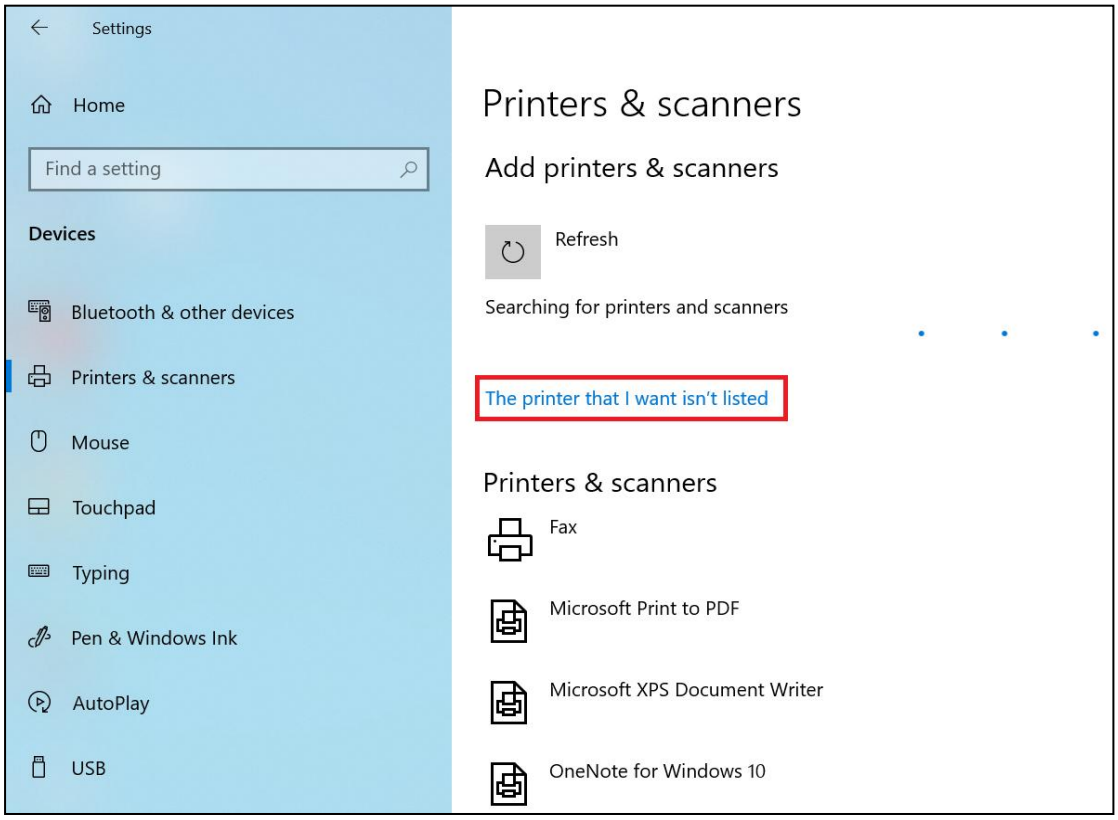
STEP 4: Select **Printers & scanners**.



STEP 5: Select **Add a printer or scanner**.



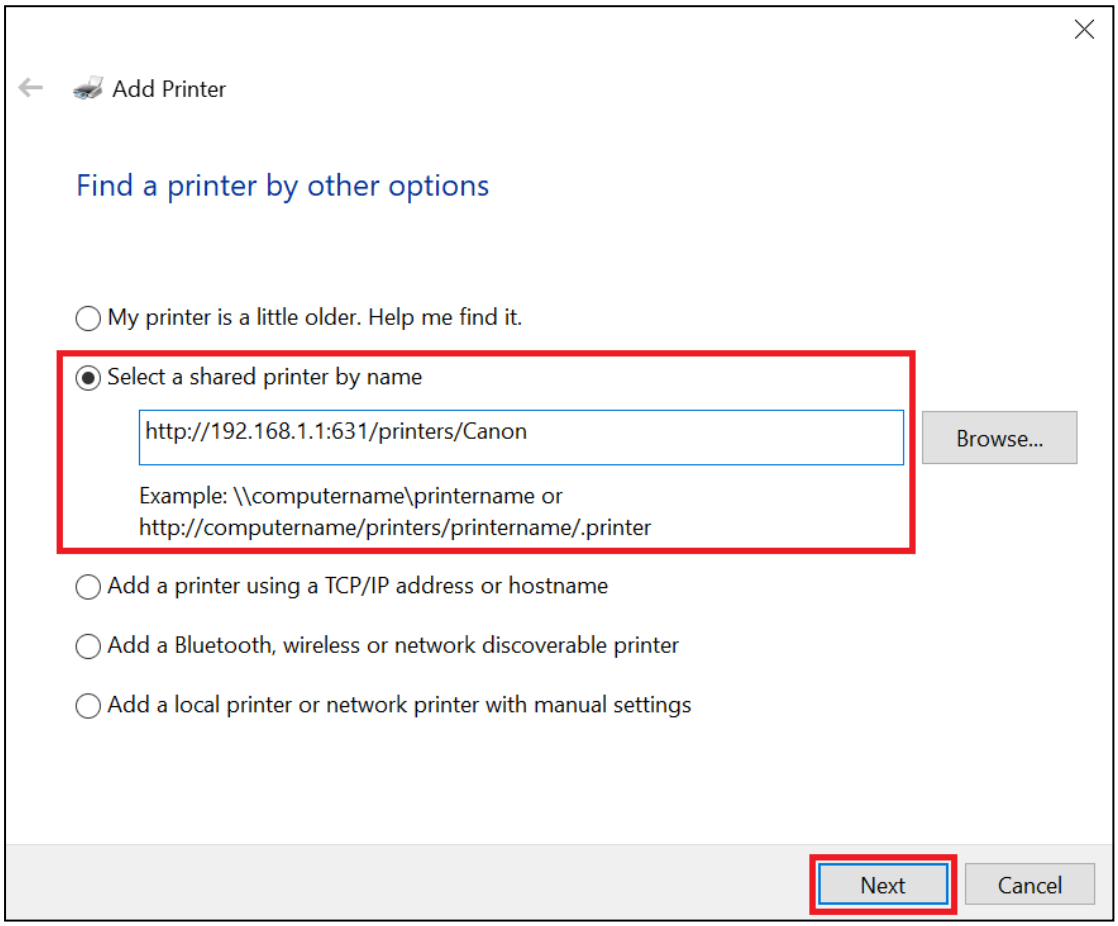
STEP 6: → Select **The printer that I want isn't listed**.



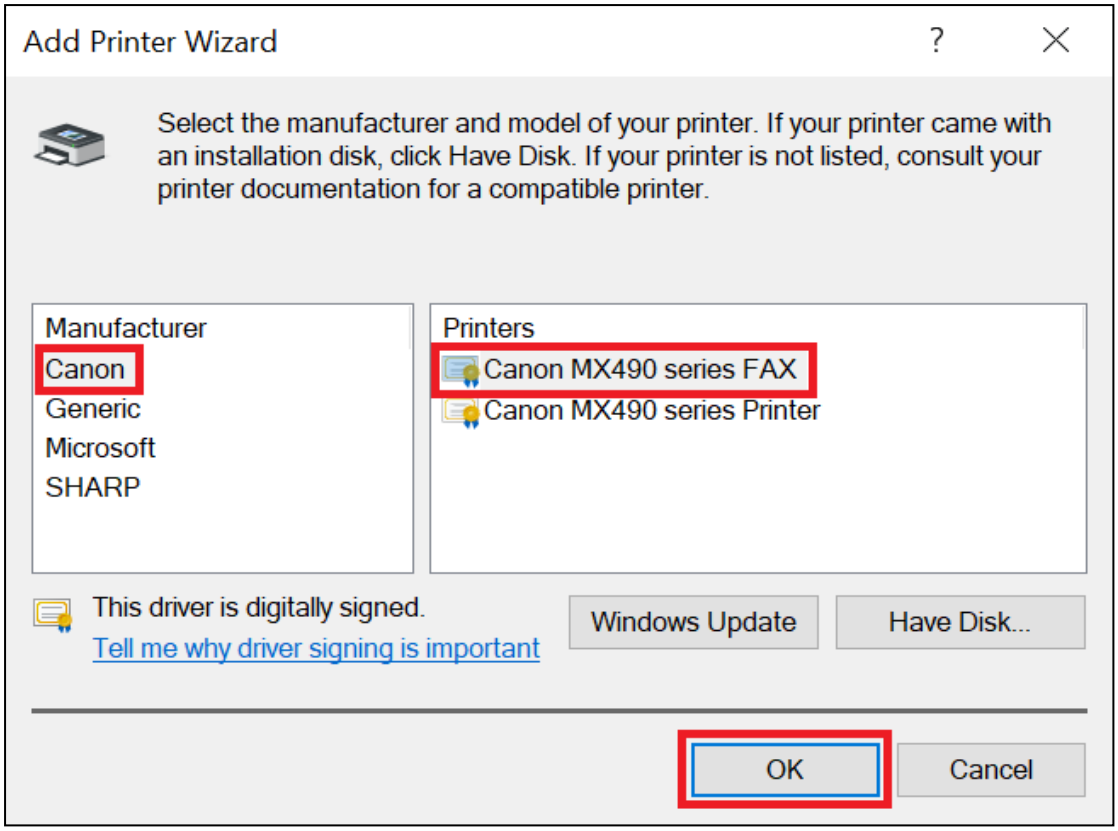
STEP 7: Choose **Select a shared printer by name**. Then input the printer link and click **Next**.

http://LAN IP:631/printers/Canon

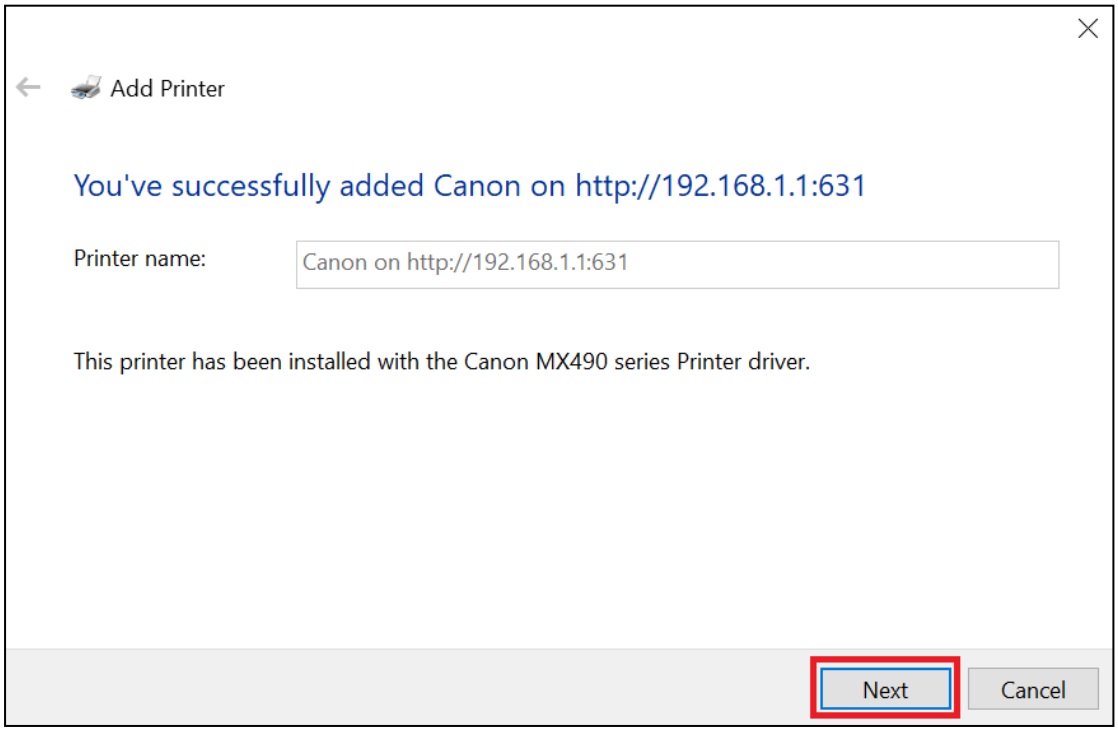
NOTE:	The printer name must be the same name inputted in the WEB UI "Print Server settings" as in step 1.



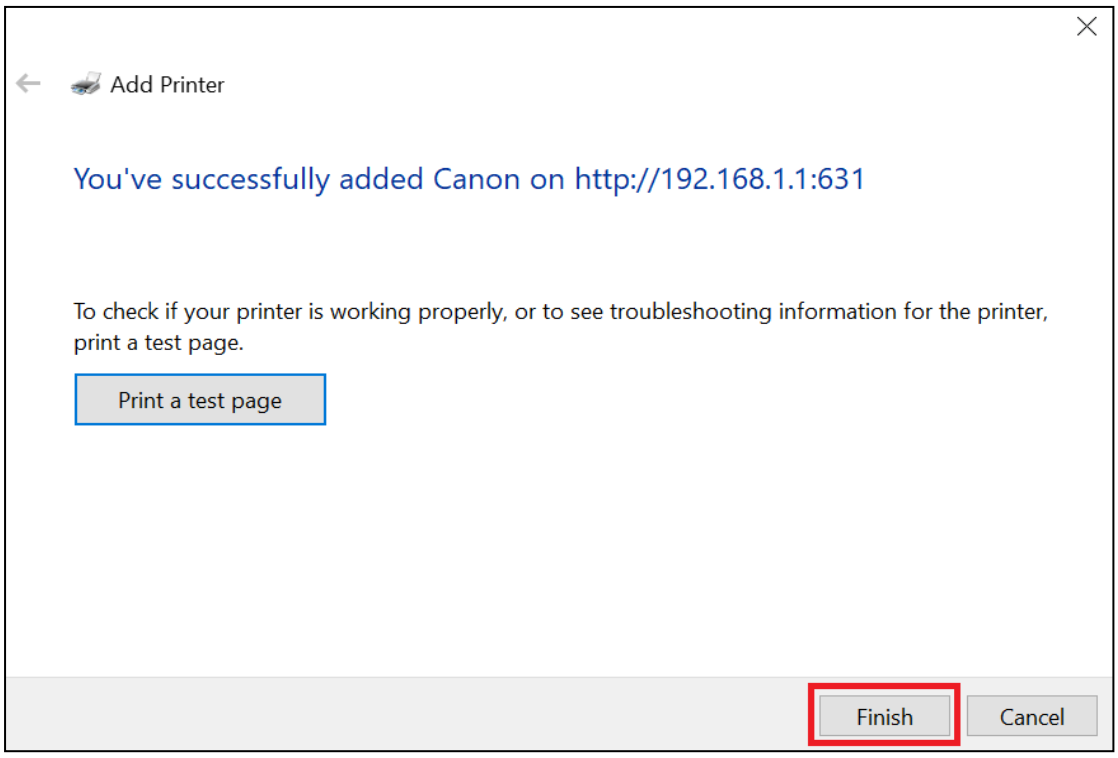
STEP 8: Select the manufacturer → and model of your printer → then, click **OK**.



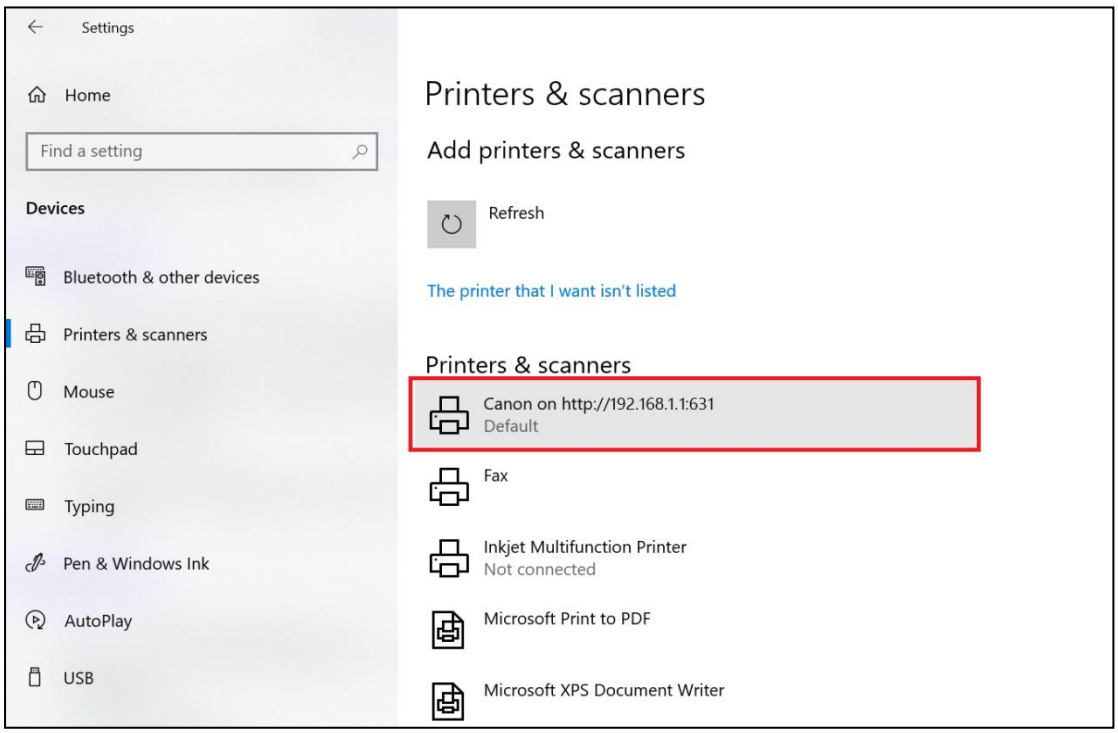
STEP 9: The printer has been successfully installed. Click the **Next** button.



STEP 10: Click Finish (or print a test page if required).



STEP 11: Go to → **Settings** → **Devices** → **Printers & scanners** to confirm that the printer has been configured.



Appendix F - Connection Setup

Creating a WAN connection is a two-stage process.

1 - Setup a Layer 2 Interface (ATM, PTM or Ethernet).
2 - Add a WAN connection to the Layer 2 Interface.

The following sections describe each stage in turn.

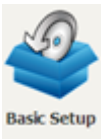
F1 ~ Layer 2 Interfaces

Every layer2 interface operates in Multi-Service Connection (VLAN MUX) mode, which supports multiple connections over a single interface. Note that PPPoA and IPoA connection types are not supported for Ethernet WAN interfaces. After adding WAN connections to an interface, you must also create an Interface Group to connect LAN/WAN interfaces.

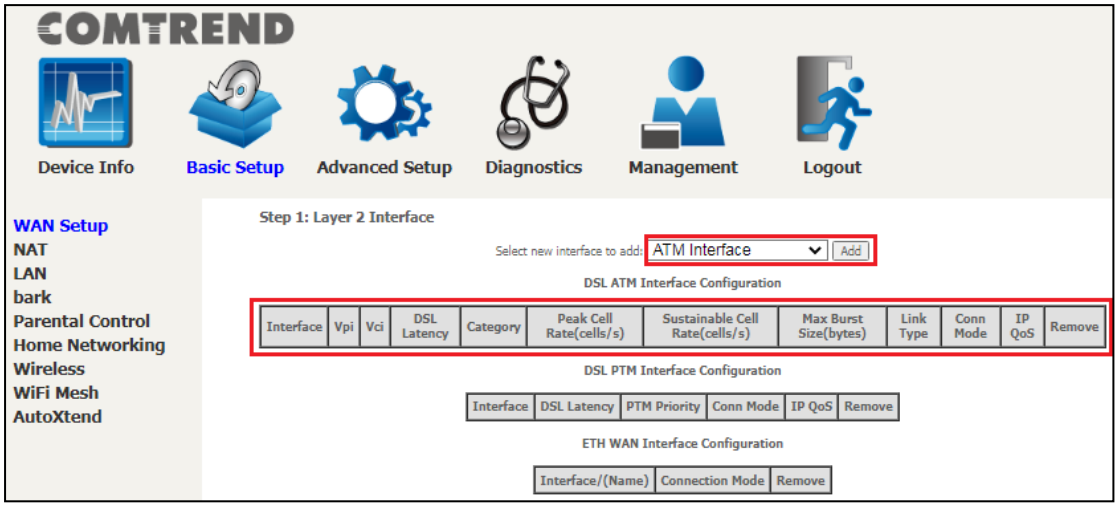
F1.1 ATM Interfaces

Follow these procedures to configure an ATM interface.

NOTE:	The PBL-6201v2 supports up to 16 ATM interfaces.

STEP 1: Go to Basic Setup 

→ WAN Setup → Select ATM Interface from the drop-down menu.

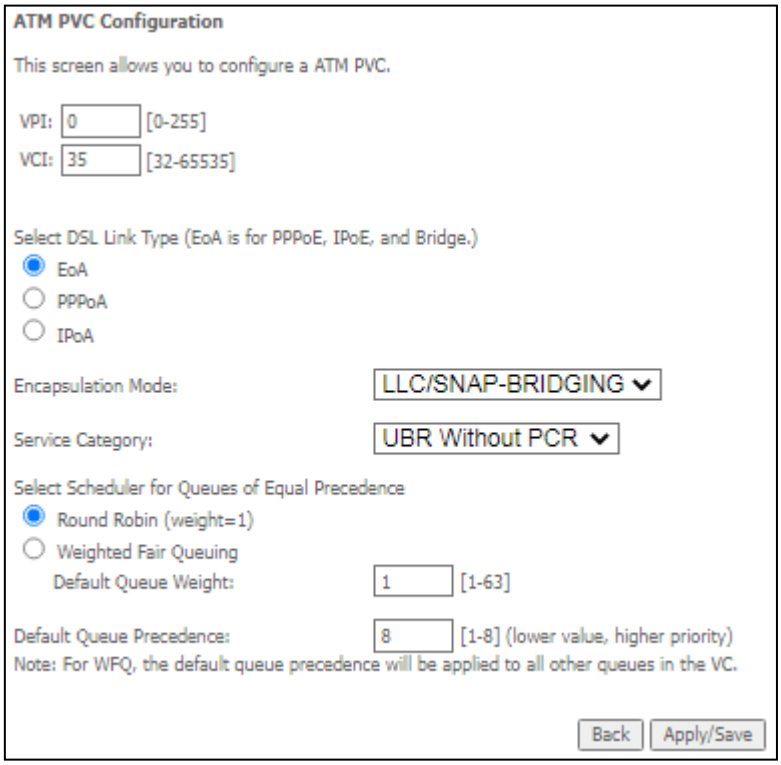


This table is provided here for ease of reference.

Item	Description
Interface	WAN interface name
VPI	ATM VPI (0-255)
VCI	ATM VCI (32-65535)
DSL Latency	{Path0} → portID = 0
Category	ATM service category
Peak Cell Rate	Maximum allowed traffic rate for the ATM PCR service connection
Sustainable Cell Rate	The average allowable, long-term cell transfer rate on the VBR service connection
Max Burst Size	The maximum allowable burst size of cells that can be transmitted continuously on the VBR service connection
Link Type	Choose EoA (for PPPoE, IPoE, and Bridge), PPPoA, or IPoA.
Connection Mode	Default Mode – Single service over one connection Vlan Mux Mode – Multiple Vlan service over one connection
IP QoS	Quality of Service (QoS) status
Remove	Select items for removal

STEP 2: Click **Add** to proceed to the next screen.

NOTE:	To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.

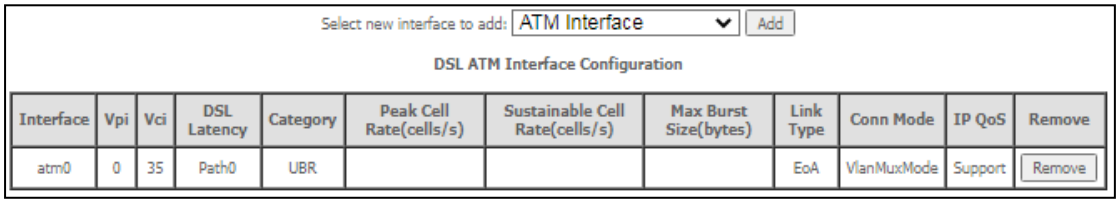


There are many settings here including: VPI/VCI, DSL Link Type, Encapsulation Mode, Service Category and Queue Weight.
Here are the available encapsulations for each xDSL Link Type:

- EoA- LLC/SNAP-BRIDGING, VC/MUX
- PPPoA- VC/MUX, LLC/ENCAPSULATION
- IPoA- LLC/SNAP-ROUTING, VC MUX

STEP 3: Click **Apply/Save** to confirm your choices.

On the next screen, check that the ATM interface is added to the list. For example, an ATM interface on PVC 0/35 in Default Mode with an EoA Link type is shown below.

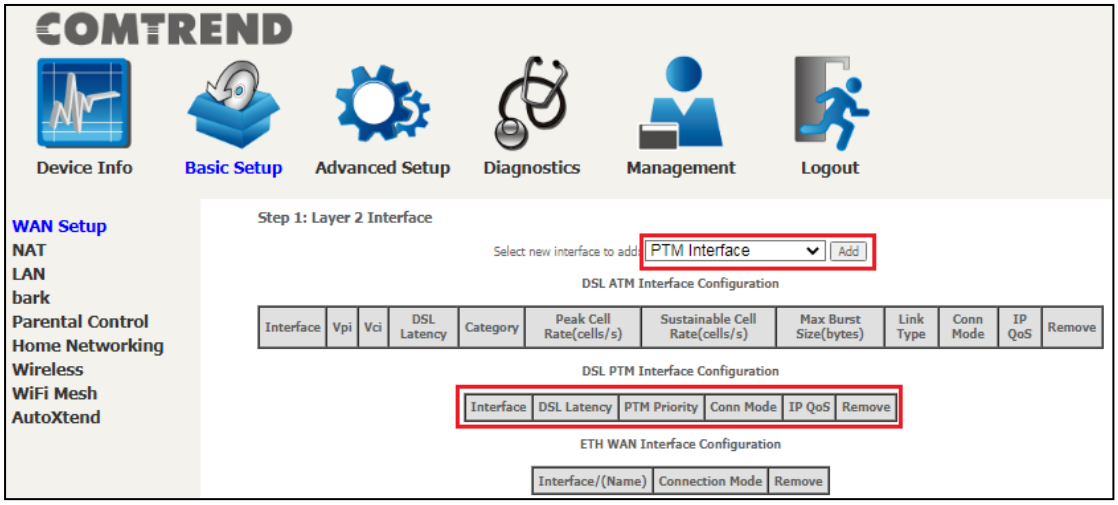


To add a WAN connection go to Section F2 ~ WAN Connections.

F1.2 PTM Interfaces

Follow these procedures to configure a PTM interface.

STEP 1: Go to Basic Setup → WAN Setup → Select PTM Interface from the drop-down menu.

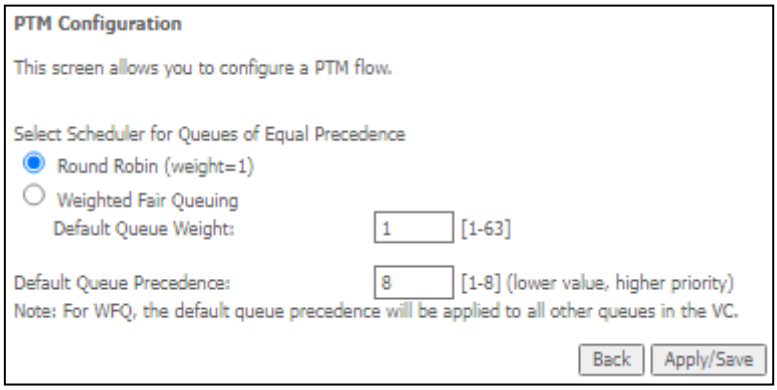


This table is provided here for ease of reference.

Item	Description
Interface	WAN interface name.
DSL Latency	{Path0} → portID = 0
PTM Priority	Normal or High Priority (Preemption).
Connection Mode	Default Mode – Single service over one interface. Vlan Mux Mode – Multiple Vlan services over one interface.
IP QoS	Quality of Service (QoS) status.
Remove	Select interfaces to remove.

STEP 2: Click **Add** to proceed to the next screen.

NOTE:	To add WAN connections to one interface type, you must delete existing connections from the other interface type using the **remove** button.

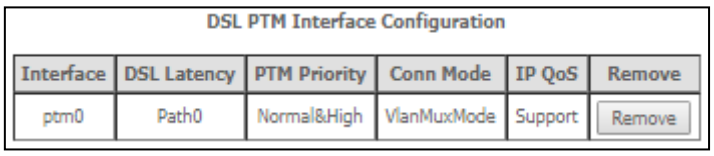


Default PTM interface Quality of Service can be configured here, including Scheduler, and Queue Weight.

STEP 3: Click **Apply/Save** to confirm your choices.

On the next screen, check that the PTM interface is added to the list.

For example, a PTM interface in Default Mode is shown below.



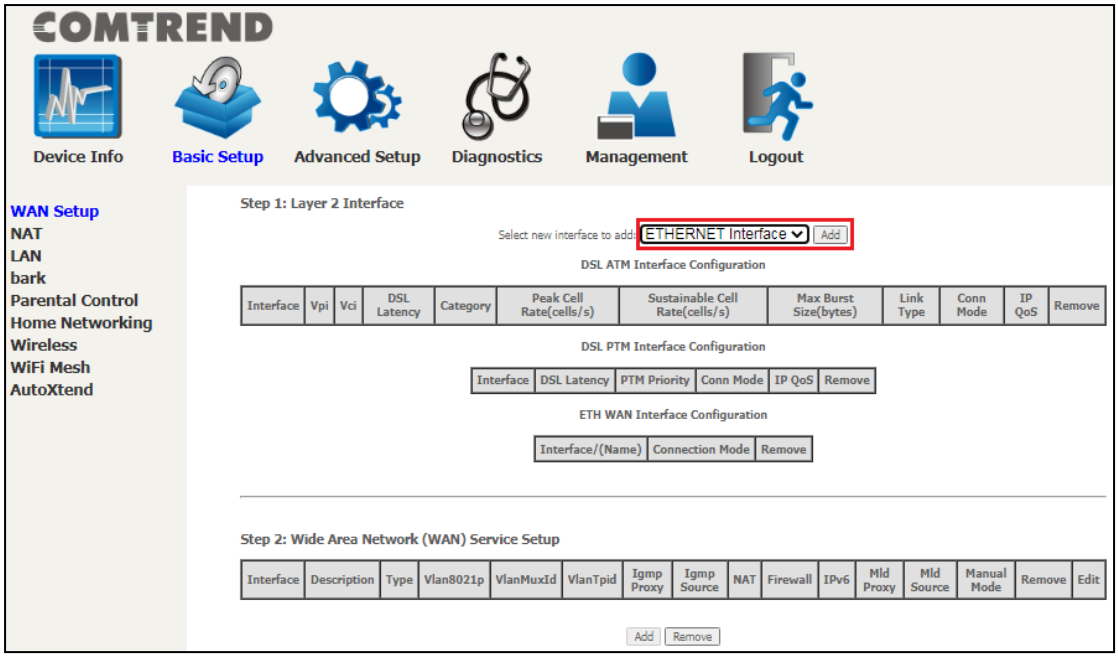
To add a WAN connection go to Section F2 ~ WAN Connections.

F1.3 Ethernet WAN Interface

The PBL-6201v2 supports a single Ethernet WAN interface over the ETH WAN port. Follow these procedures to configure an Ethernet interface.

STEP 1: Go to Basic Setup 

→ WAN Setup → Select ETHERNET Interface from the drop-down menu.

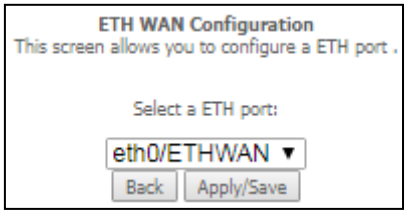


STEP 2: Click **Add** to proceed to the next screen.

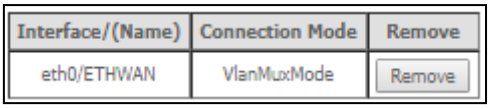
This table is provided here for ease of reference.

Item	Description
Interface/ (Name)	WAN interface name.
Connection Mode	Default Mode – Single service over one interface. Vlan Mux Mode – Multiple Vlan services over one interface.
Remove	Select interfaces to remove.

STEP 3: Select an Ethernet port and Click **Apply/Save** to confirm your choices.



On the next screen, check that the ETHERNET interface is added to the list.



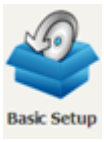
Interface/(Name)	Connection Mode	Remove
eth0/ETHWAN	VlanMuxMode	Remove

To add a WAN connection go to Section F2 ~ WAN Connections.

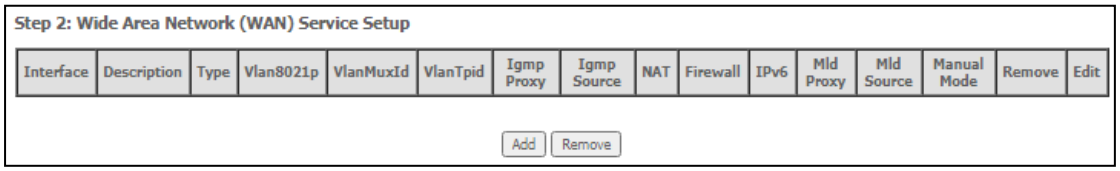
F2 ~ WAN Connections

The PBL-6201v2 supports one WAN connection for each interface, up to a maximum of 16 connections.

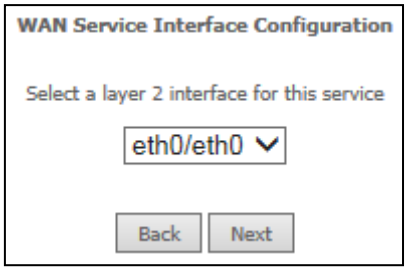
To setup a WAN connection follow these instructions.

STEP 1: Go to Basic Setup 

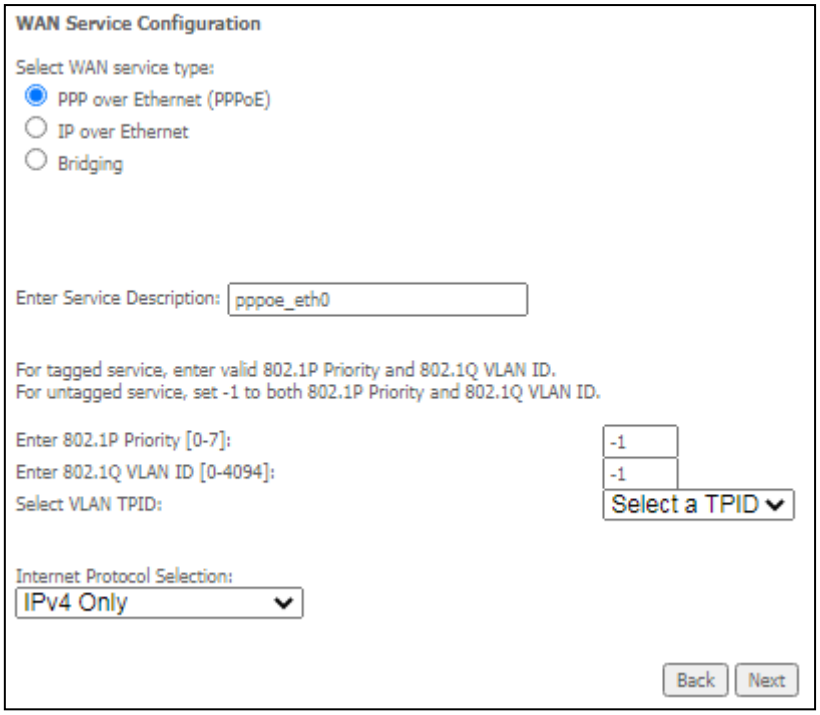
→ WAN Setup.



STEP 2: Click **Add** to create a WAN connection. The following screen will display.



STEP 3: Choose a layer 2 interface from the drop-down box and click **Next**. The WAN Service Configuration screen will display as shown below.



NOTE:	The WAN services shown here are those supported by the layer 2 interface you selected in the previous step. If you wish to change your selection click the **Back** button and select a different layer 2 interface.

STEP 4: For VLAN Mux Connections only, you must enter Priority & VLAN ID tags.

Select a TPID if VLAN tag Q-in-Q is used.

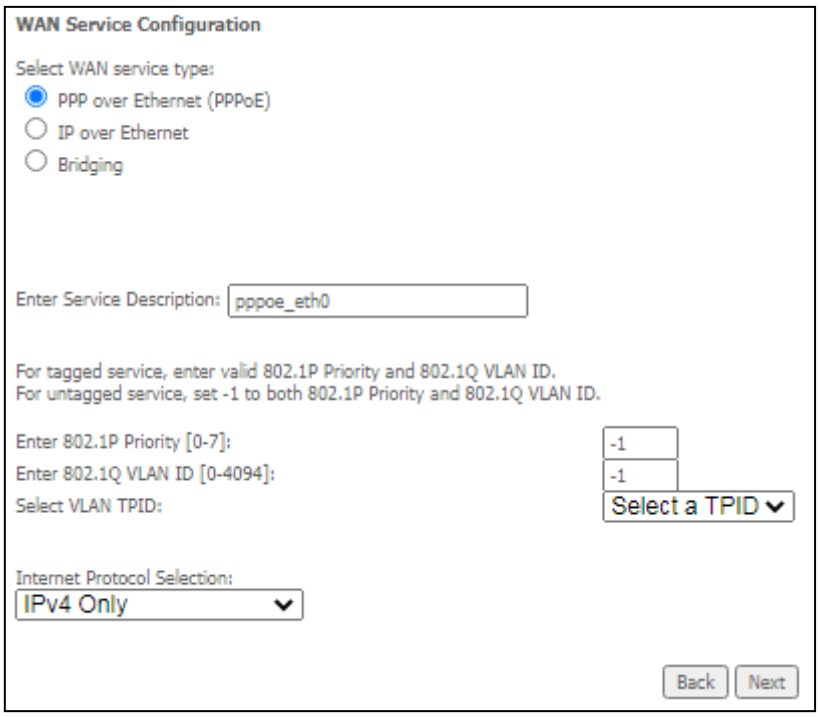
STEP 5: You will now follow the instructions specific to the WAN service type you wish to establish. This list should help you locate the correct procedure:

(1) For PPP over ETHERNET (PPPoE) – IPv4
(2) For IP over ETHERNET (IPoE) – IPv4
(3) For Bridging – IPv4
(4) For PPP over ATM (PPPoA) – IPv4
(5) For IP over ATM (IPoA) – IPv4
(6) For PPP over ETHERNET (PPPoE) – IPv6
(7) For IP over ETHERNET (IPoE) – IPv6
(8) Bridging – IPv6 (Not Supported)
(9) For PPP over ATM (PPPoA) – IPv6
(10) IPoA – IPv6 (Not Supported)

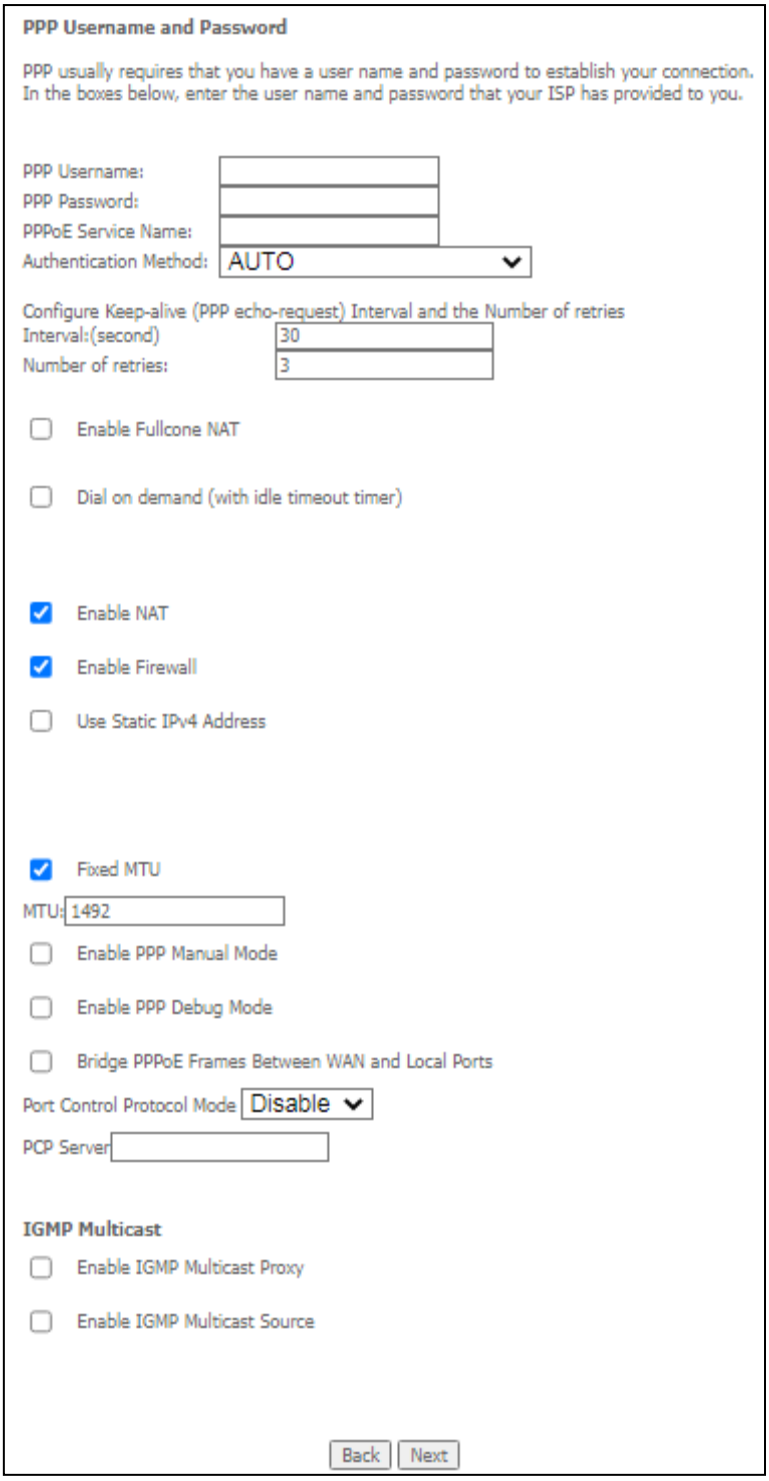
The subsections that follow continue the WAN service setup procedure.

F2.1 PPP over ETHERNET (PPPoE) – IPv4

STEP 1: Select the PPP over Ethernet radio button and click **Next**.



STEP 2: On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.



Click **Next** to continue or click **Back** to return to the previous step.

The settings shown above are described below.

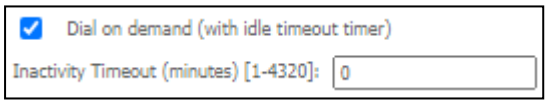
PPP SETTINGS

The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

CONFIGURE KEEP-ALIVE
Configures the interval and number of keep alive packets (PPP echo-request) sent by the device for the PPP connection.
Interval (second): Time between sending out each PPP echo-request packet.
Number of retries: Number of retries before PPP connection is dropped.

ENABLE FULLCONE NAT
This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND
The PBL-6201v2 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox ☑. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected to free up system resources for better performance.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS
Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IPv4 Address** field.
Don't forget to adjust the IP configuration to Static IP Mode as described in section 3.2 IP Configuration.

FIXED MTU
Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1492 for PPPoE.

ENABLE PPP MANUAL MODE
Use this button to manually connect/disconnect PPP sessions.

ENABLE PPP DEBUG MODE
When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS
(This option is hidden when PPP IP Extension is enabled)
When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The PBL-6201v2 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

PORT CONTROL PROTOCOL MODE

1.DS-Lite:
Encapsulates the IPv4 packet and transmits it across an IPv6 tunnel.
2.NAT444:
It maps multiple private IP addresses to one public IP address and uses a different port block for each private IP address.

PCP SERVER

An IP address of the PCP server so that a CPE (PCP client) can send a request to establish a PCP connection to the PCP server.

ENABLE IGMP MULTICAST PROXY

Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

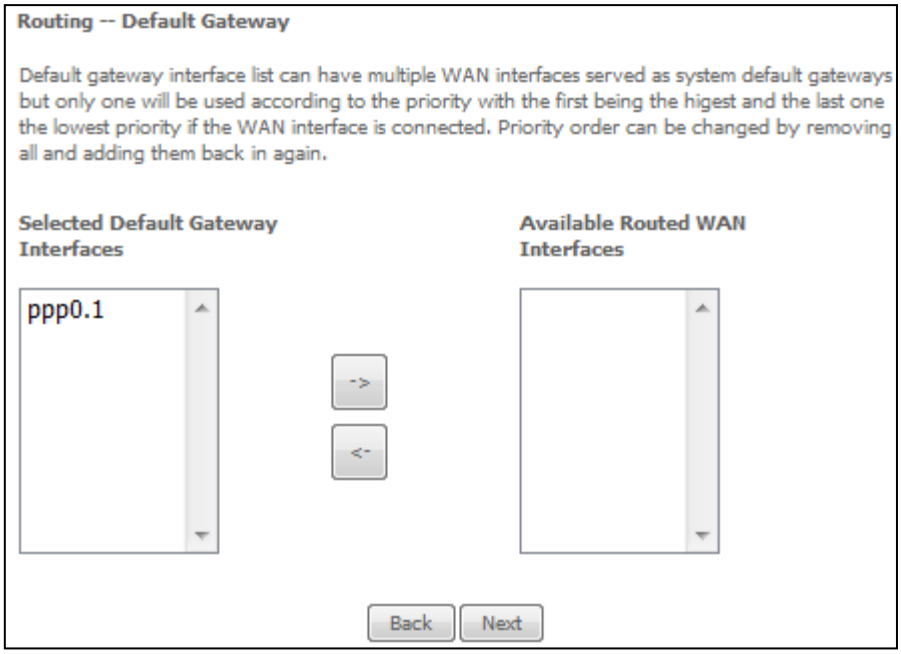
ENABLE IGMP MULTICAST SOURCE

Enable the WAN interface to be used as IGMP multicast source.

Enable WAN interface with base MAC

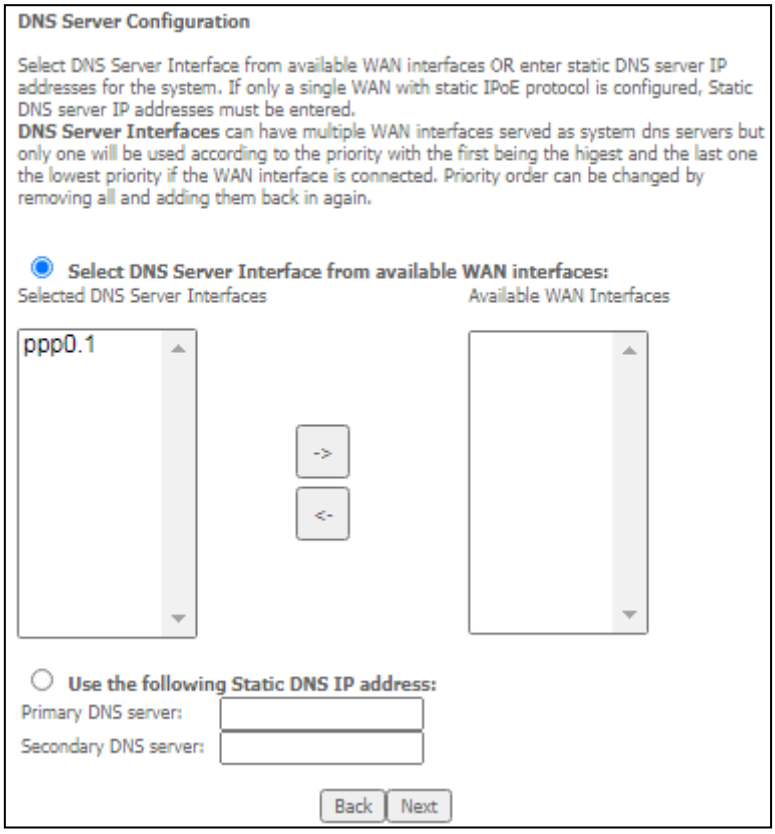
Tick the checkbox ☑ to enable this function which will hook up the br0 MAC address to this very WAN service.

STEP 3: Choose an interface to be the default gateway.



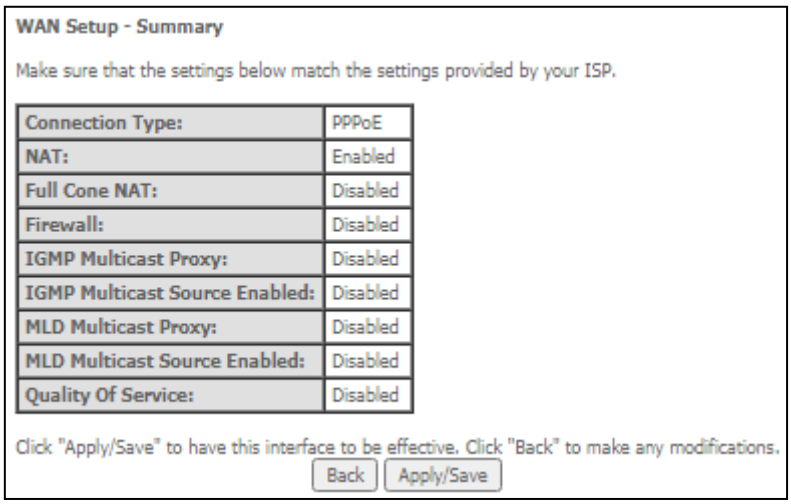
Click **Next** to continue or click **Back** to return to the previous step.

STEP 4: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.



Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Disabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

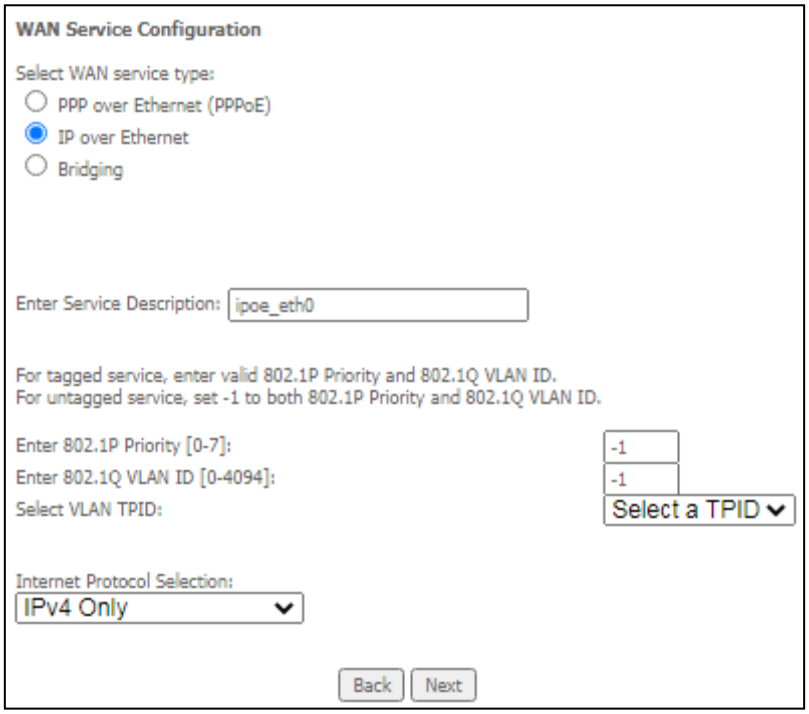
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

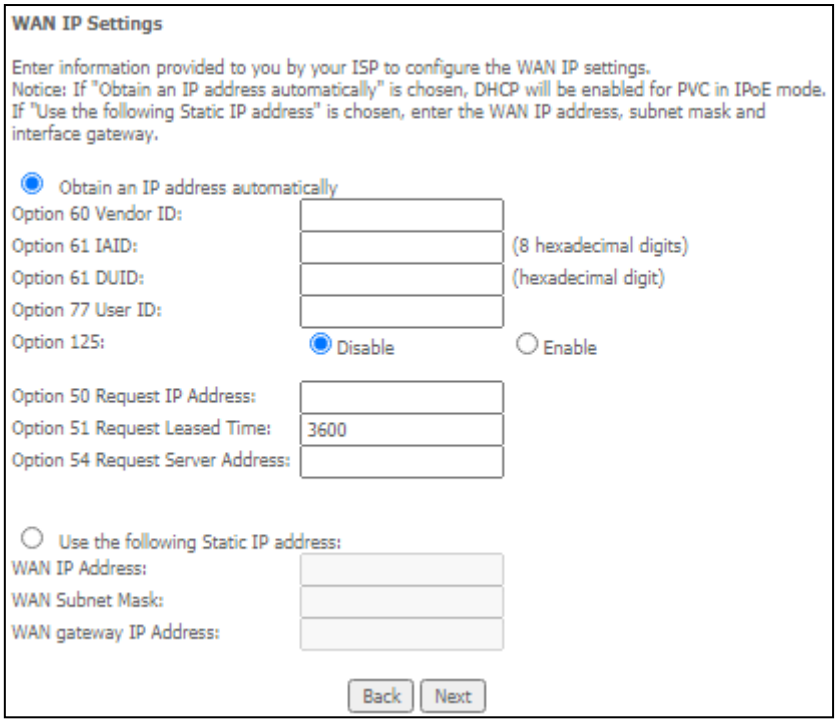
After clicking **Apply/Save**, the new service should appear on the main screen.

F2.2 IP over ETHERNET (IPoE) – IPv4

STEP 1: Select the IP over Ethernet radio button and click **Next.**



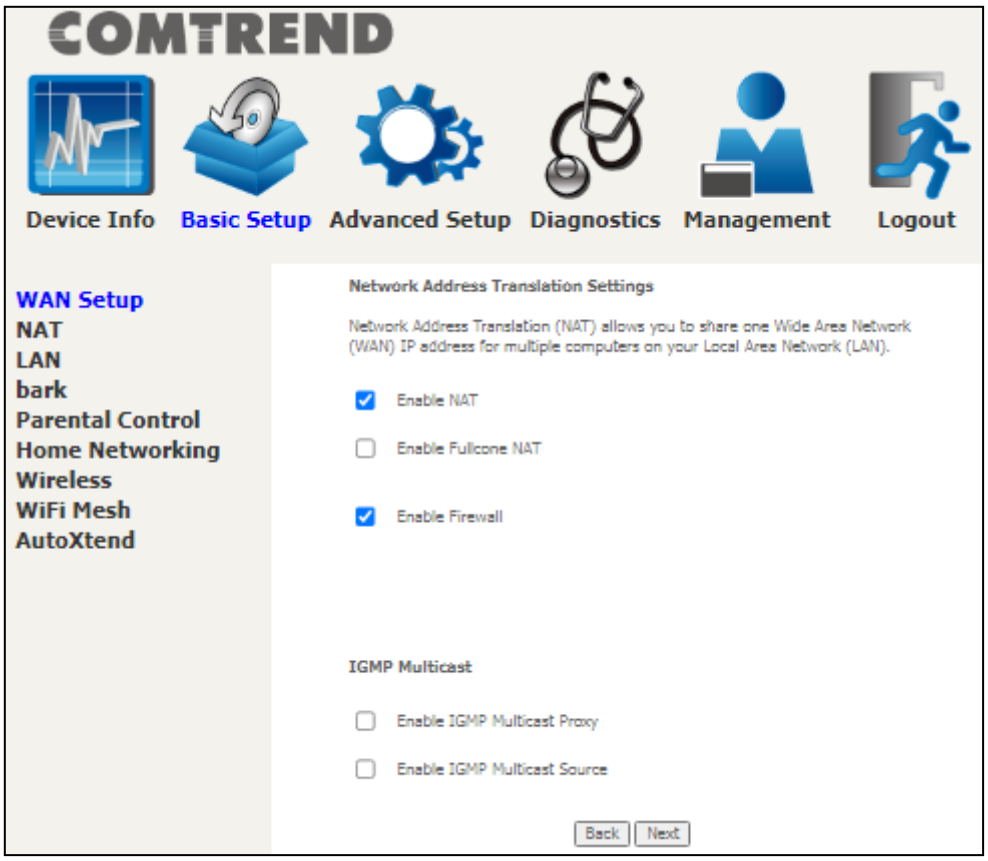
STEP 2: The WAN IP settings screen provides access to the DHCP server settings. You can select the **Obtain an IP address automatically** radio button to enable DHCP (use the DHCP Options only if necessary). However, if you prefer, you can use the **Static IP address** method instead to assign WAN IP address, Subnet Mask and Default Gateway manually.



With reference to different options, please contact your ISP (Internet Service Provider) for more details.

Click **Next** to continue or click **Back** to return to the previous step.

STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑. Click **Next** to continue or click **Back** to return to the previous step.



ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected, so as to free up system resources for improved performance.

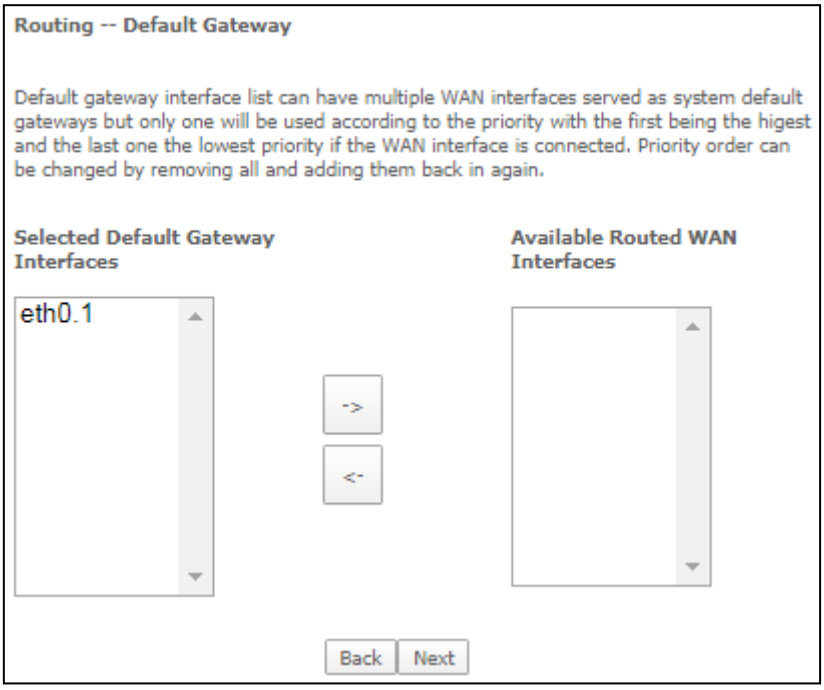
ENABLE FULLCONE NAT
This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected so as to free up system resources for better performance.

ENABLE IGMP MULTICAST PROXY
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

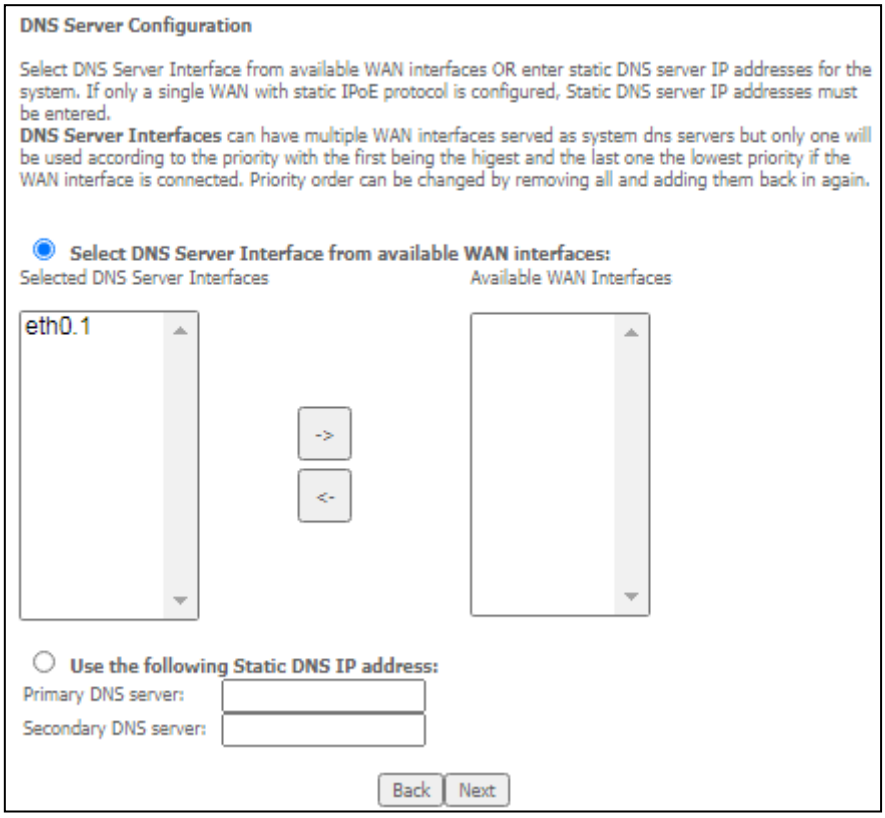
ENABLE IGMP MULTICAST SOURCE
Enable the WAN interface to be used as IGMP multicast source.

STEP 4: Choose an interface to be the default gateway.



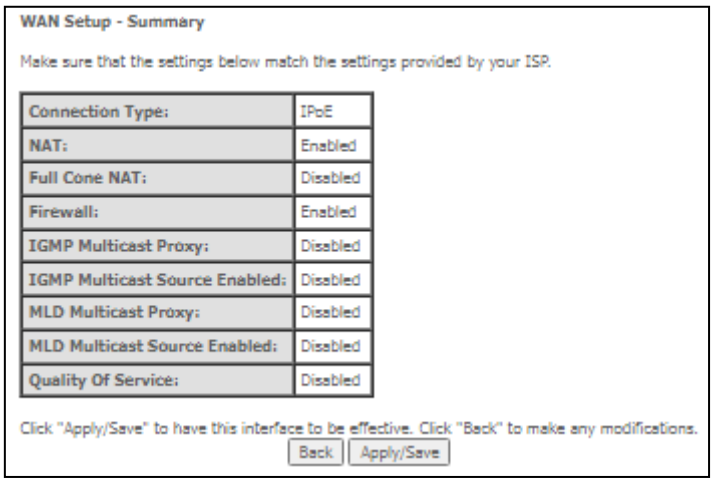
Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.



Click **Next** to continue or click **Back** to return to the previous step.

STEP 6: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoE
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

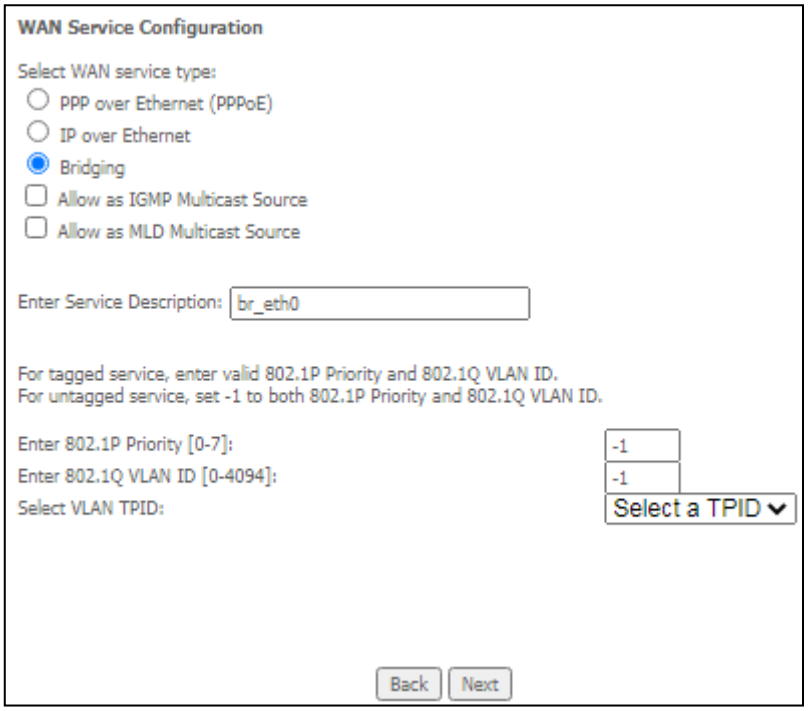
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

After clicking **Apply/Save**, the new service should appear on the main screen.

F2.3 Bridging – IPv4

STEP 1: Select the Bridging radio button and click **Next**.



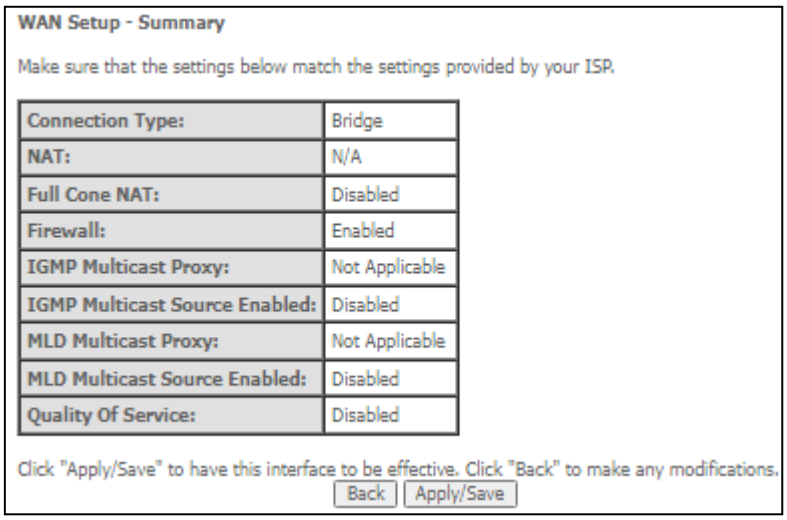
Allow as IGMP Multicast Source

Click to allow use of this bridge WAN interface as IGMP multicast source.

Allow as MLD Multicast Source

Click to allow use of this bridge WAN interface as MLD multicast source.

STEP 2: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to return to the previous screen.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	Bridge
NAT:	N/A
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Not Applicable
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Not Applicable
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

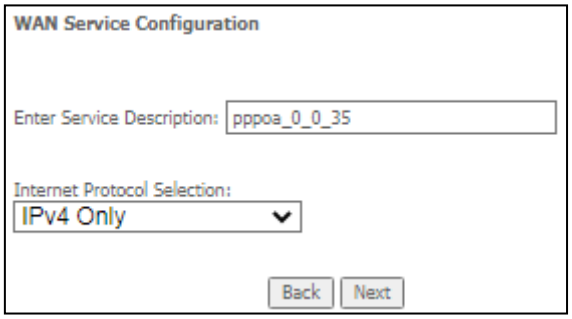
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

After clicking **Apply/Save**, the new service should appear on the main screen.

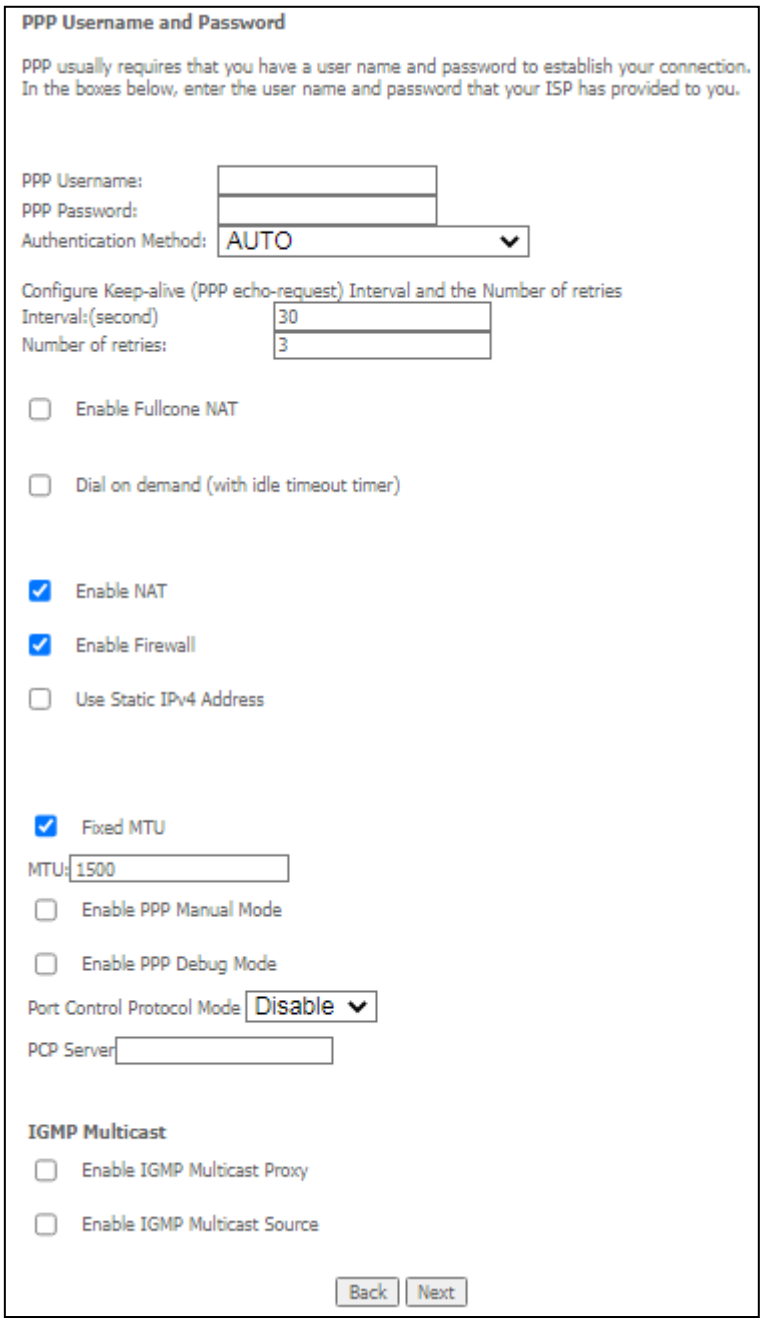
NOTE:	If this bridge connection is your only WAN service, the PBL-6201v2 will be inaccessible for remote management or technical support from the WAN.

F2.4 PPP over ATM (PPPoA) – IPv4



STEP 1: Click **Next** to continue.

STEP 2: On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.

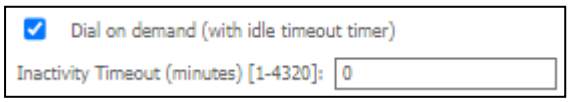


PPP SETTINGS
The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

CONFIGURE KEEP-ALIVE
Configures the interval and number of keep alive packets (PPP echo-request) sent by the device for the PPP connection.
Interval (second): Time between sending out each PPP echo-request packet.
Number of retries: Number of retries before PPP connection is dropped.

ENABLE FULLCONE NAT
This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host, by sending a packet to the mapped external address.

DIAL ON DEMAND
The PBL-6201v2 can be configured to disconnect if there is no activity for a period of time by selecting the **Dial on demand** checkbox ☑. You must also enter an inactivity timeout period in the range of 1 to 4320 minutes.



ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected to free up system resources for better performance.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS
Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IP Address** field. Also, don't forget to adjust the IP configuration to Static IP Mode as described in 3.2 IP Configuration

Fixed MTU
Fixed Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1500 for PPPoA.

ENABLE PPP MANUAL MODE
Use this button to manually connect/disconnect PPP sessions.

ENABLE PPP DEBUG MODE
When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

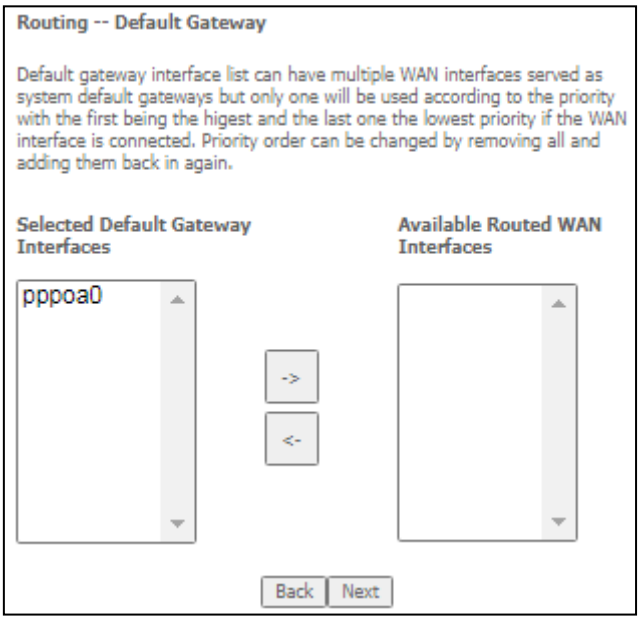
PORT CONTROL PROTOCOL MODE
1.DS-Lite:
Encapsulates the IPv4 packet and transmits it across an IPv6 tunnel.
2.NAT444:
It maps multiple private IP addresses to one public IP address and uses a different port block for each private IP address.

PCP SERVER
An IP address of the PCP server so that a CPE (PCP client) can send a request to establish a PCP connection to the PCP server.

ENABLE IGMP MULTICAST PROXY
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

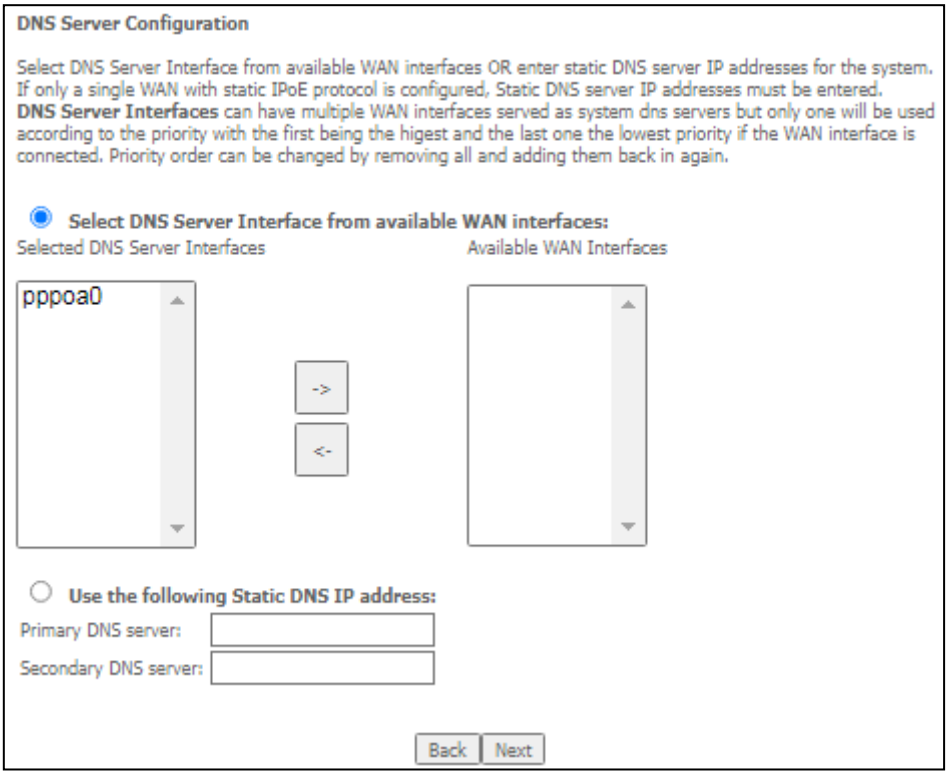
Enable IGMP Multicast Source
Enable the WAN interface to be used as IGMP multicast source.

STEP 3: Choose an interface to be the default gateway.



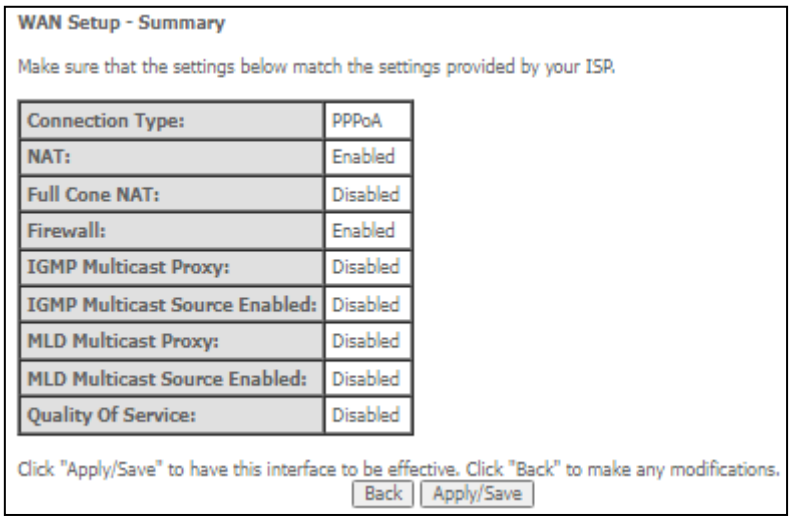
Click **Next** to continue or click **Back** to return to the previous step.

STEP 4: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.



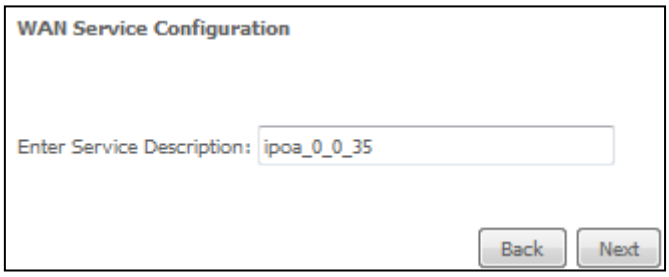
Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



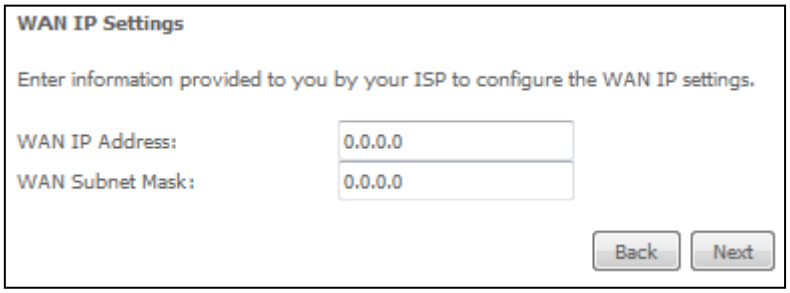
After clicking **Apply/Save**, the new service should appear on the main screen.

F2.5 IP over ATM (IPoA) – IPv4

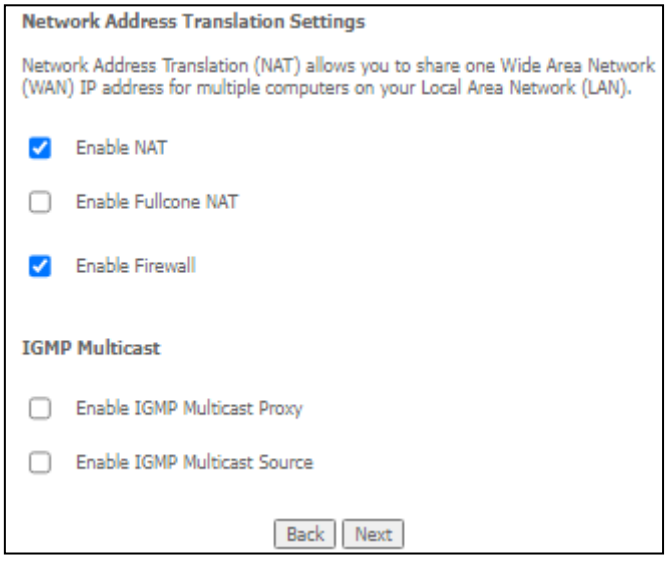


STEP 1: Click **Next** to continue.

STEP 2: Enter the WAN IP settings provided by your ISP. Click **Next** to continue.



STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑. Click **Next** to continue or click **Back** to return to the previous step.



ENABLE NAT
If the LAN is configured with a private IP address, the user should select this checkbox ☑. The NAT submenu will appear in the Advanced Setup menu after reboot. On the other hand, if a private IP address is not used on the LAN side (i.e. the LAN side is using a public IP), this checkbox ☑ should not be selected, so as to free up system resources for improved performance.

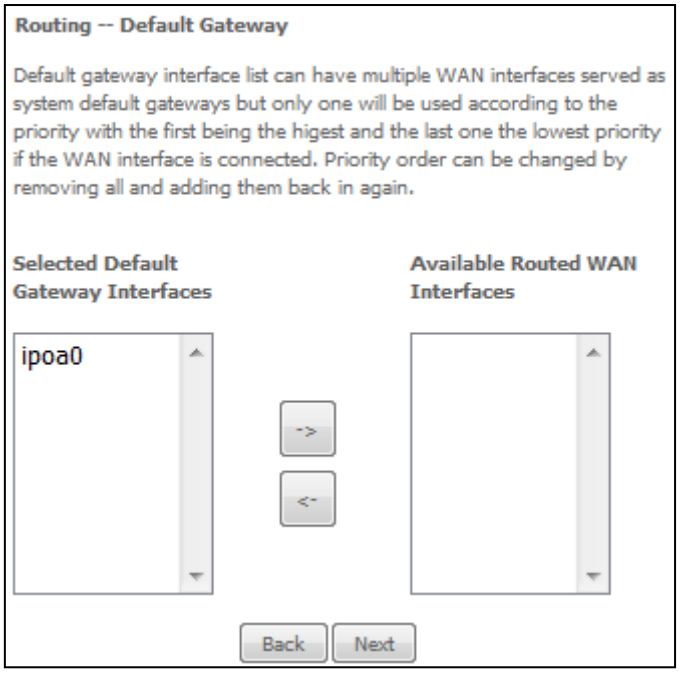
ENABLE FULLCONE NAT
This option becomes available when NAT is enabled. Known as one-to-one NAT, all requests from the same internal IP address and port are mapped to the same external IP address and port. An external host can send a packet to the internal host by sending a packet to the mapped external address.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected so as to free up system resources for better performance.

ENABLE IGMP MULTICAST PROXY
Tick the checkbox ☑ to enable Internet Group Membership Protocol (IGMP) multicast. This protocol is used by IPv4 hosts to report their multicast group memberships to any neighboring multicast routers.

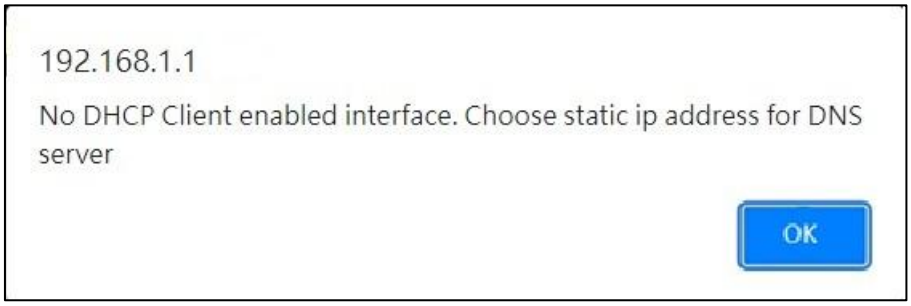
Enable IGMP Multicast Source
Enable the WAN interface to be used as IGMP multicast source.

STEP 4: Choose an interface to be the default gateway.

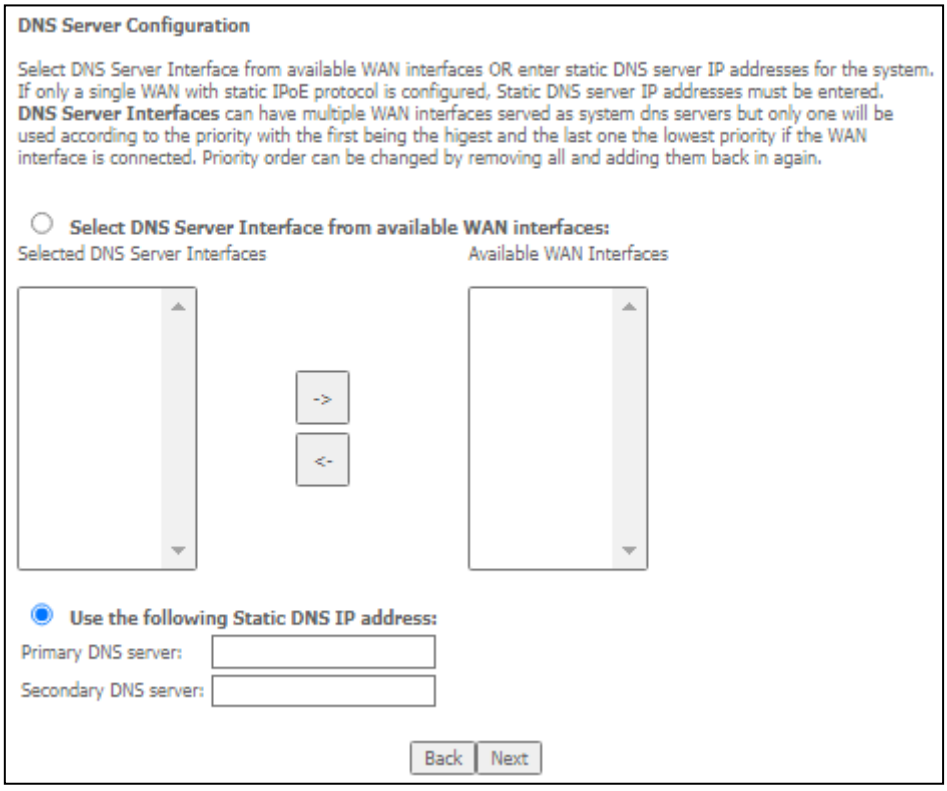


Click **Next** to continue or click **Back** to return to the previous step.

NOTE: If the DHCP server is not enabled on another WAN interface then the following notification will be shown before the next screen.

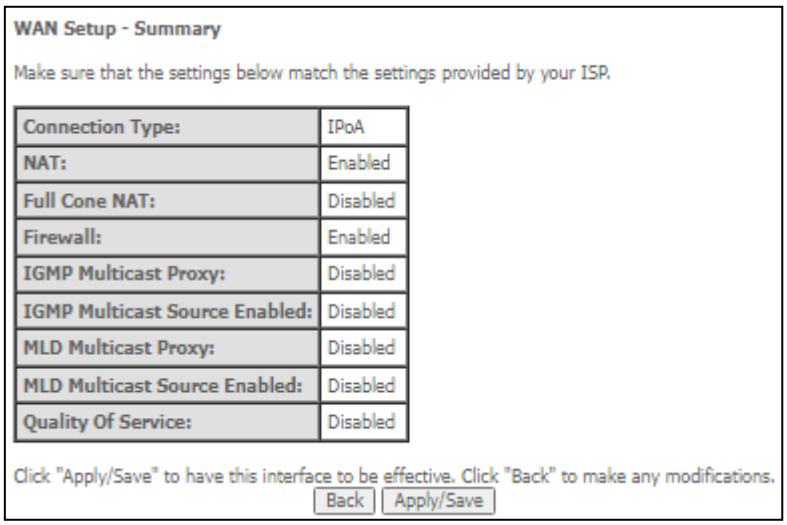


STEP 5: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.



Click **Next** to continue or click **Back** to return to the previous step.

STEP 6: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoA
NAT:	Enabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

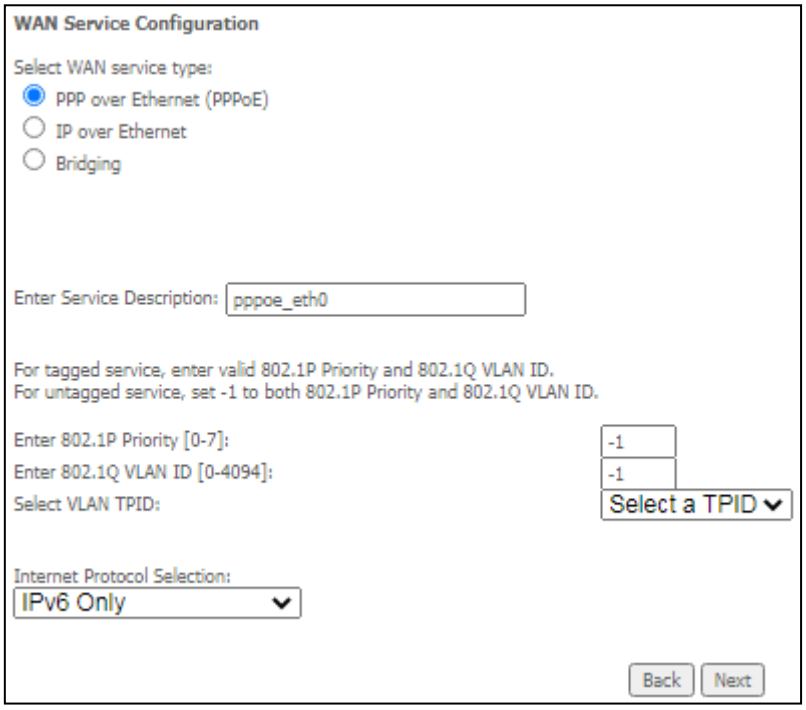
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

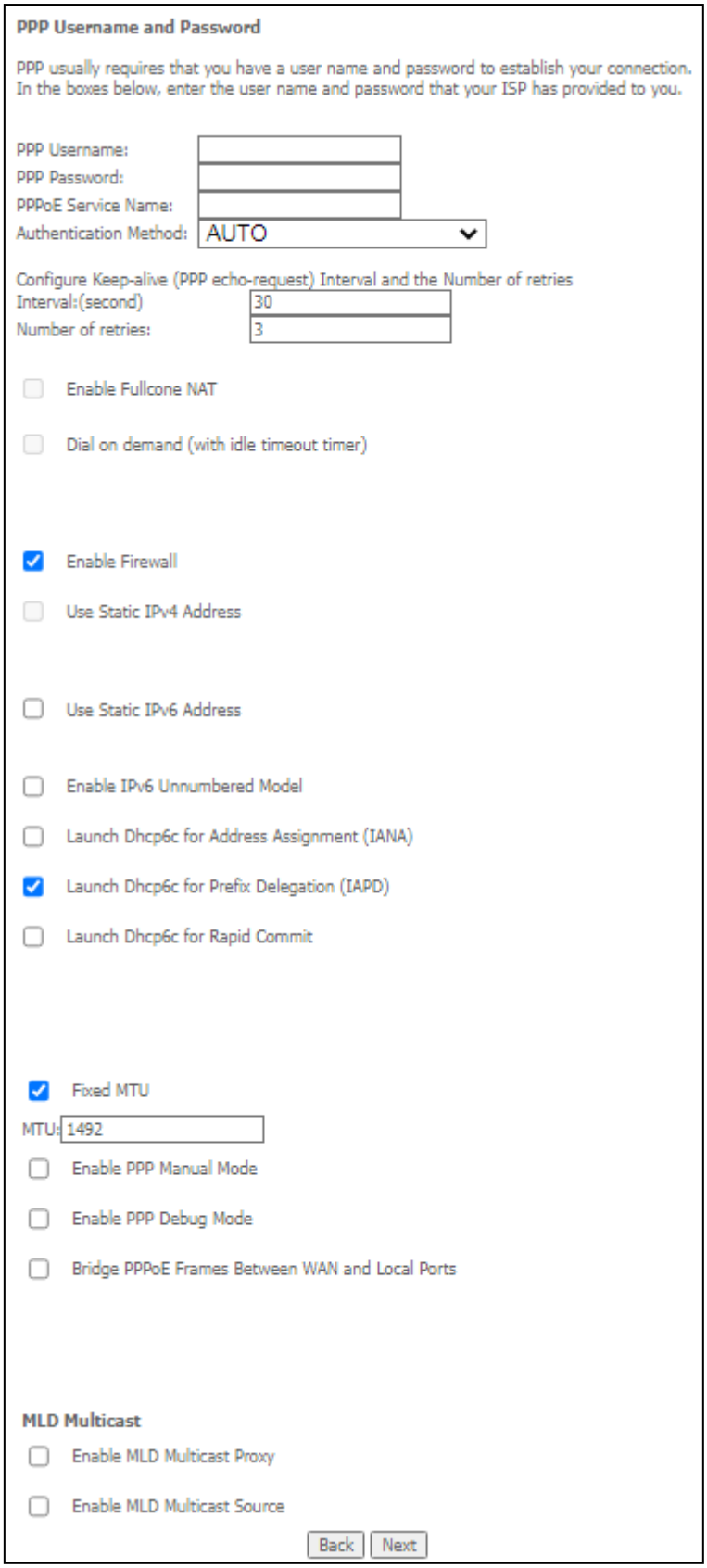
After clicking **Apply/Save**, the new service should appear on the main screen.

F2.6 PPP over ETHERNET (PPPoE) – IPv6

STEP 1: Select the PPP over Ethernet radio button. Then select IPv6 only from the drop-down box at the bottom off the screen and click **Next**.



STEP 2: On the next screen, enter the PPP settings as provided by your ISP.



Click **Next** to continue or click **Back** to return to the previous step.
The settings shown above are described below.

PPP SETTINGS
The PPP Username, PPP password and the PPPoE Service Name entries are dependent on the particular requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. For Authentication Method, choose from AUTO, PAP, CHAP, and MSCHAP.

CONFIGURE KEEP-ALIVE
Configures the interval and number of keep alive packets (PPP echo-request) sent by the device for the PPP connection.
Interval (second): Time between sending out each PPP echo-request packet.
Number of retries: Number of retries before PPP connection is dropped.

ENABLE FULLCONE NAT
Not available for IPv6.

DIAL ON DEMAND
Not available for IPv6.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS
Not available for IPv6.

USE STATIC IPv6 ADDRESS
Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IPv6 Address** field.
Don't forget to adjust the IP configuration to Static IP Mode as described in section 3.2 IP Configuration.

ENABLE IPv6 UNNUMBERED MODEL
The IP unnumbered configuration command allows you to enable IP processing on a serial interface without assigning it an explicit IP address. The IP unnumbered interface can "borrow" the IP address of another interface already configured on the router, which conserves network and address space.

LAUNCH DHCP6C FOR ADDRESS ASSIGNMENT (IANA)
The Internet Assigned Numbers Authority (IANA) is a department of ICANN responsible for coordinating some of the key elements that keep the Internet running smoothly. Whilst the Internet is renowned for being a worldwide network free from central coordination, there is a technical need for some key parts of the Internet to be globally coordinated, and this coordination role is undertaken by IANA.
Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet. IANA's various activities can be broadly grouped in to three categories:

- Domain Names
  IANA manages the DNS Root, the .int and .arpa domains, and an IDN practices resource.
- Number Resources
  IANA coordinates the global pool of IP and AS numbers, providing them to Regional Internet Registries.
- Protocol Assignments
  Internet protocols' numbering systems are managed by IANA in conjunction with standards bodies.

LAUNCH DHCP6C FOR PREFIX DELEGATION (IAPD)
An Identity Association for Prefix Delegation (IAPD) is a collection of prefixes assigned to a requesting device. A requesting device may have more than one IAPD; for example, one for each of its interfaces.
A prefix-delegating router (DHCPv6 server) selects prefixes to be assigned to a requesting router (DHCPv6 client) upon receiving a request from the client. The server can select prefixes for a requesting client by using static and dynamic assignment mechanisms. Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID.
When the delegating router receives a request from a client, it checks if there is a static binding configured for the IAPD in the client's message. If a static binding is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.
An IPv6 prefix delegating router can also select prefixes for a requesting router based on an external authority such as a RADIUS server using the Framed-IPv6-Prefix attribute.

LAUNCH DHCP6C FOR RAPID COMMIT
Rapid-Commit; is the process (option) in which a Requesting Router (DHCP Client) obtains "configurable information" (configurable parameters) from a Delegating Router (DHCP Server) by using a rapid DHCPv6 two-message exchange. The messages that are exchanged between the two routers (RR and DR) are called the DHCPv6 "SOLICIT" message and the DHCPv6 "REPLY" message.

FIXED MTU
Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1492 for PPPoE.

ENABLE PPP MANUAL MODE
Use this button to manually connect/disconnect PPP sessions.

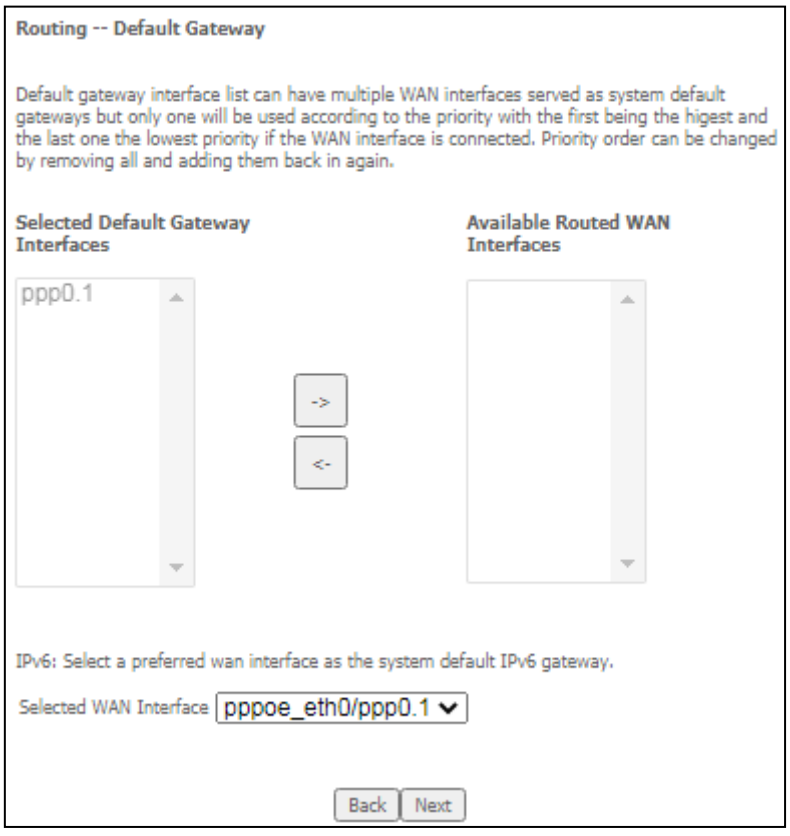
ENABLE PPP DEBUG MODE
When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

BRIDGE PPPOE FRAMES BETWEEN WAN AND LOCAL PORTS
(This option is hidden when PPP IP Extension is enabled)
When Enabled, this creates local PPPoE connections to the WAN side. Enable this option only if all LAN-side devices are running PPPoE clients, otherwise disable it. The PBL-6201v2 supports pass-through PPPoE sessions from the LAN side while simultaneously running a PPPoE client from non-PPPoE LAN devices.

ENABLE MLD MULTICAST PROXY
Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

ENABLE MLD MULTICAST SOURCE
Click to allow use of this WAN interface as Multicast Listener Discovery (MLD) multicast source.

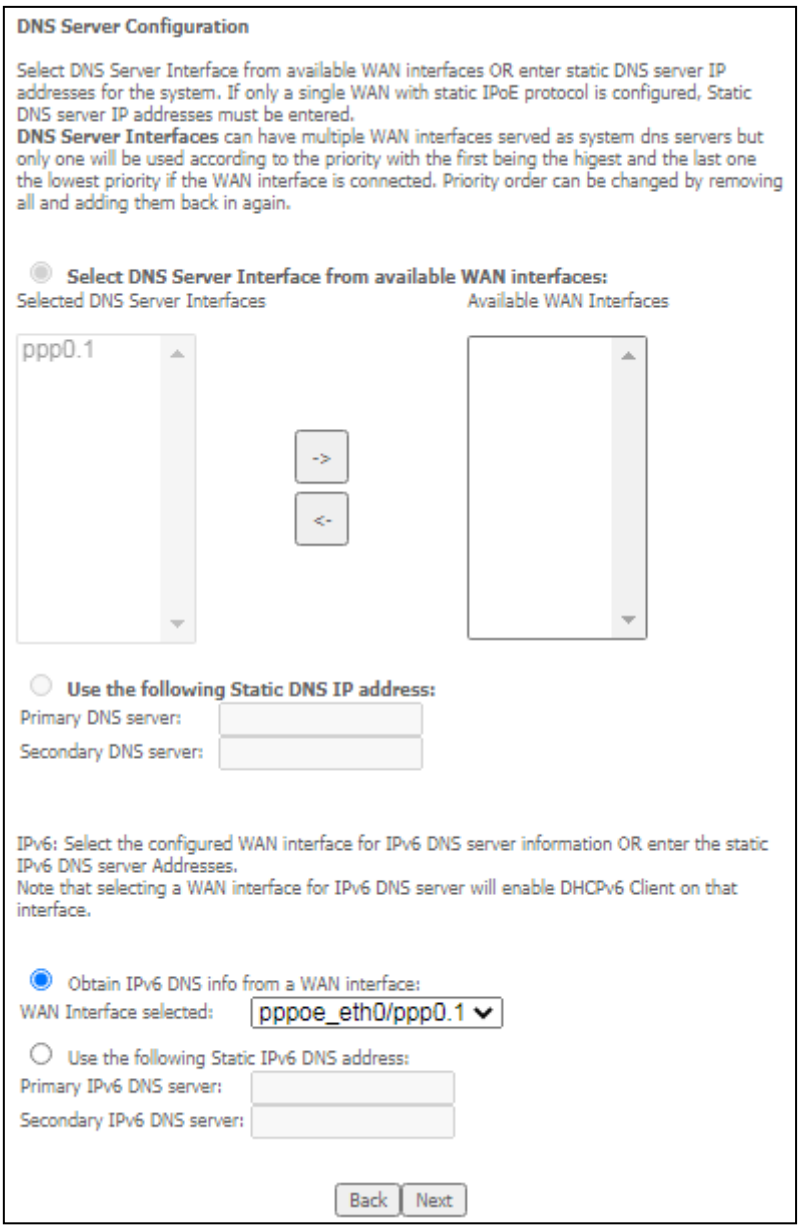
STEP 3: Choose an interface to be the default gateway. Also, select a preferred WAN interface as the system default IPv6 gateway (from the drop-down box).



Click **Next** to continue or click **Back** to return to the previous step.

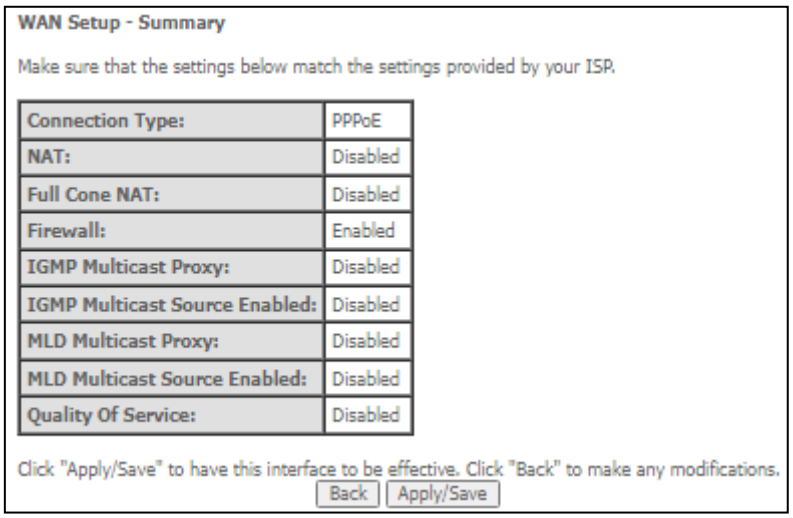
STEP 4: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.

Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses. Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.



Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoE
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

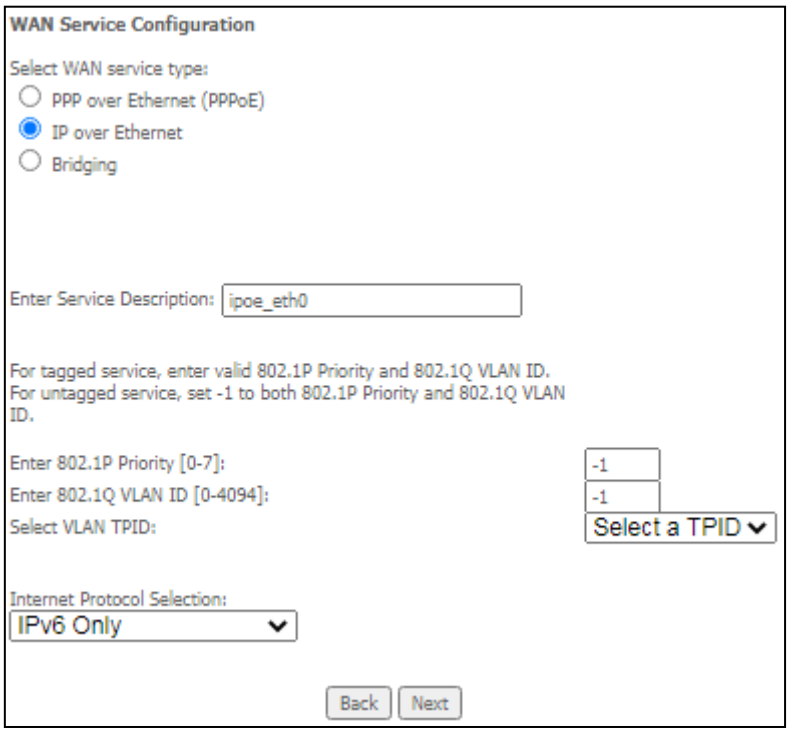
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

After clicking **Apply/Save**, the new service should appear on the main screen.

F2.7 IP over ETHERNET (IPoE) – IPv6

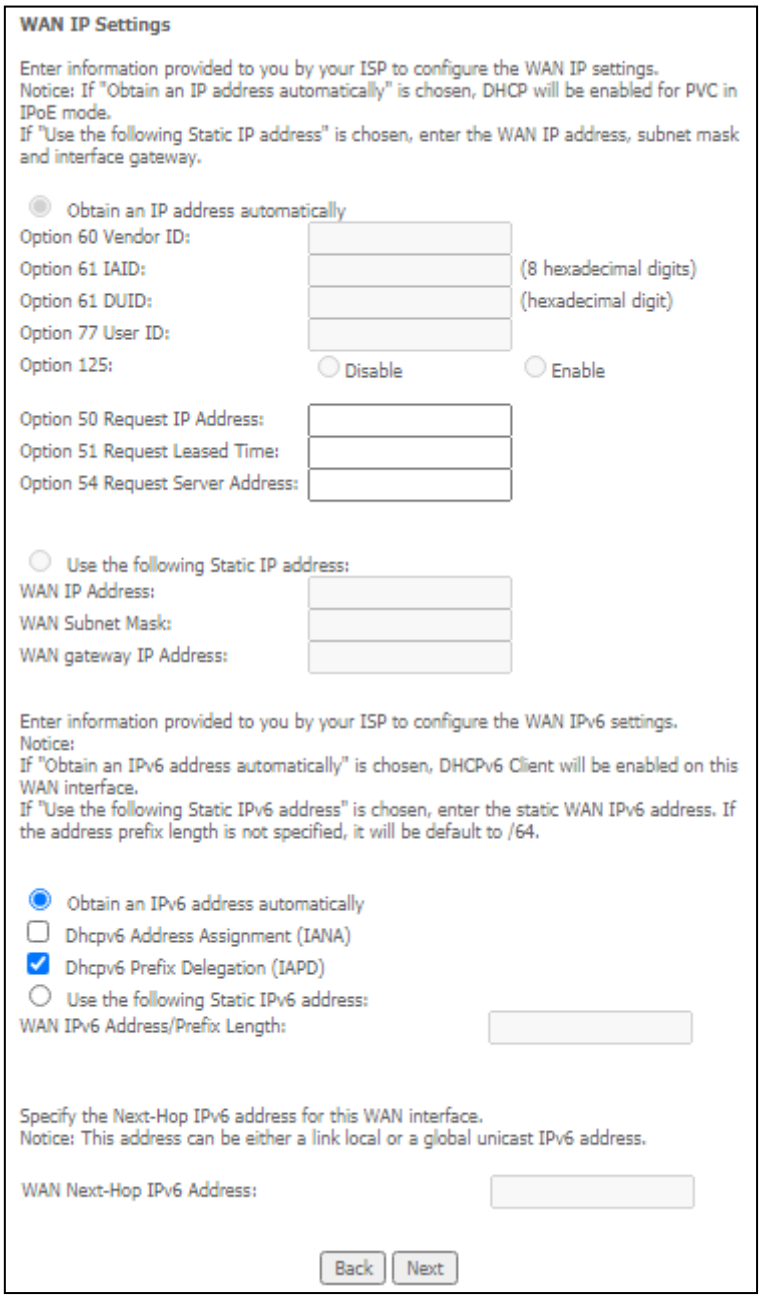
STEP 1: Select the IP over Ethernet radio button and click **Next.** Then select IPv6 only from the drop-down box at the bottom off the screen and click **Next**.



STEP 2: The WAN IP settings screen provides access to the DHCP server settings. You can select the **Obtain an IPv6 address automatically** radio button to enable DHCP (use the DHCP Options only if necessary). However, if you prefer, you can use the **Static IPv6 address** method instead to assign WAN IP address, Subnet Mask and Default Gateway manually.

Enter information provided to you by your ISP to configure the WAN IPv6 settings.

Notice: If "Obtain an IPv6 address automatically" is chosen, DHCP client will be enabled on this WAN interface.
If "Use the following Static IPv6 address" is chosen, enter the static WAN IPv6 address. If the address prefix length is not specified, it will be default to /64.



Click **Next** to continue or click **Back** to return to the previous step.

DHCP6C FOR ADDRESS ASSIGNMENT (IANA)

The Internet Assigned Numbers Authority (IANA) is a department of ICANN responsible for coordinating some of the key elements that keep the Internet running smoothly. Whilst the Internet is renowned for being a worldwide network free from central coordination, there is a technical need for some key parts of the Internet to be globally coordinated, and this coordination role is undertaken by IANA.

Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet. IANA's various activities can be broadly grouped in to three categories:

- Domain Names
  IANA manages the DNS Root, the .int and .arpa domains, and an IDN practices resource.
- Number Resources
  IANA coordinates the global pool of IP and AS numbers, providing them to Regional Internet Registries.
- Protocol Assignments
  Internet protocols' numbering systems are managed by IANA in conjunction with standards bodies.

DHCP6C FOR PREFIX DELEGATION (IAPD)

An Identity Association for Prefix Delegation (IAPD) is a collection of prefixes assigned to a requesting device. A requesting device may have more than one IAPD; for example, one for each of its interfaces.

A prefix-delegating router (DHCPv6 server) selects prefixes to be assigned to a requesting router (DHCPv6 client) upon receiving a request from the client. The server can select prefixes for a requesting client by using static and dynamic assignment mechanisms. Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID.

When the delegating router receives a request from a client, it checks if there is a static binding configured for the IAPD in the client's message. If a static binding is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.

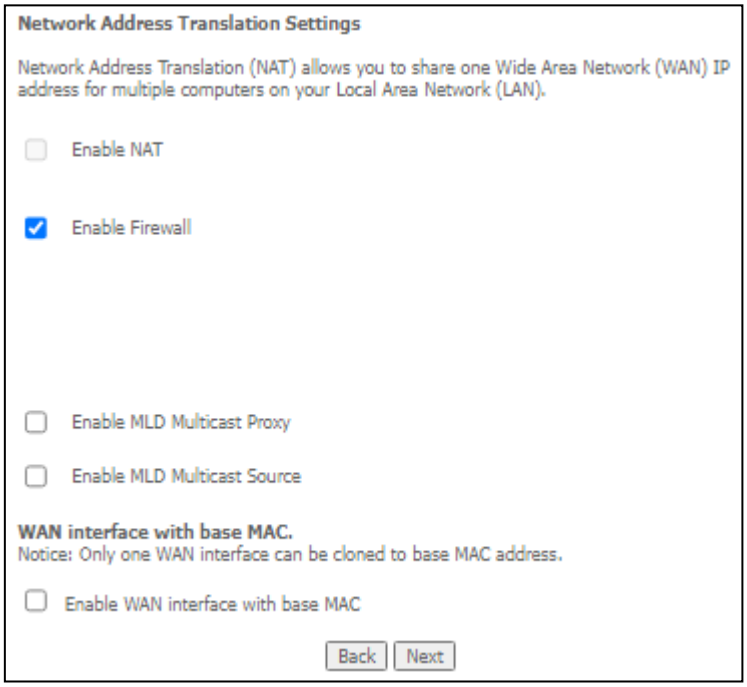
An IPv6 prefix delegating router can also select prefixes for a requesting router based on an external authority such as a RADIUS server using the Framed-IPv6-Prefix attribute.

WAN NEXT-HOP IPv6 ADDRESS

Specify the Next-Hop IPv6 address for this WAN interface.

This address can be either a link local or a global unicast IPv6 address.

STEP 3: This screen provides access to NAT, Firewall and IGMP Multicast settings. Enable each by selecting the appropriate checkbox ☑.



Click **Next** to continue or click **Back** to return to the previous step.

ENABLE NAT
Not available for IPv6.

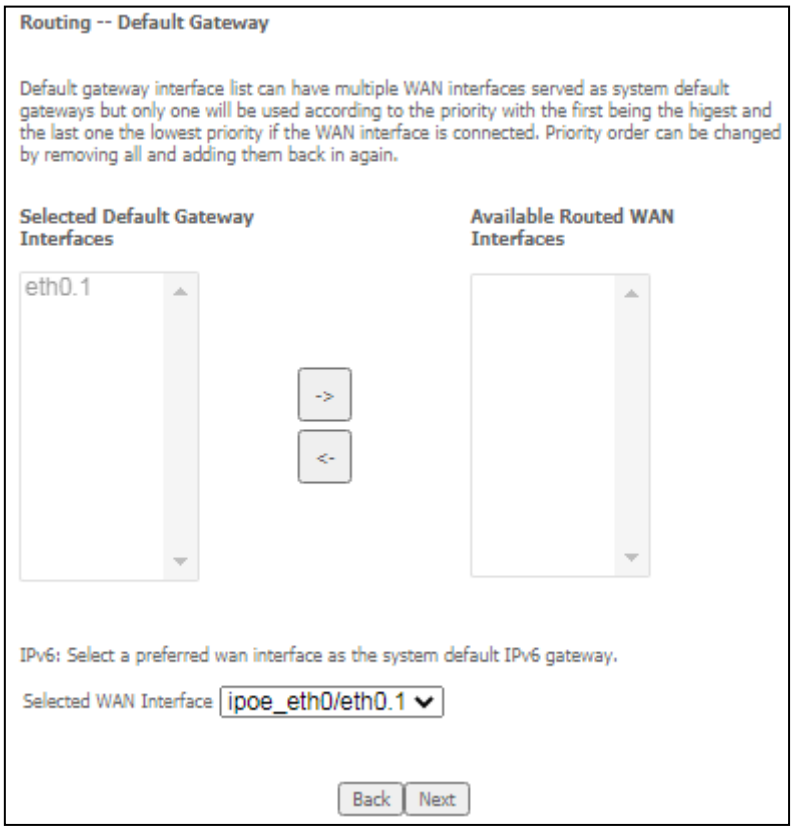
ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected so as to free up system resources for better performance.

ENABLE MLD MULTICAST PROXY
Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

ENABLE MLD MULTICAST SOURCE
Click to allow use of this WAN interface as Multicast Listener Discovery (MLD) multicast source.

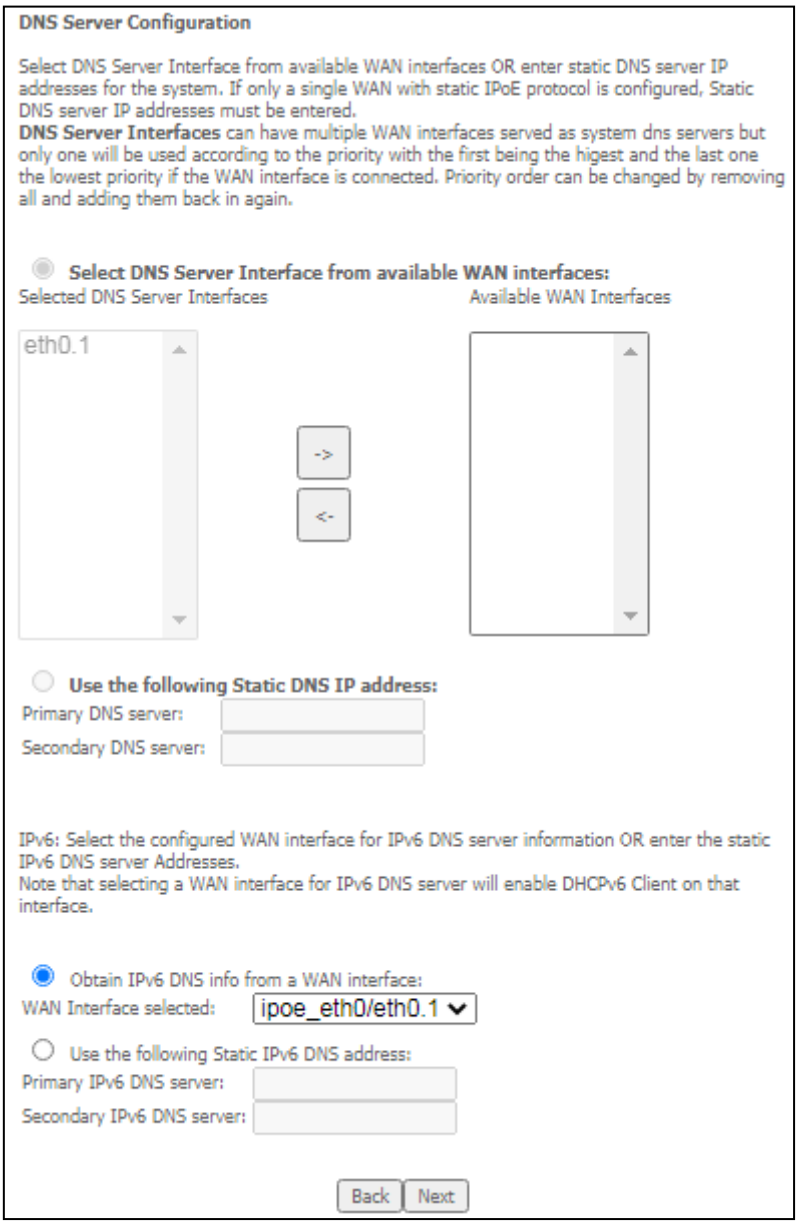
Enable WAN interface with base MAC
Enable this option to use the router's base MAC address as the MAC address for this WAN interface.

STEP 4: To choose an interface to be the default gateway. Also, select a preferred WAN interface as the system default IPv6 gateway (from the drop-down box).



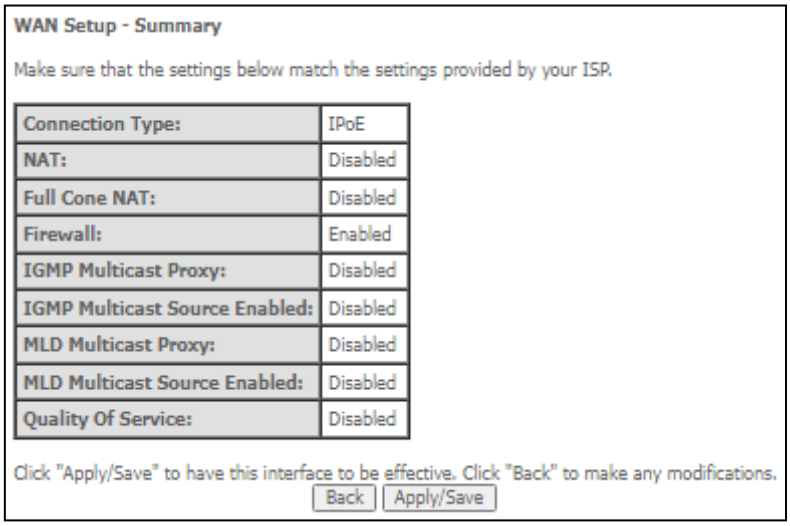
Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: Select DNS Server Interface from available WAN interfaces OR enter static DNS server IP addresses for the system. In ATM mode, if only a single PVC with IPoA or static IPoE protocol is configured, Static DNS server IP addresses must be entered.



Click **Next** to continue or click **Back** to return to the previous step.

STEP 6: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	IPoE
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

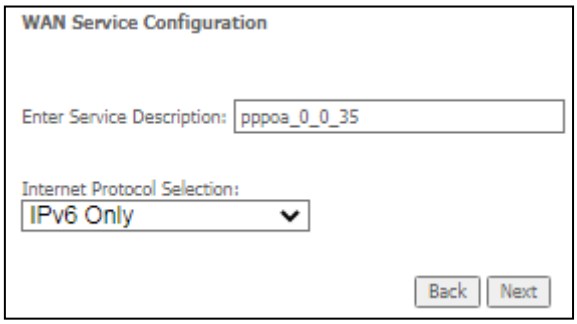
Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

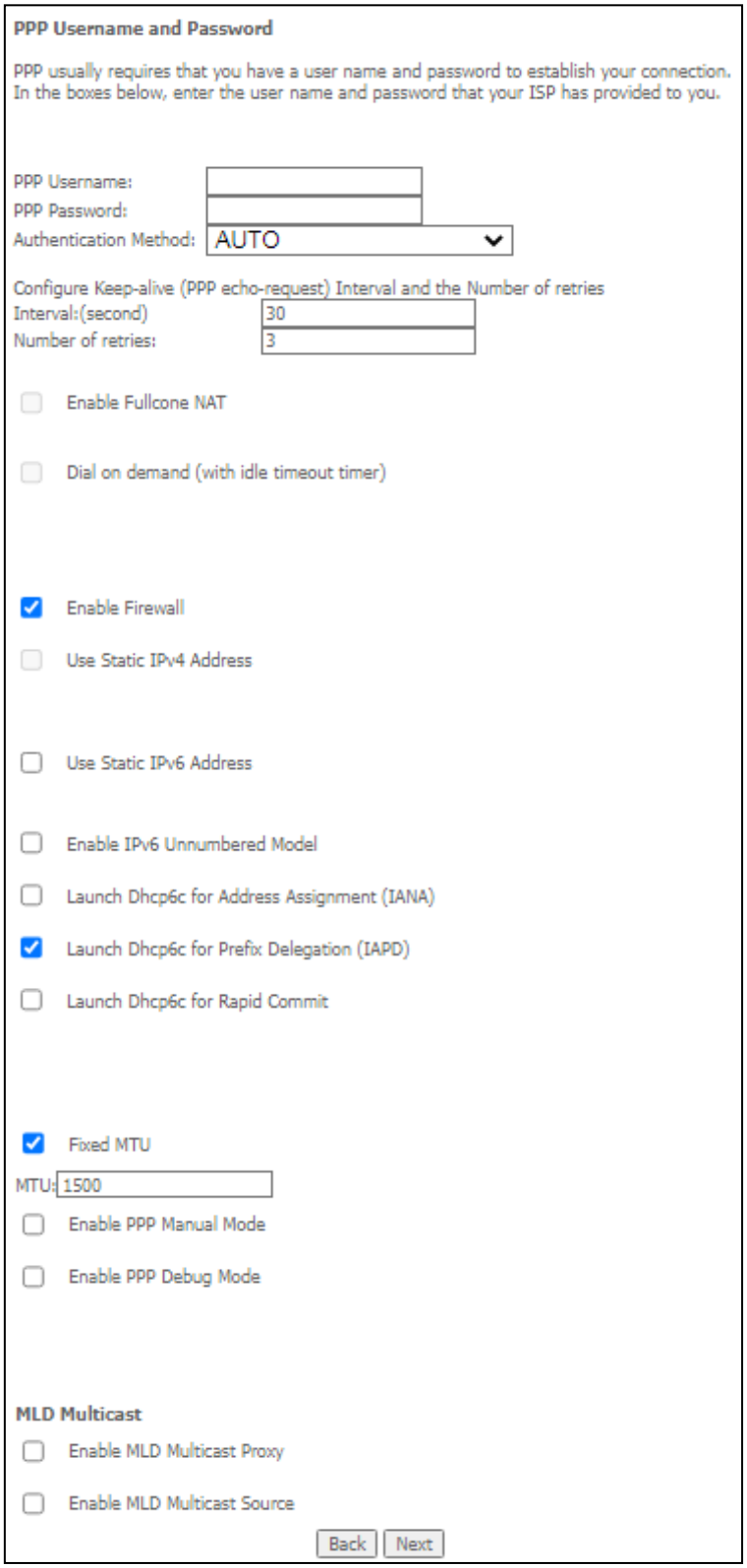
After clicking **Apply/Save**, the new service should appear on the main screen.

F2.8 PPP over ATM (PPPoA) – IPv6

STEP 1: Select IPv6 Only from the drop-down box at the bottom of this screen and click **Next**.



STEP 2: On the next screen, enter the PPP settings as provided by your ISP. Click **Next** to continue or click **Back** to return to the previous step.



PPP SETTINGS

The PPP username and password are dependent on the requirements of the ISP. The user name can be a maximum of 256 characters and the password a maximum of 32 characters in length. (Authentication Method: AUTO, PAP, CHAP, or MSCHAP.)

CONFIGURE KEEP-ALIVE
Configures the interval and number of keep alive packets (PPP echo-request) sent by the device for the PPP connection.
Interval (second): Time between sending out each PPP echo-request packet.
Number of retries: Number of retries before PPP connection is dropped.

ENABLE FULLCONE NAT
Not available for IPv6.

DIAL ON DEMAND
Not available for IPv6.

ENABLE FIREWALL
If this checkbox ☑ is selected, the Security submenu will be displayed on the Advanced Setup menu after reboot. If firewall is not necessary, this checkbox ☑ should not be selected to free up system resources for better performance.

USE STATIC IPv4 ADDRESS
Not available for IPv6.

USE STATIC IPv6 ADDRESS
Unless your service provider specially requires it, do not select this checkbox ☑. If selected, enter the static IP address in the **IPv6 Address** field.
Don't forget to adjust the IP configuration to Static IP Mode as described in section 3.2 IP Configuration.

ENABLE IPv6 UNNUMBERED MODEL
The IP unnumbered configuration command allows you to enable IP processing on a serial interface without assigning it an explicit IP address. The IP unnumbered interface can "borrow" the IP address of another interface already configured on the router, which conserves network and address space.

LAUNCH DHCP6C FOR ADDRESS ASSIGNMENT (IANA)
The Internet Assigned Numbers Authority (IANA) is a department of ICANN responsible for coordinating some of the key elements that keep the Internet running smoothly. Whilst the Internet is renowned for being a worldwide network free from central coordination, there is a technical need for some key parts of the Internet to be globally coordinated, and this coordination role is undertaken by IANA.

Specifically, IANA allocates and maintains unique codes and numbering systems that are used in the technical standards ("protocols") that drive the Internet. IANA's various activities can be broadly grouped in to three categories:

- Domain Names
  IANA manages the DNS Root, the .int and .arpa domains, and an IDN practices resource.
- Number Resources
  IANA coordinates the global pool of IP and AS numbers, providing them to Regional Internet Registries.
- Protocol Assignments
  Internet protocols' numbering systems are managed by IANA in conjunction with standards bodies.

LAUNCH DHCP6C FOR PREFIX DELEGATION (IAPD)
An Identity Association for Prefix Delegation (IAPD) is a collection of prefixes assigned to a requesting device. A requesting device may have more than one IAPD; for example, one for each of its interfaces.
A prefix-delegating router (DHCPv6 server) selects prefixes to be assigned to a requesting router (DHCPv6 client) upon receiving a request from the client. The server can select prefixes for a requesting client by using static and dynamic assignment mechanisms. Administrators can manually configure a list of prefixes and associated preferred and valid lifetimes for an IAPD of a specific client that is identified by its DUID.
When the delegating router receives a request from a client, it checks if there is a static binding configured for the IAPD in the client's message. If a static binding is present, the prefixes in the binding are returned to the client. If no such binding is found, the server attempts to assign prefixes for the client from other sources.
An IPv6 prefix delegating router can also select prefixes for a requesting router based on an external authority such as a RADIUS server using the Framed-IPv6-Prefix attribute.

LAUNCH DHCP6C FOR RAPID COMMIT
Rapid-Commit; is the process (option) in which a Requesting Router (DHCP Client) obtains "configurable information" (configurable parameters) from a Delegating Router (DHCP Server) by using a rapid DHCPv6 two-message exchange. The messages that are exchanged between the two routers (RR and DR) are called the DHCPv6 "SOLICIT" message and the DHCPv6 "REPLY" message.

FIXED MTU
Fixed Maximum Transmission Unit. The size (in bytes) of largest protocol data unit which the layer can pass onwards. This value is 1500 for PPPoA.

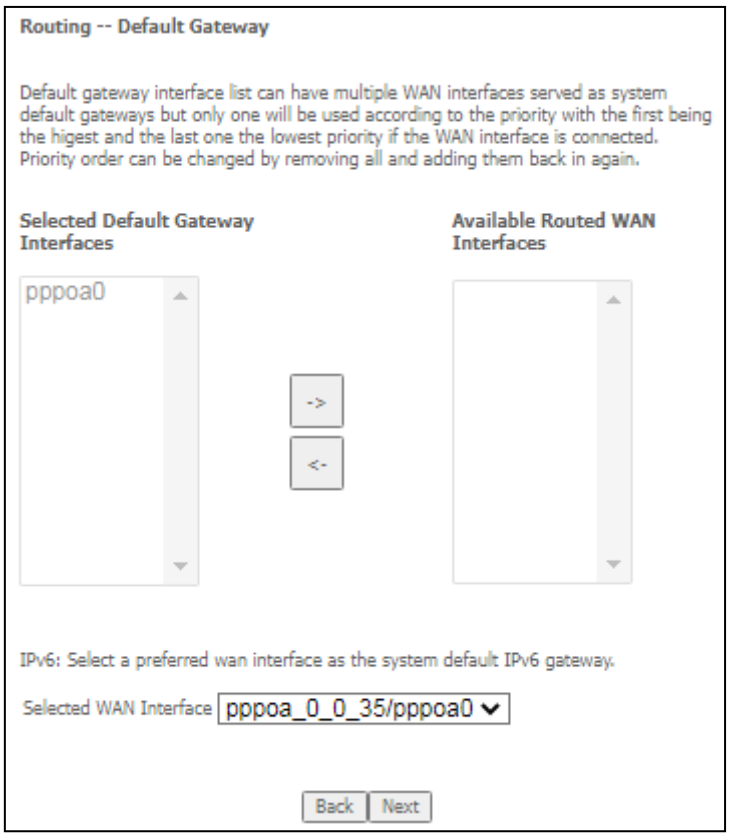
ENABLE PPP MANUAL MODE
Use this button to manually connect/disconnect PPP sessions.

ENABLE PPP DEBUG MODE
When this option is selected, the system will put more PPP connection information into the system log. This is for debugging errors and not for normal usage.

ENABLE MLD MULTICAST PROXY
Multicast Listener Discovery (MLD) is a component of the Internet Protocol Version 6 (IPv6) suite. MLD is used by IPv6 routers for discovering multicast listeners on a directly attached link, much like IGMP is used in IPv4. The protocol is embedded in ICMPv6 instead of using a separate protocol.

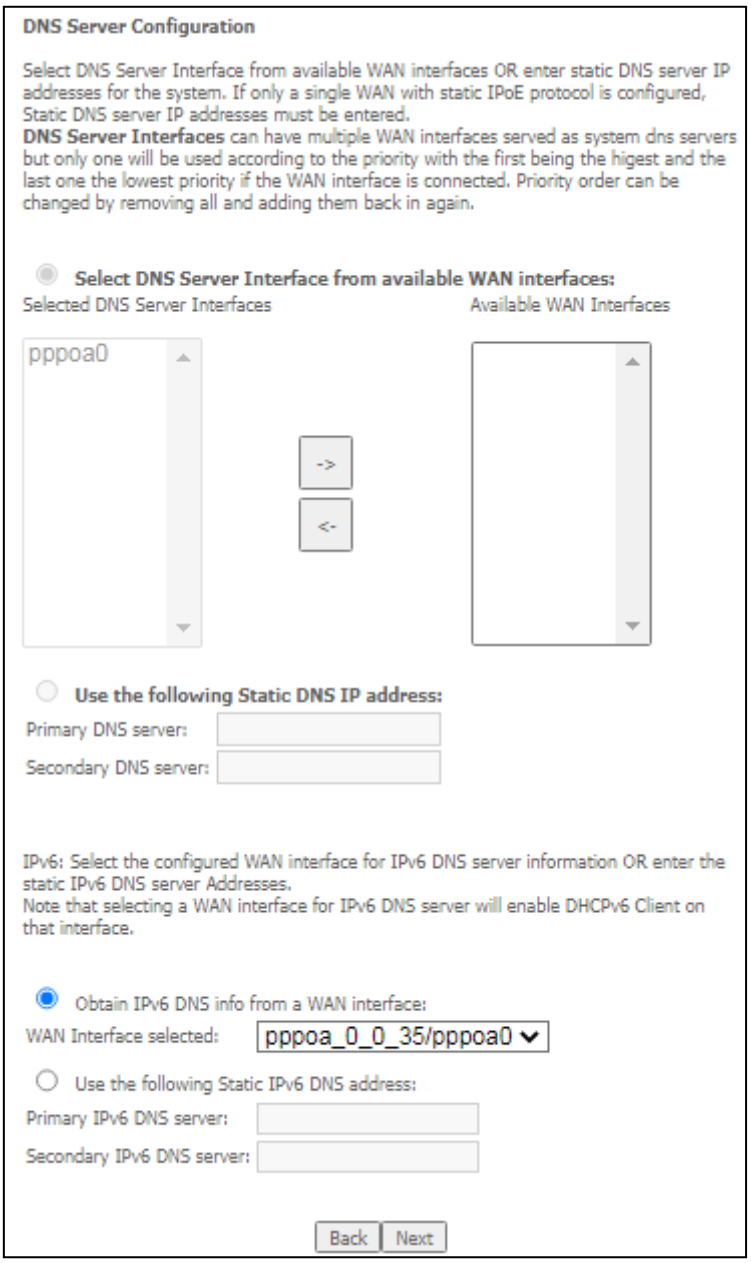
ENABLE MLD MULTICAST SOURCE
Click to allow use of this WAN interface as Multicast Listener Discovery (MLD) multicast source.

STEP 3: Choose an interface to be the default Ipv6 gateway.



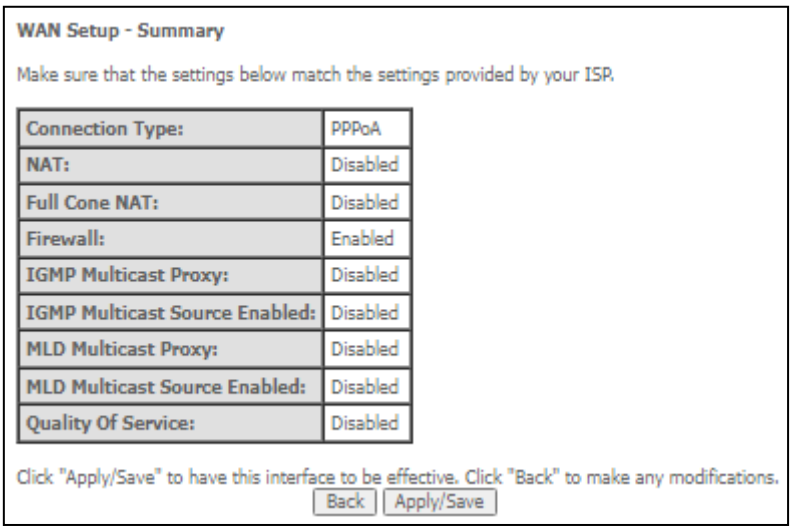
Click **Next** to continue or click **Back** to return to the previous step.

STEP 4: Select the configured WAN interface for IPv6 DNS server information OR enter the static IPv6 DNS server Addresses. Note that selecting a WAN interface for IPv6 DNS server will enable DHCPv6 Client on that interface.



Click **Next** to continue or click **Back** to return to the previous step.

STEP 5: The WAN Setup - Summary screen shows a preview of the WAN service you have configured. Check these settings and click **Apply/Save** if they are correct, or click **Back** to modify them.



WAN Setup - Summary

Make sure that the settings below match the settings provided by your ISP.

Connection Type:	PPPoA
NAT:	Disabled
Full Cone NAT:	Disabled
Firewall:	Enabled
IGMP Multicast Proxy:	Disabled
IGMP Multicast Source Enabled:	Disabled
MLD Multicast Proxy:	Disabled
MLD Multicast Source Enabled:	Disabled
Quality Of Service:	Disabled

Click "Apply/Save" to have this interface to be effective. Click "Back" to make any modifications.

Back Apply/Save

After clicking **Apply/Save**, the new service should appear on the main screen.